Community Network Quality Of Service Monitoring System

Clayton Sibanda

Department of Computer Science
University of Cape Town
South Africa

April 2019

Abstract

Characterising the internet through measurements has become very important to both end users and network managers. Most end users want to know what is causing their network based applications to slow down or take too long to respond. On the other hand network managers want to troubleshoot and detect faulty nodes in a network.

The rise of cybersecurity has also made it mandatory for networks to be monitored constantly with tools that can detect anomalous behaviour in a timely manner before the network gets compromised.

This paper investigates the use of different measurement tools in different networks with the main focus being community based networks. The main goal is to study how network measurement tools can be used in community based networks to analyse the Quality of Service(QoS) in the network.

In the past there has not been many network measurement tools deployed in community based networks. Most prominent tools have been deployed in large corporate networks that are rich in resources and bandwidth. This makes it very difficult to estimate the Quality of Service of community based networks and in turn the Quality of Experience(QoE) of the end users which is partly influenced by the QoS.

This paper also looks at the challenges involved in carrying out research in a community based networks.

Most network measurement tools collect data that is to be processed and analysed. Different data analysis and visualisation tools and platforms are studied in depth.

Keywords Data Driven Networking, network measurement tool, Quality of Service, Quality of Experience, visualisation, network traffic

1. Introduction

Internet measurement tools have become equally important to end-users as it is to network managers. Managers and end-users both have different use cases for the measurement tools [7].

For managers and regulators network measurement tools provide a different view of the internet e.g routing, topology, addressing and naming, security, dataplane performance or impairment and traffic matrices [Ford et al 2015]. In some cases network measurement tools are used to detect anomalous behaviour in the network which could be caused by cyber attacks on the network. With measurement tools, cyber attacks and other unusual behaviour can easily be detected and be attended to without any delay. For network regulators, measurement tools also simplify and make troubleshooting a trivial job.

Measurement platforms are also identified as providing the engineering to bridge the gap between practice and research in terms of representation producing universally applicable results and allowing measurement to scale. Internet Service Providers(ISPs) don't only use internet measurement tools to fix problems in its access network, but also to evaluate the Quality of Service(QoS) experienced by its users [2]. Consumers use such measurements to confirm whether the ISP is living up to its Service-Level Agreement(SLA) offers. Another possible use of these measurement tools by the user in a community network is to diagnose network problems in the local network.

For some users network measurement tools like perfSONAR, empower them with the ability to have performance visibility of their network-based applications.

2. Challenges with newtwork measurement tools

Internet measurement tools come with their own challenges both minor and big ones. The first concern is that of cyber security risks that could be brought into the

network through the use of internet measurement softwares. Some network providers fear that if they allow a alien software to crawl their servers, it would collect data that is sensitive causing a confidentiality and privacy breach. In some cases also, the fear is that some network measurement tools will expose the system to a lot of malicious softwares.

When it comes to perfSONAR for example, the main question asked about the tool was if it will pass the integrity scans or was it going to make a network more vulnerable to cyber attacks?[3].

The coming of new paradigms like software defined networking to aid in traffic analysis and data measurements brings about new challenges for current measurement tools.

Mobile based tools like LiveLab also pose a privacy challenge in that the user needs to know what kind of information the tool will collect and when will it do so.

3. research challenges in community networks

Community networks are IP-based networks that are built, operated and owned by communities of citizens. These networks are normally ran by non-profit organisation working together with local stakeholders. To describe community in technical terms one would say they are large-scale, decentralised and distributed systems with many nodes, links and services. Community networks are diverse in that they are built as a mixture of both wireless and wired links. As a result different routing systems and protocols are used.

Such networks introduce different challenges for researchers due to their dynamic and decentalised structure. Some of the challenges in are unique to community networks and some are similar to those in coorperate networks.

The first challenge is brought about by the extensive use of wireless links. Wireless links have proven to be very challenging to set up in a community network when there are not enough wired links to support the network. There is therefore a need for MAC protocols to be optimised or changed for the network to operate.

Network neutrality and openness are also great challenges to normal routing protocols and how it is implemented in low cost devices(the nodes). Neutrality and openness of the network also raise cyber security challenges for users in that the users are not guaranteed privacy when using the network[5].

Most community networks have limited capaicty of servers and links. This causes most application that are bandwidth demanding like file sharing and VOIP to experience intermittent connections often in the network.

The diversity in community networks also makes it hard to standardise them. Hence creattive ways to interact with the network are needed.

