UNIVERSITY OF AMSTERDAM

SYSTEM AND NETWORK ENGINEERING

RESEARCH PROJECT 1

Traffic anomaly detection using a distributed measurement network

Author:
Razvan C. OPREA

Supervisor:
Emile ABEN

February 22, 2012

Abstract

This report focuses on the relationship between traffic anomalies and the data collected by the RIPE Atlas measurement network. Two distinct vectors of research are used: first, a ground-truth search which looks to see in what degree real-life network events reflect in the RIPE Atlas data, and second, the collected data is analyzed to find the time and location where several probes' measurements in a certain network or geographical area yield abnormal results. The ground-truth events searched are not found with a good degree of confidence in the Atlas data and the possible reasons are detailed in the paper. The data analysis uses control charts to map the deviations from the mean of each probe. Two methods for aggregating the results in a certain area are then proposed.

Contents

1

Introduction

1.1 General overview

With the continuous expansion of the Internet, the need for accurate and objective performance measurements became more and more acute. The Réseaux IP Européens Network Coordination Centre (RIPE NCC), an independent, not-for-profit membership organization that supports the infrastructure of the Internet through technical coordination in its service region[15] (Europe, Middle East and parts of Asia), started such a project in 1998 to fill this need in its service region. The service is called Test Traffic Measurement Service (TTM) and consists of a network of about 100 measurement devices with GPS (Global Positioning System) antennas connected to them for synchronization and increased time accuracy. TTM's main purpose is to provide standardized metrics for one-way delay and one-way packet loss between measurement devices in a format which is easily understood by users[16]

After more than 10 years, RIPE NCC launched in 2010 a new distributed measurement network which measures critical operational aspects of the Internet infrastructure in real time - the RIPE Atlas. This new measurement network was designed to be extremely scalable, economically produced and deployed and thus being equally suitable for end users and network operators.

RIPE Atlas's goal is ”to produce an atlas of different kinds of high-resolution maps of the Internet: geographical, topological, real-time, long-term and in many novel and useful formats. As with classical geographic mapping, those maps will get more accurate” with the increase of the number of measurement points.[12]

While global network events visibility is important and as such a global presence is needed for the Atlas network, RIPE NCC's focus is on the RIPE service region and therefore, this is the area with the highest density of Atlas probes.

Volunteers from anywhere in the world can register to receive a free probe and, upon receiving and connecting the probe they become ”RIPE Atlas hosts” and participate in the global Atlas measurement network.

Each host can then login to the RIPE Atlas website and see, in a graphical representation, the results of the network measurements his probe performed. The host has also the option of making his probe public, allowing for any other host to access his own measurement results, and, in turn he can access the data produced by any other public probes.

The first 300 probes were distributed among the attendees of RIPE 61, in November 2010. As of January 2012, over 1024 Atlas probes have been deployed worldwide. The Figure 1.1 displays the actual coverage map: the probes actively doing measurements are represented by green triangles, while the probes which have not performing measurements for the last 5 days are represented by red triangles.

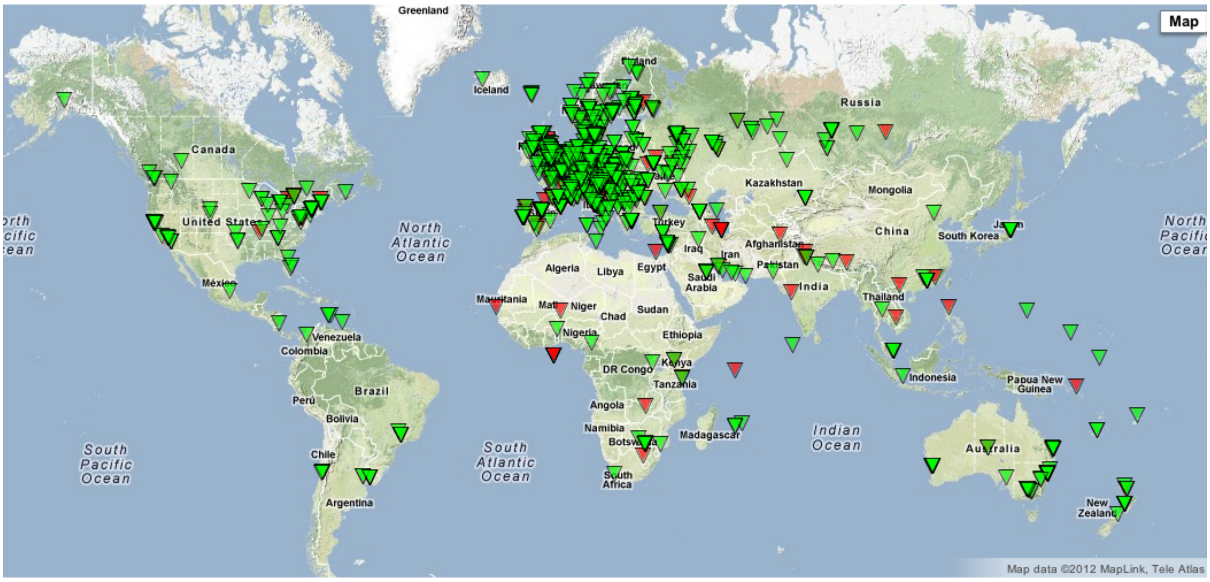


Figure 1.1: RIPE Atlas coverage map

The focus of this paper is to determine in what degree Internet traffic anomalies are reflected in the results of the measurements performed by the Atlas network.

1.2 RIPE Atlas Network

The RIPE Atlas network consists of many small hardware devices (probes) which run measurements and pass the results to a controlling infrastructure for storage, processing and presentation of the data. The probes which perform the active network measurements are located on the end-points of Internet distribution (for example, on customer premises, in data centers, etc.). Both the number and the diversity of vantage points offers new potential for network operational situational awareness.

The RIPE Atlas hardware probes are thumb size miniature devices, Universal Serial Bus (USB) -powered, featuring an RJ-45 connector for 10base-T and 100base-TX Ethernet connectivity (Figure 1.2). They are based on the Lantronix XPort Pro embedded networking module with custom powering and housing, featuring a Lantronix DSTni-FX 32-bit microprocessor, running at 166 MHz internal bus and 83 MHz external bus, with 16 MB Flash and 8 MB SDRAM.

The Atlas probes are designed to be maintenance-free; even the installation requires only the physical connection to a free Ethernet port for connectivity and to a USB (5V, 500mA) socket for power. The probe will use Dynamic Host Configuration protocol (DHCP) for obtaining Internet Protocol version 4 (IPv4), Internet Protocol version 6 (IPv6) addresses and Domain Name Service (DNS) resolver address. The connection to the controlling infrastructure is done using outgoing Hypertext Transfer Protocol (HTTP) over encrypted Secure Sockets Layer (SSL) connections on port 443.

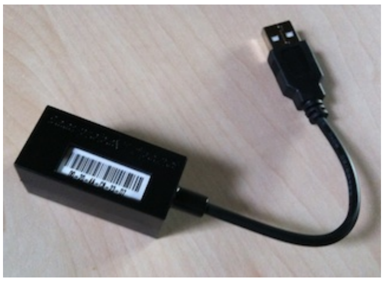


Figure 1.2: RIPE Atlas probe

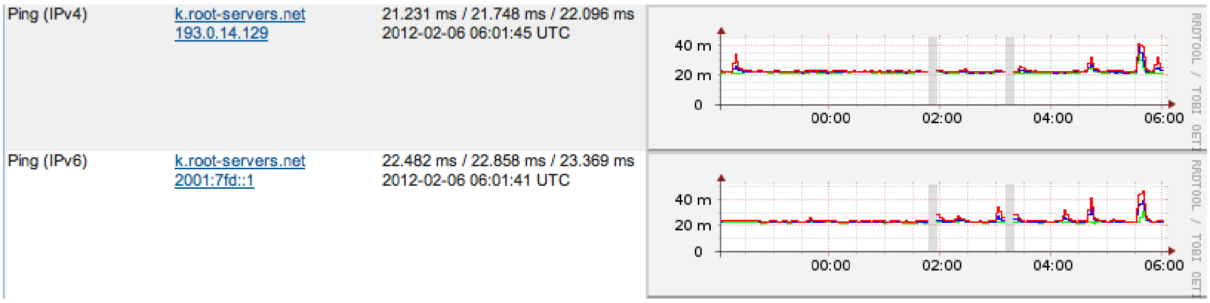
The types of measurements performed by the probes are:

- Internet Protocol version 4 and 6 (IPv4 and IPv6) Internet Control Message protocol (ICMP) echo requests (ping) determining the Round-Trip Time (RTT) and the packet loss
- traceroute to fixed anycast and unicast[1] destinations
- DNS Start of Authority (SOA) resource record checking for the root name servers
- Determination of the instance names of the anycast root name servers[2]
- User-defined measurements

The user defined measurements are customized tests the hosts can run against the entire RIPE Atlas network in addition to the tests performed by the probes by default.. The maximum number of destinations and the frequency of the measurements is in direct correlation with the number of probes the hosts have and with their total uptime.

Indirect information is obtained by retrieving the times in which the host was down (for instance, due to a power outage). These measurements have not been used in this research, but they could prove useful for future research in this topic.

Figure 1.3 shows IPv4 and IPv6 RTT measurements to an anycast destination (K-root DNS server), as they are seen in the web-based user interface.



Ping (IPv4)	k.root-servers.net 193.0.14.129	21.231 ms / 21.748 ms / 22.096 ms 2012-02-06 06:01:45 UTC
Ping (IPv6)	k.root-servers.net 2001:7fd::1	22.482 ms / 22.858 ms / 23.369 ms 2012-02-06 06:01:41 UTC

Figure 1.3: RTT measurements to an anycast destination

1.3 Similar Projects

Many other projects focused on Internet network measurements exist, in various phases of development and deployment. Two of the better-known ones are SamKnows and Project BISmark.

SamKnows

SamKnows is a commercial project developed by SamKnows Limited and run with the help of a community of volunteers. It receives funding from, among others, the United States Federal

[1] http://en.wikipedia.org/wiki/Routing#Delivery_semantics
[2] http://tools.ietf.org/rfc/rfc4892.txt

Communications Commission (US FCC) and, since the fall of 2011, the European Commission[13]. Its goal is to measure consumers' broadband Internet connection speeds by collecting performance data which is used by regulators, consumers, industry and consumers[23]

Volunteers register to receive a TP-Link router (various models) running a modified firmware which will be used as a bridge, being placed in between the existing router and the networked computers in the home. In this way, all the traffic in the home network will have to pass through the measurement device (router), which, in turn, will run a battery of measurements when the uplink is not congested. In the US the device provides also a wireless network, while in Europe, the wireless capability of the device are solely used for passive monitoring of the wireless traffic. Remote troubleshooting, if necessary, is done by means of a Secure Shell (SSH) session initiated after the user's consent.

The tests run by SamKnows measurement device range from layer 3 network measurement - packet loss and latency using ICMP and User Datagram Protocol (UDP) packets, DNS query resolution time to application layer testing - Multi-threaded HTTP download and upload speed test.[22]

Project BISmark

Broadband Internet Service BenchMARK (BISmark) is an academic project led by Georgia Tech and the University of Napoli Federico II to conduct measurements on the Internet access links. The measurement device is a NetGear WNDR3700v2 router with an OpenWRT-based firmware which is intended to perform measurements of Internet Service Provider's (ISP) performance, as well as traffic inside the home.[2]. The founding of the project comes from the US National Science Foundation (NSF) and Google Inc.

The project is still in an incipient stage: in September 2011 the first batch of 20 routers were flashed and sent to customers, the data presentation web interface is still under development and the set of measurements is limited at the moment to Round-Trip Time (RTT) and upload and download throughput.

Project BISmark require the volunteers to plug the measurement router into their existing router, or, preferably, to replace their home router with the one received from Project BISmark - a major difference to SamKnows, whose device does not act as a router, but only as a bridge. Also, the Netgear router from Project BISmark creates two wireless networks intended to be used by the volunteer (using the 2.4 GHz frequency band and respectively the 5 GHz one) and has a visual indicator on the measurements (the WPS LED on the router blinks while measurements are conducted)

Project BISmark also allows users to download the modified firmware and use it to program their own compatible routers.

1.4 Key differences between the projects

SamKnows and Project BISmark share one common objective: providing a clear and objective view on the end -users Internet connectivity. RIPE Atlas, while also using measurement probes at the edges of the network, is equally aimed at end-users, network operators and the Internet at large.

General differences

Each project has a different scope, target user base and area of coverage.

RIPE Atlas:

→ provides up-to-date information about the Internet network status

→ it targets end users as well as network operators

→ global coverage area, but with a focus on the RIPE service region

SamKnows:

→ broadband Internet connections measurement

→ it targets end users only

→ US and European Union (EU) coverage area

Project BISmark:

→ broadband Internet connections measurement

→ it targets end users only

→ global coverage, but it started with US only for now

Technical differences

Each project's architectural decisions has an impact on the probes' form factor, cost, support and capabilities. It is remarkable that the high-level architecture is similar (distributed probes network, backend processing machines and user display of data). While detailed backend information is not available for any measurement network, the probes employed by the RIPE Atlas and the other two networks are very different.

One major difference in probe's architecture is represented by the installation options. If RIPE Atlas can be plugged in any free Ethernet port of any network equipment, the other two measurement networks' probes are actual routers which have to be connected to or replace the existing router of the host network so that all local traffic could pass through them. The stated reason for this requirement is that the probes should be aware of the link congestion and refrain from performing network measurements in those moments.

RIPE Atlas probes:

→ are small and unobtrusive

→ are relatively inexpensive

→ deployment is very easy, no user maintenance is required

→ are distributed as a bundle (hardware plus software)

→ have small computing power, therefore limited types of measurements are possible

SamKnows' and Project BISmark's probes:

→ have to be connected to or replace the host network's router

→ are distributed as a hardware and software bundle or as a software download and the user will provide a compatible hardware

→ have higher computing power, therefore more types of measurements are possible

Differences Conclusion

While the characteristics and differences between the three measurement networks have been detailed, there has to be noted that this short list is not exhaustive by far. There are other measurement networks which deserve to be included in a future research on this topic, for example:

- CAIDA Archipelago[11]
- Netdimes[26]
- iPlane[29]

As shown, RIPE Atlas probes are small and unobtrusive. They do not have any idea on the host network's congestion and cannot therefore schedule their measurements to be performed in the moments when the Internet connection link is not saturated. A valid question is then:

"Assuming there is a traffic anomaly detected by one of the RIPE Atlas probes, how can this event be distinguished between a local problem (congestion for instance) and a problem at an ISP level?"

The answer is that one cannot make always such a distinction by looking at just one probe. But, when looking at other probes in the same geographical area, or network Autonomous Number (AS), there is a clear view on the problem type - depending on if only a single probe experienced an anomaly or if these results are shared among several probes.

Therefore the RIPE Atlas network's real strength comes from the numbers of its measurement devices. Being small, unobtrusive and very easy to install and maintain means it can be deployed in large numbers, and this confers the advantage of multiple vantage points for the same anomaly detected in a network.

In conclusion, while the goals of the distributed measurement networks mentioned are similar in part, they differ in the architecture and implementation of their probes, and, as a consequence, there are major differences in development, deployment and support costs (which partially impacts the scalability) and in the types of measurements each network performs.

2

Research methodology

The scope of this project is to see how real life events reflect in the RIPE Atlas collected data, to examine the feasibility of detecting traffic anomalies using RIPE Atlas and to research methods for localizing these events in a network (same AS for instance) or in a geographical area (same region or country).

Taking into account the type measurements Atlas probes can perform, traffic anomalies can be related to, for instance, availability, jitter or latency.

Research Question

How can the data collected by the RIPE Atlas provide information for indicating a network operational problem?

Hypothesis

The hypothesis is that *it is possible to find the necessary correlation between the RIPE Atlas probes' collected data and the existence of operational issue with a sufficient degree of confidence.*

The research question can be followed-up by two more -in-depth subquestions:

SubQuestion 1

What metrics are useful for traffic anomaly detection in RIPE Atlas data?

SubQuestion 2

How can traffic anomalies detected by the RIPE Atlas be localized within a network or geographic location?

The research conducted has three major parts:

1. Choosing a metric that is suitable for qualitative analysis of the data
2. Considering a list of real-life events, try to see how these are reflected in the RIPE Atlas logs
3. How can the RIPE Atlas data be analyzed in such a way that a traffic anomaly is detected and, potentially localized within a network of geographical area

3

Metric

Choosing a suitable metric is an important first step in researching network anomalies using RIPE Atlas data. Obviously, the metric has to be one of those generated by the RIPE Atlas probes' measurements, as described in Section 1.2:

→ ***Packet loss***

Packet loss is one of the results of the ICMP echo request (ping) measurement that RIPE Atlas probes perform. It is a perfectly adequate metric for measuring performance and determining anomalies in a network, especially when combined with the RTT metric.

→ ***Root name server checks***

The root name server checks (DNS SOA record verification and anycast instance determination) can signal potential problems with some zone transfers between the name servers (not a performance metric) and, in case of the anycast instance query, problems with some anycast instances.