3.1 Prominent network measurement tools and platforms

There are number of network measurement software that currently deployed in different networks to monitor and observe different patterns in the network. The first one that we discuss is perfSONAR. perfSONARis a multi-domain network performance measurement and monitoring software tool. It empowers the ability of users to have performance visibility of their network-based applications[3]. It also eases the operational burden on distributed cyberinfrastructure supporting data-intensive scientific activities[3].

LiveLab is a method used to measure smartphone users in the field and wireless networks with smartphone users[16]. It makes use of a tool that is built for Iphone users only. It was one of the few tools that is implemented on an Iphone to take network measurements. LiveLab provides a comprehensive in-device logging of smartphone usage and measurement of wireless networks[16]. The tool takes advantage of the mobility of smartphone users and the ability of the smartphone to switch connections between different routers. Since the LiveLab tool is based on Iphone, there is need to "jailbreak" the Iphone in order to access some hardware functionalities that provide network performance of the phone[16].

RIPE ATLAS is also another tool used extensively to measure network performance. It uses thousands of distributed probes and anchors as measurement devices. The tool can perform IPv4 and IPv6 traceroute, ping, DNS, NTP[2].

PlanetLab is a measurement platform used for testing of new network services. However PlanetLab is rather unusable due to unpredictable load issues and tendency of nodes to be located in a national research network[2].

PeerMetric is a measurement tool used to measure P2P network performance experienced by broadband hosts[2].

Mobiperf is an android based application that is used to collect mobile network measurements. On the backend it uses a data collection server to collect and aggregate data. The app periodically checks in with the measurement server which sends it a list of measurement tasks to perform. These measurement tasks include ping, traceroute, HTTP GET, DNS lookup, TCP Throughput, IPv4/v6 compatibility check and UDP Burst. Each task is given a respective set of measurement parameters.

Netradar is one of the most famouse tools used by app developers and business owners to monitor user experience based on region and connectivity around the world. It also enables developers to understand the mobile and Wi-Fi connection quality and speeds across the world. This enables developers to develop apps that are customised to specific region.

M-Lab is a tool that empowers users to test the speed of their internet connection. The tool only performs active measurement, meaning that it only runs when a user has prompted it to do so. The results from the tool come in the form of upload speed, download speed and latency.

The last tool to be discussed here is mPlane, which is a measurement platform that uses an error-tolerant RPC protocol connecting clients with componetns to cooperatively perform network measurements and anlysis using heterogeneous tools[2].

3.2 Use of network measurement tools in community-based networks

The way in which community networks are constructed is such that they are not standardised. They are built using limited resources and financial backing. As a result this makes it complicated to implement and install a measurement tool in the network.

3.3 Measuring network performance using smart phones

Most community networks consist of wireless links more than wired links. As a result the most dominant way of accessing the network in a community network is through smart phones.

Smart phones allow users to access the network from multiple wireless access points at different times of the day due to their mobility. Thus by logging the observed network activities together with time and location, a user can contribute to the number of measurements everyday[3].

The measurements collected from a user over time can be put together into a personal network map[6]. This can give users insight on the type of content they are accessing mostly on the network and also how the network generally performs on their device.

Network measurements from multiple users can be aggregated to produce a more complete network coverage map for the whole community network. The produced network map will be valuable for both users and network managers [3]. For mobile users, a detailed coverage map that provides the performance of local networks at a given location and time can help the client a great deal[16].

Netalyzr is a tool that communicates with a farm of measurement servers to probe key network performance and diagnostic parameters of the broadband user. The tool can detect outbound port filters, hidden Hypertext Transfer Protocol (HTTP) caches, Domain Name System (DNS) and NAT behaviours, path Maximum Transmission Unit (MTU),bufferbloat issues and IPv6 support[2].

For network operators a detailed coverage map could help detect blind spots in the networks and help with continuous network deployment and capacity growth[16].

The measurement method outlined above describes a user-collaborative approach to network measurement. This method is better than most existing measurement methods.

Existing network-based methods measure and produce a map for a particular network, and hence are unable to help devices find the best available network. While existing client-based methods depend on wardriving which is expensive and is unlikely to capture detailed features in a geographic coverage. The usage of smart phones for measuring networks provides tailored information regarding both mobile users and the networks[16].

4. Data driven networking

The coming of networking to computers improves the way in which data is transferred and handled between computers. Through having a network of computers, data is made available to the multitudes at any time and anywhere.