→ ***User defined measurements***

In the second part of 2011, RIPE NCC developed a new firmware version for the probes, which allowed users to define their own measurements parameters. For instance, they can choose to have a number of probes from a certain country or geographical area send ping or traceroute requests to a certain IP address. While useful for troubleshooting, such a measurement comprises only a small subset of the available probes and, being a new feature, there is a limited number of hosts using it.

→ ***Traceroute***

Traceroute is a computer network diagnostic program which sends out a series of IP packets with increasing Time-to-Live (TTL) values towards the destination. The TTL value actually means the *hop count*, the maximum number of hops a packet can go through before being discarded by a router on its path. By receiving successive ICMP Time Exceeded error messages from the routers in the path, the traceroute diagnostic program can actually display the path the packet took towards its destination and the time it took for traversing each hop.

When used for network performance measurements, traceroute can provide some useful statistics, such as the latency per hop and the number of hops towards a destination. It can be reasonably expected that the number of hops to a destination increases or decreases depending on the network events on its path (de-peerings for instance).

→ ***ping (RTT)***

RTT, as measured by the *ping* command which sends out ICMP echo requests to a destination, displays the latency between the two nodes, meaning the time it takes a packet to reach its destination. It records any packet loss that occurred to the tested destination, and it returns three RTT values: the minimum, the maximum and the average. Changes in the RTT values over time can mean, for instance, congestions or network topology changes.

Summarizing the information above, the two metrics that stand out are the RTT and the packet loss. For this research, we focused on the RTT values. In choosing between which network utility should provide the RTT values, *ping* was simpler to work with than *traceroute* and the granularity of its measurements' results was better (the Atlas probes perform one ping for every 4 minutes, compared to one traceroute for every 30 minutes).

There is a wealth of previous work conducted on network performance based on RTT values:

- Dinan Gunawardena et al. show[8] that in ”IP networks, RTT measurements constitute the basic feedback information that end hosts can use to infer the state of the network connection between them”.

- In [10], the authors describe the usage of The Cooperative Association for Internet Data Analysis's (CAIDA) Macroscopic Topology Project to ”collect and analyze Internet-wide topology and latency (round trip time (RTT)) data at a representatively large scale” (few hundred and more than one-half million destinations).

- In [4], the authors agree on RTT measurements being a common method for assessing network latencies and they look further in breaking down symmetric RTT measurements for measuring single direction latency. The RIPE NCC's TTM project also provides single direction latency measurements between its approximatively 100 units distributed around the world.

- In [27], the authors propose a ”Network Radar”, realizing a ”network tomography' using RTT measurements.

4

Ground-Truth Reflection

This chapter looks at how real world events (i.e. ”ground-truth”) reflect in the data collected by the RIPE Atlas probes. The types of events relevant or this search are those who might have affected the Internet network (globally or on a local level) in general and those who might have influenced the RTT measurements of the Atlas probes in particular.

A list of these events localized in time from September 2011 until January 2012 was then made. Obviously, for an event to be reflected in the RIPE Alas data, the probes must ”experience” the event - this means that, at the moment the event occurs, there must have been probes in the area, or otherwise it is likely that the event will not be easily seen. There are exceptions, of course - for instance when a major transit provider has outages, or when de-peerings happen - but it is still much more likely that a reflection of ground-truth in the RIPE Atlas data is found when probes are at or near the location where the event occurred.

Once the real-life events with significant potential for visibility in the RIPE Atlas data have been compiled, the identification or reflection of these events starts. For this purpose, two visualization methods were used. First is the default visual representation of RIPE Atlas measurements results in the web interface available to every host - RRD graphs, plotting RTT values (minimum, maximum and the average) over a time period. The second visualization method is one developed within RIPE NCC, which displays the data in a three-dimensional graph , showing the dates, times and the minimum RTT values per probe.

4.1 Real-life events

When building the list of events, several types were identified. They tend to affect network performance in various ways and thus are seen by the probes differently. For instance, the RTT of a probe to a fixed destination with a network event in its path is altered, but an electrical power failure in an area could mean that the majority of the probes in the area will not reach any destination at all.

Some of the event types considered were:

- ISP outages
- Transit providers outages
- Electrical power outages
- Political unrests and calamities

- Fiber cuts and fiber landings
- Other types of outages

ISP outages

Widespread or long outages in an ISP's network should be seen by the Atlas probes located in its network. The IP address assigned to the probe localizes any probe in a specific AS, allowing the grouping of the Atlas probes' results per AS. The bigger chances of visibility are, of course, the places where there is a high density of Atlas probes, such as Western Europe.

The majority of ISPs have their own outage announcement pages publicly available. Some publish RSS feeds. But relatively few provide historical data with their outages.

Searching for network outages in ISP networks brought the realization of the fact that there are few outages announcements aggregation efforts, but nowhere is a place where this information is aggregated comprehensively, categorized correctly and published in an easy to parse format, such as Extensible Markup Language (XML).

For example:

- in the Netherlands, there is the `http://storingsoverzicht.nl/`. This website, while aggregates outage reports from a variety of sources, mixes and matches all sorts of types of reports, from hosting providers, to network (ADSL and cable) providers and applications malfunctions (such as the post code check on a provider's web site not functioning properly).
- for worldwide outages there is `http://outagecenter.com/`. Like the one mentioned above, this website aggregates everything related to outages or malfunctions, be it Amazon Web Services availability problems to issues with a hosting provider such as Rackspace

Transit providers outages

The webpage `http://www.outages.org/index.php/Dashboard` provides a good list of references to a multitude of major telecom companies and Tier 1 transit providers' outage announcement pages. Unfortunately though, they mostly provide a dashboard-like view of the current state of their services, with little, if any, historical information.

Electrical power outages

An electrical power outage can be very visible, especially if it occurs in a high Atlas probes density area and if it last significantly more than few minutes.

This Wikipedia article `http://en.wikipedia.org/wiki/List_of_power_outages#2011` compiles a list with the major power outages from 2011 and was used as the source for this type of ground-truth search. One of the most visible power outages was in San Diego area, US (September). Another one was a major explosion in Cyprus (July).

Political unrests and calamities

Political unrests in some areas conduct to Internet access and/or transit shut downs. These events are well reflected in the mainstream media. In 2011 politically decided Internet shut downs happened for instance in Egypt (January) and in Libya (February) during the "Arab Spring" movements[5].

Calamities affect the network in an area for a sufficient time for the event to be seen by any Atlas probe in an area. Such an even was for instance in 2011 the Japanese earthquake and tsunami (March)[6].

Fiber cuts and fiber landings

A fiber cut means that some of the traffic has to re-routed to a potentially longer path to a destination, leading to a higher RTT value. Similarly, the a new cable landing has the potential of reducing the RTT by offering a shorter route to a destination.

Fiber cuts are generally reflected in the technology-focused media. There have been relatively few fiber cuts in 2011 - Philippines (May)[18], Northern Egypt (August)[1] and Nebraska, US (October)[21] are few of the most visible instances).

The website `http://www.cablemap.info` generates fiber path maps and compiles the list of all the new cable landings.

The following fiber landings occurred in 2011:

- *TURCYOS-2* - runs between Turkey and Northern Cyprus
- *TGN-Gulf* - links the countries in the Gulf area (regional cable)
- *LIME* - between Jamaica, Dominican Republic and British Virgin Islands
- *JONAH* - links Israel to Italy
- *EIG* - links Western Europe, Northern Africa and Arabic peninsula
- *CeltixConnect* links Ireland to UK
- *Balkans-Italy Network* links Italy with Albania

Other types of outages

This category include any other type of event which might have caused network effects, such as de-peerings and network equipment bugs. While no major de-peering occurred in 2011, the most notable event in this category was a bug in the Juniper routers' firmware update which caused few large outages in some ISP's networks (November)[25]

4.2 Data visualization

From the real-life events sources specified in Section 4.1, most of them were not well localized in time (because they occurred before September 2011) and space (they happened in an area with few, if any RIPE Atlas probes). A notable exception is represented by one of the cable landings, the *JONAH*, which links Italy to Israel and which was commercially launched around 6 January 2012. In Figure 4.1, two probes from Tel Aviv are seen to have a visible drop in their RTT measurements to an European fixed destination two to three weeks after the fiber was put into production. If the graph corresponding to Probe 885 has a single visible drop in RTT measurements, the one corresponding to Probe 99 has multiple increases and drops of RTT for about a week, before settling at a constant value of about 75% from the value it had two weeks prior. Different providers can start using the new cable at different times, which makes it difficult to localize this type of event in time.

Data visualization methodology

For each such event, a visual comparison ensued between all the probes in the affected area to see whether the probes generated different measurement results.

The analysis used two different method for graphical representation of data series: RRD graphs and ”heat maps”.

RRD graphs

Each host of a RIPE Atlas probe has a personalized page on the Atlas portal which contains RRD graphs representing the RTT data of the measurements his probe conducted. The results of each measurement are detailed in graphs with a granularity of 5 minutes, 10 minutes, 1 hour, 1 day and 1 week.

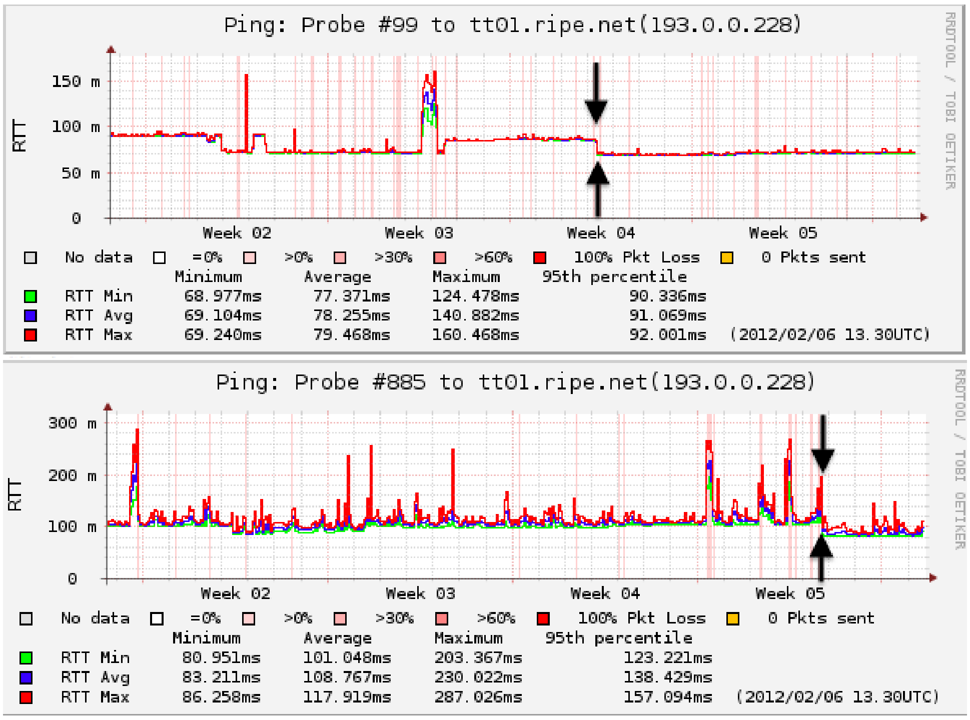


Figure 4.1: RTT measurements from two probes in Tel Aviv to the same destination

Heat Maps

Emile Aben implemented within RIPE NCC a method for representing three-dimensions graphs of the RIPE Atlas measurements data, based on the ”heat map” idea. His method creates series of data from the raw files collected from the Atlas probes containing the timestamp and the minimum RTT (minRTT) value, one time series per probe. This data is then visualized in graph which has the day on the x-axis, the time of the day on the y-axis and the minRTT value represented by a certain color.

For instance, in Figure 4.2, a probe’s RTT measurement to a fixed destination is represented in a ”heat map”. It is easy to observe an RTT decreasing shift around 22 October 2011 as well as some patterns (increased RTT values roughly between 8-10 UTC and 16-18 UTC), which could be attributed for example, to increased data traffic causing link congestion around the same time every day.

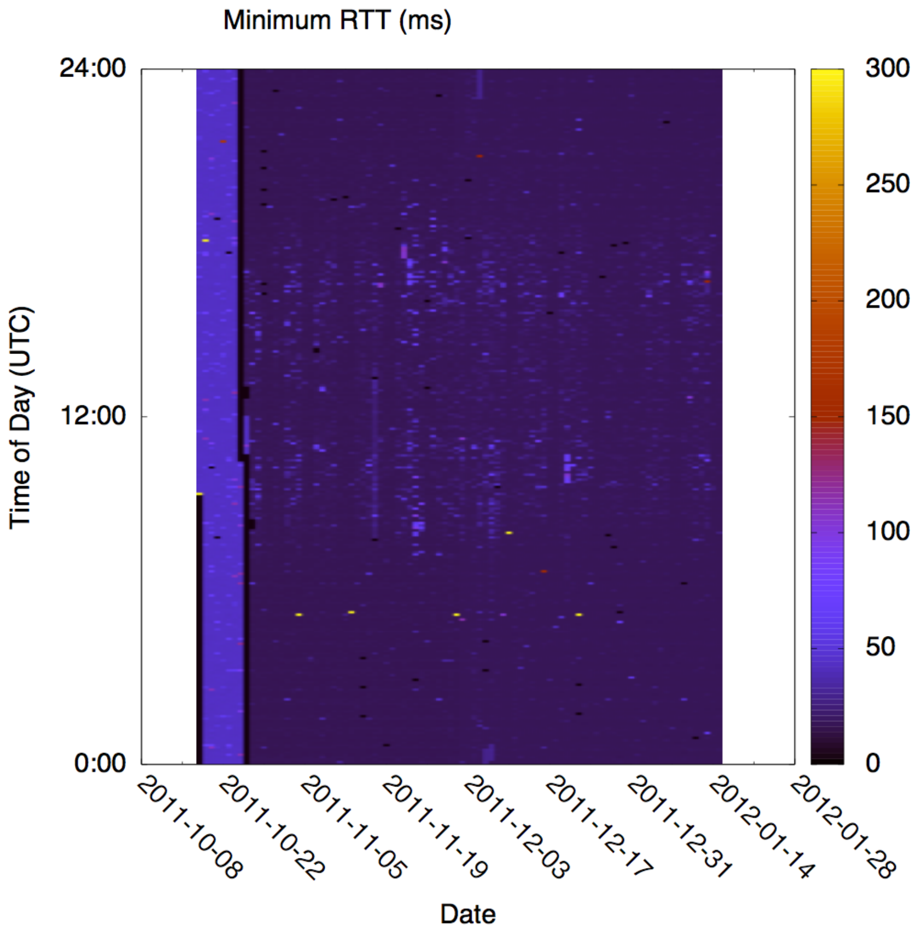


Figure 4.2: Heat map showing patterns and RTT shift

4.3 Conclusions

Ultimately though, none of the events researched was clearly reflected in the graphical representation of the Atlas data. Even the possibly related drop in RTT values for the two probes in Tel Aviv (Figure 4.1) is difficult to label it as a ground truth reflection since there are only two probes in the area. Looking at the traceroute data (future research) could offer more information on what actually happened with these two probes.

In terms of visualization techniques, the RRD graphs proved to be good in showing small changes in the RTT measurements and the ”heat map” graphs excel at observing patterns (for instance, day-night traffic patterns)

The ground-truth search identified the following challenges when identifying real-life events with a reflection in the data collected by the Atlas probes:

→ *Atlas probes are mainly concentrated in the European area*

There is no visibility in the areas where there are no Atlas probes. Visibility increases with the number of probes active in an area affected by the specific event researched

→ *No major network events happened in Europe in the second half of 2011* There weren't any major power outages, the ISP -related problems were limited in the area they affected, the Juniper firmware update bug had limited impact in Europe

→ *European Internet providers do not generally publish network outage history* The research revealed the difficulty of manually selecting the potential events which have a good reflection in the Atlas data

5

Data Analysis

The basic idea behind data analysis is to look for anomalies in the data collected by one of the RIPE Atlas probes, compare the results with the ones obtained from other probes in its network or geographical vicinity and identify potential network events that might have caused these anomalies.

An important requirement for the data analysis is represented by the practical implementation possibilities. RIPE NCC needs a data analysis method which can be later implemented in an algorithm that will sift through the vast amount of data collected by the Atlas probes and identify the ″interesting″ events and, ideally, as close to real time as possible.

5.1 Data representation

In order to analyze this data based on the metric chosen in Chapter 3 (RTT), the necessary information has to be filtered first. Emile Aben's method of creating heat maps actually generates for each probe an univariate time series from the raw data files, containing the timestamp and the minRTT value. The RTT values returned by the *ping* network utility are collected every 4 minutes, while the time series have a granularity of 10 minutes. From the 2 - 3 measurements performed in a 10 minute time interval, the minRTT was selected and introduced as the reference value for that time slot in the time series.

The minRTT was chosen because it displays the smallest sensitivity to random packets having problems, but it has the same sensitivity as the maximum and medium RTT to systematic packet delays or packet loss, which would be indicative of an actual network problem.