In simple terms one would say networking has completely changed the way data is handled and manipulated. The results and patterns observed in the data can then be used to improve the system from which it was collected from.

In networking the question to asked is whether data can also be used improve the way networking is done[11]. Or can we significantly achieve better performance in a network by collecting a lot of data[11].

Most networked applications require methods to respond to changing network conditions. Traditionally, these methods have relied on manually designed strategies. One example would be TCP that relies on multiple human-selected constants.

Solving such challenges requires us to rethink the design of traditional networking protocols or come with entirely new strategies[11]. One possible paradigm to be used to tackle these challenges is Data Driven Networking(DDN). DDN is inspired by computing ability

to collect data and extact insights from large volumes of data. DDN makes use of data co

To define DDN one would say it is a methodology for designing the control plane of network protocols [11]. It consists of two components: client side instrumentation and DDN controller. The earlier is used to measure quality observed by the client and apply decisions made by DDN and DDN controller is used run loosely couple steps which involve collecting and analysing the data collected by the client side instrumentation[11].

DDN is a very promising paradigm for new ways of designing network protocols. However it also comes with both solutions and challenges. DDN raises challenges both on the algorithmic side and the architectural front[3]. When it comes to architecture the main problem faced is that of scalability. DDN controller can become a single point of failure in logically centralized architecture. This makes it possible for clients to launch a denial of service attack on the DDN backend by sending multiple control requests or quality updates [3].

Since DDN relies on data to make decisions, it may also suffer algorithmic bias.This is because the input measurement data is based on past set of best decisions, we wont have a proper method to estimate the quality of improvements of upcoming decisions in the future[12]. A potential solution would be to use a specific percentage of sessions to investigate multiple decisions and this could get rid of the prediction bias[12].

4.1 Uses cases Data Driven Networking

Data driven networking has been tested in different applications and industries. In video on demand services like YouTube where they have the ability to stream data from multiple servers or CDNs, it was shown that data-driven approach could improve video quality(e.g., 50% less buffering time)[12, 8] . Similarly the quality of live streaming from live streaming service like twitch also improve due to data-driven methods[12].

In internet telephony, prior work has shown that compared to Anycast-base relay selection, a data-driven relay selection algorithm is superior in reducing the number of poor calls by a significant amount[12].

Data-driven networking can also be used in file sharing services like Dropbox to improve quality of experince for clients.In social networking platforms data-driven networking was observed to reduce the query time by 50%[12].

4.2 Quality Of Experience

The information technology industry spends a lot of money and time trying to improve user experience and the quality of service delivered to the user. The internet is an economy that is driven by the number of eyes that look at different webpages and on-demand content. Its backbone are applications like internet video streaming, internet telephony and social networking websites. All of these services depend on the user's usage of the service to generate income. This makes it very important for application providers to maximise Quality Of Experience(QoE) in order to maintain high user engagement.

Quality of Experience has been defined as the total acceptability of an application service, as perceived by the end-user[14]. Recent research has shown time spent watching videos online can drop by 39% due to a short video buffering on YouTube[10]. This has knock on effect on revenues of these services.

The importance of QoE has led to an enormous amount of research and talks around the world on how to optimise the QoE for end-users. However there is still a disparity between the expected QoE and what the end user experiences on the internet[10].

The purpose of QoE evaluation is split into two: to track online user experience and fully justify service based on the QoE.

4.3 Quality of Service

Quality of Service(QoS) is concerned about the network delivery capacity and resource availability to users. In other words one would say QoS is about fast internet access for the user and low latency. However there are many non-uniform views about QoS by different stakeholders. Some say QoS refers to the ability of the network to offer packet transfer in a faster way[13]. At the same time other organisations have maintain that QoS has to do with service quality for the user. These two different views raise questions of how network-level QoS measurements and control relate to the user perception of a service[5].

The two main QoS parameters are network latency and delivery speed(bandwidth)[5]. As a result QoS is considered poor if any of them is affected from their normal position i.e if bandwidth is low or if latency is high.

4.4 Quality of Service and Quality of Experience

Even though there is a big difference between QoS and QoE, there is traditional assumption that measured QoS is related to the QoE for the end-user[6]. The internet industry spends a lot of money to offer more networking resources to users so as to improve their experience with the service. On the contrary, the relationship between services and users satisfaction cannot be determined inn a trivial manner[6].

Its not clear how much of the user's experience is improved by improvements in delivery bandwidth or lower latency. This is because QoE has to do with the level of user satisfaction not the amount of resources made available to the user.