In effect, this selection of RTT values means that the raw data is ″smoothed″ by the time series (one selected RTT for every 2 - 3 raw measurements).

The RIPE Atlas data can then be represented as an univariate time series[3] of the form $(X_0, X_1, \ldots, X_t)$, with $t \in T_0$, where:

(1). X_t represents the data measurement taken at specific time t

(2). the set T_0 is a discrete set, representing the set of times at which measurements are conducted

Intial idea

The first incarnation of the basic idea formulated above had the following structure:

(1). generate the univariate time series, one per probe

(2). select the probes in the same area (for example, in the same AS)

(3). Calculate the correlation between this multiple time series and determine whether there is a cross-correlation between the time series or not (based on the value of the correlation coefficient).

The cross-correlation between multiple time series was however a short-lived research idea. Aside from the mathematical complexity associated to calculating the cross-correlation of multiple time series, the time series generated by the Atlas probes contain a lot of noise, and, in some cases, lots of null values (the times when for instance, a probe was disconnected), thus opening the way for a debate over the meaningfulness of the result. Furthermore, if a correlation was to be found, the research would not pinpoint where in time to look for events.

What was needed was a way of separating the normal fluctuations in RTT values from the meaningful deviations in RTT values which could be indicative of a network event. This can be achieved by using Control Charts, detailed in Section 5.2.

5.2 Control Charts

The use of control charts begun in the 1920s at Western Electric Company in US where Walter A. Shewhart introduced the first concepts of Statistical Process Control (SPC). The process control chart he proposed was named the Shewhart Control Chart. According to [14], the basic idea in SPC is that a process always stays in a state of statistical control, unless a special event occurs. A state of statistical control exists when certain critical process variables remain close to their target values and do not change perceptibly. The only variation should be marginal everyday fluctuations.

The most commonly used control charts are the Shewhart, Cumulative Sum Control Chart (CUSUM) and Exponentially Weighted Moving Average (EWMA) charts[14].

The Shewhart chart plots a key variable of the process versus time, together with its corresponding control limits. Process deviations which take the values of the key variable outside of its control limits have an ”assignable cause” (Shewhart terminology) and they actually represent shifts or events which need to be investigated. The particularity of the Shewhart chart is the fact it does not have any memory of the process at all - every value on the chart is linked only to the value immediately preceding it. In other words, previous observations do not influence the probability of future values to cross the control limits.

The CUSUM control chart was developed by E.S. Page at the University of Cambridge in the early 1950s. In contrast to the Shewhart chart, the CUSUM chart has ”long” memory - the value of every key variable on the chart depends on all the values preceding it. Not the value of the key variable is plotted on a CUSUM chart, but the sum of differences between the current value and the average value of the key variable.

The EWMA chart plots the weighted moving average value of the key variable, with older observations having exponentially decreasing weights.

In the case of RIPE Atlas measurements, the process' duration can be any arbitrary number of minRTT measurements. For this research project, the usual number of measurements was approximatively 3000. It is obvious that the times in which the process was ”out of control”, meaning that the CUSUM or EWMA values were outside the control limits are likely to be the ones in which network events occurred.

The Shewhart control chart does not separate the noise from the meaningful events, having no memory. Therefore the control charts used in this research are the CUSUM and the EWMA charts. These have been used for similar measurements before:

- in [7], the authors use the EWMA model for predicting packet loss rates, which is their key variable in Quality of Service (QoS) measurements in telephony applications.
- in [28], the authors use CUSUM charts for change-point monitoring to detect network denial of service (DoS) attacks

The data analysis steps detailed in the following sections are the following:

1. create simple time series, per probe, based on the minRTT
2. create control charts (one per each probe)
3. investigate whether violations of the control limits are shared by multiple probes in one area

Unless otherwise noted, all the figures in this chapter have been generated using R Language and Environment for Statistical Computing[20] and the *qcc* package for statistical control.[24]

5.3 CUSUM Control Chart

For the time series $(X_0, X_1, \ldots, X_t)$, where $t \in T_0$ (with T_0 being the set of times at which measurements are conducted) generated from the minRTT measurements, the univariate two-sided CUSUM scheme uses two cumulative sums: one to detect an increase in mean (positive shift) and another to detect a decrease (negative shift)[19]

$$S_{Ht} = \max\left(0, S_{Ht-1} + (\mu_0 - k)\right) \tag{5.1}$$

$$S_{Lt} = \min\left(0, S_{Lt-1} + (\mu_0 - k)\right) \tag{5.2}$$

where $S_{H0} = S_{L0} = 0$, $\mu_0 = \frac{X_0+X_1+\ldots+X_t}{t}$ is the average minRTT value and k is a reference value (also called allowance) which ”tunes” the CUSUM chart for a specific shift [9]. If the mean of the process starts raising, the CUSUM chart will have an upward slope; on the other hand, when for a set of observations, the mean is lower than the total average, the chart will have a downward slope.

If h is a fixed value, representing the upper value of the control limit, and if we consider for example the positive shift CUSUM formula 5.1, with $S_{Ht} = S_t$, it is suggested[17] that the process is out-of -control when,

$$S_t - \min_{0 \leq i \leq t} S_i \geq h \tag{5.3}$$

Choosing both the k and the h requires a fine-tuning process which takes time to determine optimum values.

The value of h is determined by the amount of false-positive events - its value has to be set such as the number of false-positives is kept to a minimum and the number of events detected is maximized. In the experiments conducted in this research, the value $h = 5\sigma$ was used, where σ is the standard error or the time series.

Choosing the value of k is dependent on the detection speed of mean deviations in the CUSUM chart. As shown in [9], the shift value k should be large enough to have a meaningful impact on the process operation but small enough not to be obvious to the naked eye. The trade-off is that a scheme which is optimal for detecting a shit of three standard deviations may not be so good in detecting a shift of only one standard deviation. During the experiments conducted with the Atlas probe measurements, we chose the value $k = 3\sigma$ for the clearest graphical representation of the data analyzed. For instance, Table 5.1 shows the number of points beyond control limits for the same probe's 3000 measurements with different k and h values. As expected, the number of points outside the control areas increases as the value of k and h decrease.

	h					
k	2 σ	3 σ	4 σ	5 σ	7 σ	10 σ
1 σ	141	136	129	124	116	105
2 σ	72	69	66	64	60	54
3 σ	48	45	44	43	41	37
4 σ	35	34	33	32	30	27
5 σ	28	27	27	25	24	21

Table 5.1: Number of points beyond CUSUM control limits

One particularity of the time series generated from the RIPE Atlas probe measurements is that some sets have many null values, thus obtaining intermittent time series. Taking the values out would have skewed the time scale so the goal was to replace them with a neutral value which would not cause any slopes in the control charts. The solution was to replace each null value with the average value of the time series, μ_0. In this way, the S_t value calculated during null values is constant , not affecting the control charts.

Figure 5.1 shows a CUSUM chart for one of the Atlas probes, where the shift detection reference value is $k = 3\sigma$ and the control points, called the lower decision limit (LDB) and the upper decision limit (UDB) are set at 5σ .

5.4 EWMA Control Chart

Like the CUSUM control chart, the EWMA takes into account all the previous measurements. Unlike CUSUM, which puts equal weight on all the past measurements, EWMA's weight attached to measurements is exponentially declining as the data is older.

Considering again the time series $(X_0, X_1, \ldots, X_t)$, where $t \in T_0$ (with T_0 being the set of times at which measurements are conducted) generated from the minRTT measurements, the EWMA is calculated using the following formula:

$$W_t = \lambda X_t + (1 - \lambda) W_{t-1} \tag{5.4}$$

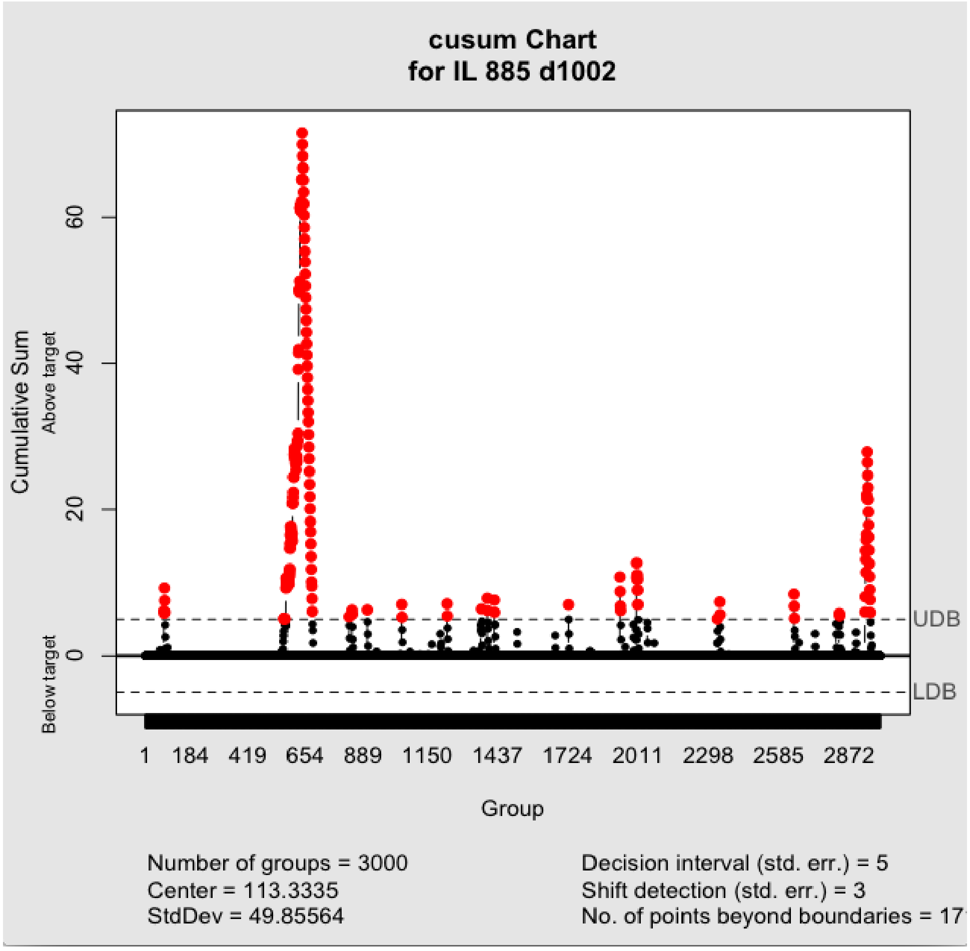


Figure 5.1: Example of a CUSUM chart associated to a RIPE Atlas probe

where $W_0 = \mu_0$ and λ is a constant with $\lambda \in \{0, 1\}$. A low value of λ (close to 0) corresponds to a long memory of the process and a high value of λ corresponds to a short memory of the process [14]. Therefore λ represents a ”smoothing value” in EWMA charts. In the extreme cases where $\lambda = 1$ the chart becomes a Shewhart chart and where $\lambda = 0$ it becomes a CUSUM chart. Therefore, the EWMA represents the middle ground between the zero-memory Shewhart chart and the long memory CUSUM chart.

Figure 5.2 shows the example EWMA chart for the same Atlas probe used in Figure 5.1 to exemplify the CUSUM control chart, with the smoothing constant $\lambda = 0.2$ and the lower control limit (LCL) and the upper control limit (UCL) set at 3σ.

It is notable that the CUSUM and EWMA control charts for the same probe and the same time period display visually matching control point violations, meaning that the CUSUM and EWMA values go beyond the upper limits in approximatively the same points. Obviously, the EWMA chart will have a lower *total* number of violation points for the simple reason that the past events are weighted exponentially less that the recent ones.

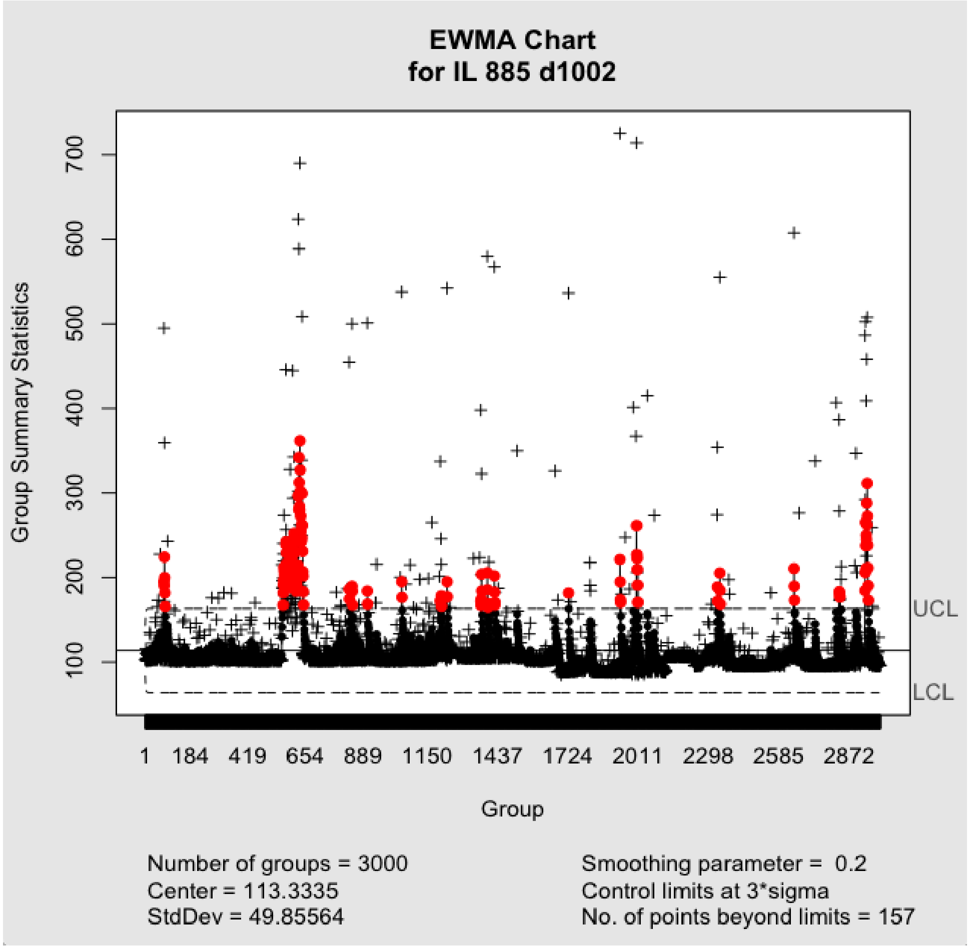


Figure 5.2: Example of a EWMA chart associated to a RIPE Atlas probe

5.5 Aggregated Control Charts

The CUSUM or EWMA control charts help identify the times when the process (measurement results) start deviating form the mean, thus crossing the control points. But, as shown in section 5.2, there is a need to investigate whether violations of the control limits are shared by multiple probes in one area.

To achieve this goal, one solution, for instance, is to aggregate the time series in the same area. Let n be the total number of probes in the area, with $X_{i1}, X_{i2}, \cdots, X_{it}, t \in T_0$ representing the time series corresponding to t measurements X (minRTT) conducted by the probe i. Then we can build the matrix:

$$\begin{bmatrix} X_{11} & X_{12} & \cdots & X_{1t} \\ X_{21} & X_{22} & \cdots & X_{2t} \\ \vdots & \vdots & & \vdots \\ X_{n1} & X_{n2} & \cdots & X_{nt} \end{bmatrix} \tag{5.5}$$

Then an aggregate control chart could be built by considering t measurements, $t \in T_0$, each with n samples.

So at any time t, the measurement X has n samples, of the form $\{X_{1t}, X_{2t}, \cdots, X_{nt}\}$, with each of the samples in the same measurement coming from a different probe.

In this case, the μ_0 value has the form:

$$\mu_0 = \frac{m_0 + m_1 + \ldots + m_t}{t}$$

with

$$m_i = \frac{1}{t}\sum_{k=1}^{t} X_{ik}, t \in T_0$$

Similarly, the EWMA equation (5.4) will become:

$$W_t = \lambda M_t + (1 - \lambda)W_{t-1}$$

with

$$M_i = \frac{1}{t}\sum_{k=1}^{t} X_{ik}, t \in T_0$$

Figures 5.3 and 5.4 show the aggregated CUSUM and EWMA charts for the same country. The figures can be compared with CUSUM (5.1) and EWMA(5.2) charts for a single probe within the same country. The violations points occur approximatively at the same times, but their number is different, depending on how many probes in the area simultaneously display anomalies at that specific time.

5.6 Aggregation of individual control charts

It can be argued that in the control charts aggregation model from Section 5.5, if some probes have average RTT values very different from the rest, then these probes' variations from the mean could influence the aggregation control charts too much. Therefore, it can be stated that that specific aggregation model is entirely valid only if RTT values are within a close range.

To overcome this limitation, a simple idea was used: instead of constructing CUSUM and EWMA charts based on vectors of measurements (the matrix (5.5)), we could plot, for example, the number of probes in an AS (in percentage points) which, at a time t_i, are crossing the control limits boundaries.

Let n be the number of probes in a specific AS and the $\{X_{i1}, X_{i2}, \cdots, X_{it}\}, t \in T_0$ represents the time series corresponding to the number t of measurements X (minRTT) conducted by the probe i. If we calculate, for example, the positive shift CUSUM values for the measurements of this probe, and taking into account the equation (5.3) which determines whether the CUSUM value S_t is outside the control limit at the moment t, we can create for each probe i the set C_i containing t elements:

$$C_{it} = \begin{cases} 0 & \text{if} \quad S_t - \min\limits_{0 \le i \le t} S_i < h \\ 1 & \text{if} \quad S_t - \min\limits_{0 \le i \le t} S_i \ge h \end{cases} \tag{5.6}$$

The equation (5.6) creates sets of elements which have the value 1 when the CUSUM value is outside the control limit and 0 for the rest of the time.

By adding the elements in all the sets from one specific AS results a new set A with the elements:

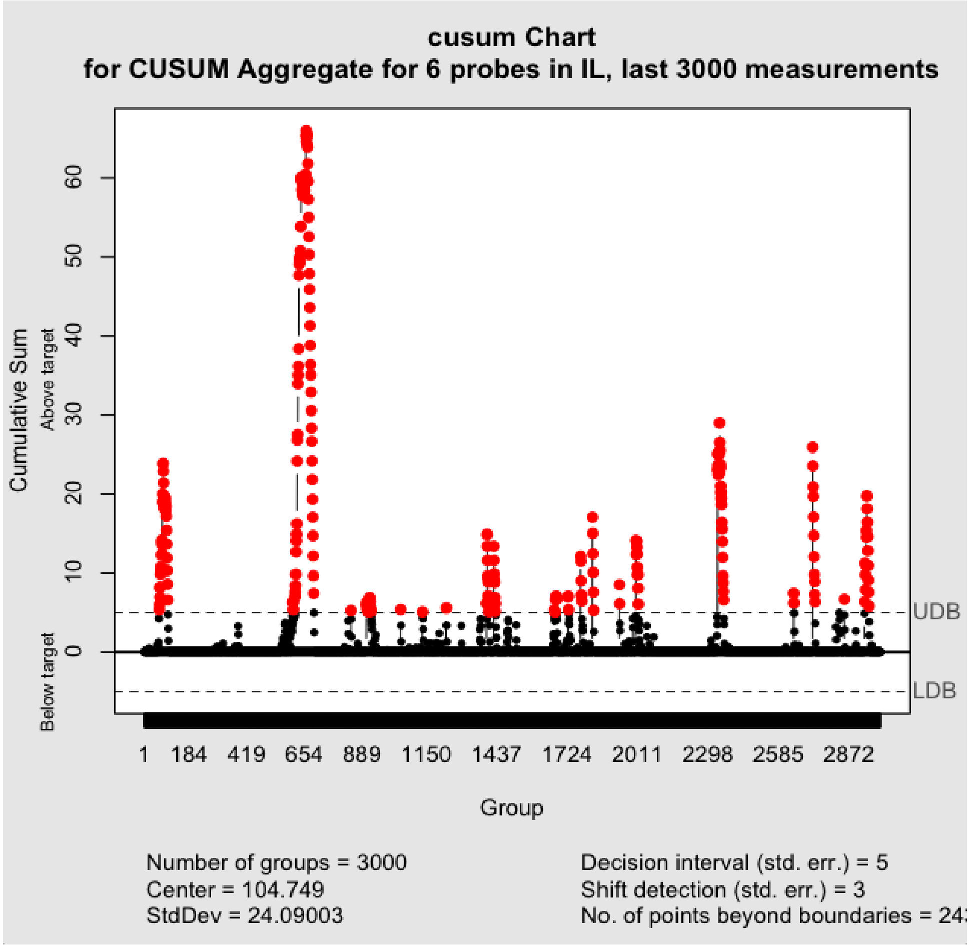


Figure 5.3: An aggregate CUSUM chart for one area

$$A_t = \sum_{k=1}^{n} C_{ik}, t \in T_0 \tag{5.7}$$

The elements of the set A will therefore contain, for each time t, the absolute number of probes whose CUSUM value is outside the control limits.

But plotting absolute numbers does not give sufficient information on the scale of a potential event, therefore these numbers have to be transformed into percentage points, relative to the total number of probes in the AS. So, the set A_p will be created, containing the relative values of the elements of A:

$$A_{pt} = \frac{A_t}{n} \times 100, t \in T_0 \tag{5.8}$$

Figure 5.5 shows an example of a plot[30] for A_p for one AS, which was plotted by aggregating individual CUSUM charts. It shows the percent of probes in one AS, which, at a certain time t, are outside the control limits. As with any CUSUM chart, the beginning and the end values are 0. Almost constantly there are 40 - 60% of the probes outside of the control limits, which could mean that either there is still a lot of noise in the collected data, or simply there are too many false positives (and the values of k and h could be adjusted accordingly). Neverthe-

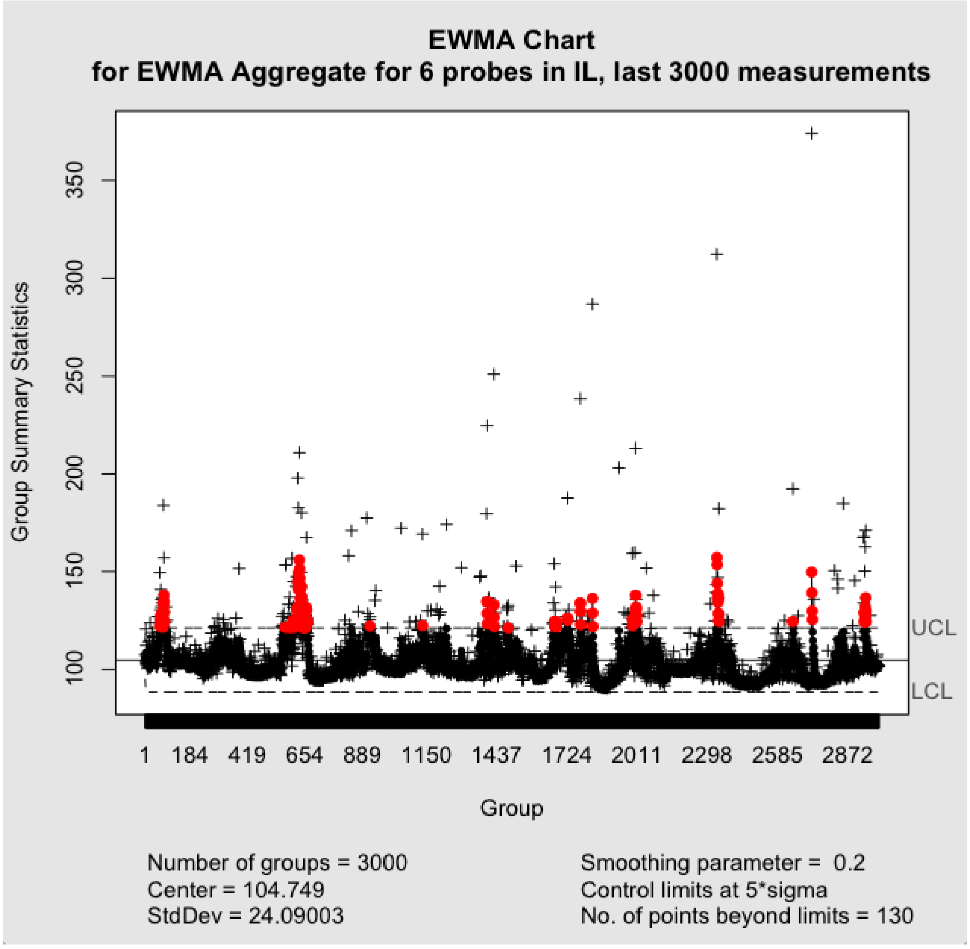


Figure 5.4: An aggregate EWMA chart for one area

less, at around time index 3000, almost 80% of the probes in the AS are outside of the control zone, so this is certainly one time index worth investigating for network anomalies.

Obviously, the exact same procedure can be applied to aggregate individual EWMA charts.

5.7 Conclusions

In the data analysis chapter two control charts were used for plotting the same RIPE Atlas measurement data. The reason is twofold:

- first of all, CUSUM and EWMA do not have the same suitability when it comes to practical implementations of their algorithms. For instance, EWMA, with its exponentially decreasing weight put on old measurements can be better suited for more close-to-real-time data analysis than CUSUM. On the other hand, in the experiments conducted using R, CUSUM was much faster to compute than EWMA.
- secondly, and perhaps, an even more important reason is that it good to have two models for analyzing the data which can help cross-verify the validity of the results.

Similarly, two different ways of aggregating the results were offered. They have different algorithms, and this means that the practical implementation can favor one over another, but,

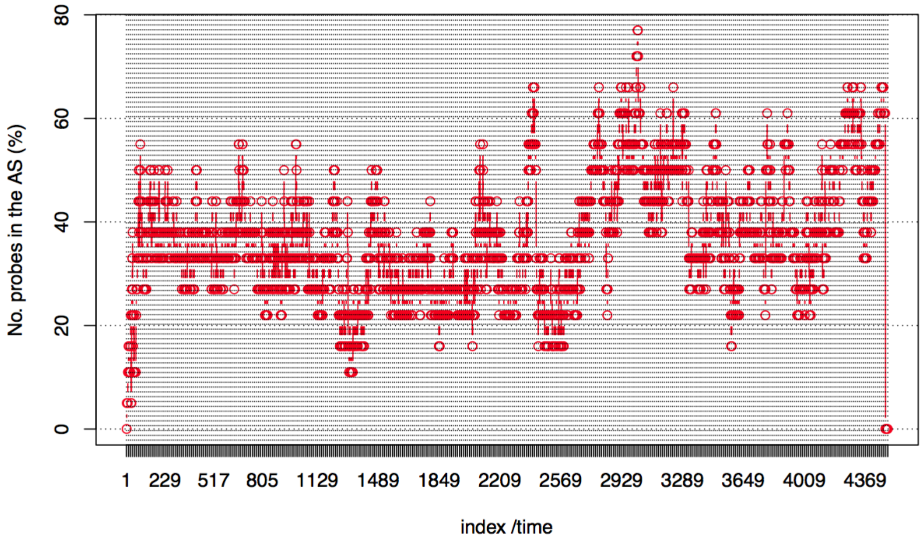


Figure 5.5: Aggregation of individual control charts for one AS

more importantly, they can be used to verify the consistency of the data analysis results.

6

Final conclusions and recommendations

The data analysis reveals through the use of control charts the points in time where it is likely to have an event in the network. However, to validate the results, these should be verified against ground truth events.

As was shown in the ground truth conclusions in Section 4.3, unfortunately, none of the real-life events researched was clearly reflected in the RIPE Atlas data.

But this does not reduce the importance of data analysis. As shown previously, ground truth reflection in the RIPE Atlas data is dependent on the density of probes and on dependable, systematic gathering of information regarding network outages.

The RIPE Atlas network is continuously expanding and such the density of the probes in every AS in the RIPE service region will increase, and this means that there is a stringent need for better information knowledge building. For instance, as most ISPs publish online at least a dashboard with the current status of their network, it should be possible to automatically fetch this information and add it into a network outages knowledge database. The ISPs announce all the events which affect their networks, and this include causes which are outside their control area, such as power outages, flooding or fiber cuts. This makes an even more compelling reason to build such a database with ground truth events.

As for the choice between CUSUM and EWMA, or between aggregated control chart vs. aggregation of individual control charts, as explained in Section 5.7, it is a matter of practical implementation suitability and if computationally possible, calculating both is a good way of cross-checking the data analysis results.

Finally, these data analysis methods are obviously not the only ones possible, and perhaps there are others better suited for certain scenarios. The ones presented in this report should at least provide some pointers in the right direction and hopefully provide a new insight in the data collected by the RIPE Atlas probes.

Bibliography

[1] IT News Africa. *Fiber cable cut in Egypt*. 2011. URL: http://www.itnewsafrica.com/2011/08/fiber-cable-cut-in-egypt.

[2] Project BISmark. *Project BISmark website*. Jan. 2012. URL: http://projectbismark.net/.

[3] Peter J Brockwell and Richard A Davis. *Time series: theory and methods*. New York, NY, USA: Springer-Verlag New York, Inc., 1986. ISBN: 0-387-96406-1.

[4] Kimberly Claffy, George C. Polyzos, and Hans werner Braun. "Measurement Considerations for Assessing Unidirectional Latencies". In: *Internetworking: Research and Experience* 4 (1993), pp. 121–132.

[5] A. Dainotti et al. "Analysis of Country-wide Internet Outages Caused by Censorship". In: *Internet Measurement Conference (IMC)*. Berlin, Germany: ACM, 2011, pp. 1–18.

[6] A. Dainotti et al. "Extracting benefit from harm: using malware pollution to analyze the impact of political and geophysical events on the Internet". In: *ACM SIGCOMM Computer Communication Review (CCR)* 1 (2012), pp. 31–39.

[7] E. Gregori. *Networking 2002: networking technologies, services, and protocols, performance of computer and communication networks, mobile and wireless communications : Second International IFIP-TC6 Networking Conference, Pisa, Italy, May 19-24, 2002 : proceedings*. Lecture notes in computer science. Springer, 2002. ISBN: 9783540437093.

[8] Dinan Gunawardena, Peter Key, and Laurent Massoulié. "Network Characteristics: Modelling, Measurements and Admission Control". In: *in Proc. Int'l Workshop on Quality of Service (IWQoS*. 2003.

[9] D.M. Hawkins and D.H. Olwell. *Cumulative sum charts and charting for quality improvement*. Statistics for engineering and physical science. Springer, 1998. ISBN: 9780387983653.

[10] B. Huffaker et al. "Topology discovery by active probing". In: *Symposium on Applications and the Internet (SAINT)*. Nara, Japan: SAINT, 2002, pp. 90–96.

[11] The Cooperative Association for Internet Data Analysis. *Archipelago Measurement Infrastructure*. Jan. 2012. URL: http://www.caida.org/projects/ark/.

[12] Daniel Karrenberg. *RIPE Labs website*. Jan. 2012. URL: https://labs.ripe.net/Members/dfk/active-measurements-sponsorship.

[13] Neelie Kroes. *European Commission Blogs website*. Jan. 2012. URL: http://blogs.ec.europa.eu/neelie-kroes/how-fast-is-your-broadband/.

[14] *Multi- and megavariate data analysis: Basic principles and applications*. v. 1. Umetrics AB, 2006. ISBN: 9789197373029.

[15] RIPE NCC. *RIPE NCC website*. Jan. 2012. URL: http://www.ripe.net/lir-services/ncc.

[16] RIPE NCC. *RIPE NCC website*. Jan. 2012. URL: http://www.ripe.net/data-tools/projects/faqs/test-traffic-measurements.

[17] E. S. Page. "Continuous Inspection Schemes". In: (1954).

[18] The Manila Paper. *Globe Telecom Fiber Optic Network Damaged by Typhoon Bebeng*. May 2011. URL: http://manila-paper.net/globe-telecom-fiber-optic-network-damaged-by-typhoon-bebeng/1140.

[19] H. Pham. *Springer handbook of engineering statistics*. Springer, 2006. ISBN: 9781852338060.

[20] R Development Core Team. *R: A Language and Environment for Statistical Computing*. ISBN 3-900051-07-0. R Foundation for Statistical Computing. Vienna, Austria, 2011. URL: http://www.R-project.org/.

[21] Imperial Republican. *Great Plains Internet service down Monday due to fiber cut*. Oct. 2011. URL: http://www.imperialrepublican.com/index.php?option=com_content&amp;view=article&amp;id=3358:great-plains-internet-service-down-monday-due-to-fiber-cut.

[22] SamKnows. *SamKnows Methodology White Paper*. Jan. 2012. URL: http://www.samknows.com/broadband/methodology.

[23] SamKnows. *SamKnows website*. Jan. 2012. URL: http://www.samknows.com/broadband/regulators.

[24] Luca Scrucca. "qcc: an R package for quality control charting and statistical process control". In: *R News* 4/1 (2004), pp. 11–17. URL: http://CRAN.R-project.org/doc/Rnews/.

[25] TechSpot. *National broadband outage caused by router bug*. Nov. 2011. URL: http://www.techspot.com/news/46163-national-broadband-outage-caused-by-router-bug.html.

[26] University of Tel Aviv. *The DIMES Project*. Jan. 2012. URL: http://www.netdimes.org/.

[27] Yolanda Tsang et al. "Network radar: tomography from round trip time measurements". In: *Proceedings of the 4th ACM SIGCOMM conference on Internet measurement*. IMC '04. 2004, pp. 175–180.

[28] Haining Wang, Danlu Zhang, and Kang G. Shin. "Change-Point Monitoring for Detection of DoS Attacks". In: *IEEE Transactions on Dependable and Secure Computing* 1 (2004), p. 2004.

[29] University of Washington. *iPlane: An Information Plane for Distributed Services*. Jan. 2012. URL: http://iplane.cs.washington.edu/.

[30] P. Wessa. *Free Statistics and Forecasting Software*. 2007.