4.5 Relationship between QoE and latency

Latency refers to any type of delay that occurs when transferring data over a network. Networks where small delays happen are termed low-latency networks and those where there is a significant delay are called high latency networks. Ideally, one would want a network connection with zero or low latency so that communication between end point devices is not delayed.

To reduce latency in network connections, more resources are added to the network. By so doing, we are improving the QoS but there is no guarantee that the QoE will improve based on improved latency. However a very high levels of latency lead to poor user-experience hence bringing down the QoE.

To measure the relationship between QoE and latency, response time is normally used. This time is a composition of the network latency and server processing time[6]. Normally the latency between the end-user host to the ISP network is difficult to measure. However due to the similarity in end-point equipment and small number of hops to the ISP network the latency is assumed to be negligible. From data it was observed that over 95% of the requests had response time less than or equal to 500mSec and over 40% had response time less than or equal to 50mSec [6].

4.6 Relationship between QoE and Effective bandwidth

Bandwidth refers to the amount of data that is sent between nodes in a network in a certain amount of time. In a communication network one of the questions often asked is how does the effective bandth of the network affect overall user satisfaction.

By increasing bandwidth we are increasing the speed at which data is delivered to the user or making the connection faster.A faster connection for the means that their requests will be served faster from the server hence less waiting time.

Increasing effective bandwidth from 56kBit/s to 200kBit/s led to a large increase in user satisfaction[4]. However there is not much of a big difference between objects sent over an effective bandwidth of 200kBit/s and those send on an effective band above 200kBit/s [6]. From this analysis, one can conclude that strong network bandwidth is very important for user satisfaction hence it also plays a role on the QoE for the user.

5. visualisation

As more people become connected to the internet large volumes of data are generated everyday from different networks. Most big networks have enormous volumes of data that is difficult to make sense of if not properly organised. Visualisation has become an essential process for capturing activities happening within a network.

When visualisation is done effectively it enables users to gain knowledge into the data information and discovery of activity patterns of network flows[15]. The numeric nature of such information makes it hard for a human beings to perceive patterns and relationships in it. Some of the features that makes such information difficult to fathom to human beings is time, packet size and, inter-packet time.

Many patterns like data structures and discriminations are perceived after visualisation of a higly complicated dataset. As result, visualisation explicitly enlightens audience of the implicit properties and relationships hidden in the data. Data visualisation also makes it easy for researchers and analysts to observe a timeline of events and potential security threats within a single graph without having to manually go through figures[15].

5.1 challenges in visualising data

The endeavour to visualise data in a large network comes with a lot of challenges to analysts. The first challenge is that network datasets normally contain large volumes of data, contents and attributes that IP packets possess could vary from each other in a great way. This makes it hard for tools to observe patterns and collect meaningful data. Another challenge is that the data in networks contains encrypted entries due to security concerns so as to prevent hackers from sniffing the data in the network. However such security precautions end up being blockages for researchers and analysts when exploring network traffic[15].

Also, according to Staheli et al.[17]], novel cyber visualizations observed are limited in integrating with human factor and adaptability. This means that visualisation algorithms to date are either too complex or basic for the targeted users and the absence of human factors in the design results in a gap between graphic representation and human understanding[15].

5.2 visualisation methods

There are many visualisation methods employed by different tools to generate human friendly visualisations. To visualise data in two or less dimensions: line graph, histogram and pie chart are normally used.However,due to the large volume and many properties of large traffic network, new visualisation methods that are can handle data with many dimensions are needed[15].

A number of multi dimensional tools exist for representing data that has more than two dimensions. The first is one is a scatter plot. A scatter plot can help in visualising data with two variables, which is fundamental to the way in which data with many dimensions is displayed.

The second method used is a hyper graph. Hyper graphs are used to reveal the relationship among multiple variables clearly that can be derived from the most item sets[15].

Force graphs are also used to visualise multidimensional data. A force graph represents nodes as dots and links segments to show how a data set is connected[15]. The fundamental idea in a force graphs is a network, thus, relations among data points within a dataset are revealed[1].

The last method to be discussed is the Parallel coordinate which analyses data from the following aspects: obtaining timeline and parallel coordinates[15]. All of these methods have their respective strengths and weaknesses.The analyst has to choose which one to use depending on the data at hand.

5.3 dimensionality reduction

Data from big networks normally contains multiple dimensions. However human beings can only see two dimensions only and they have to use eye movements to appreciate the third one. The limitations of human perception and the requirements of big traffic network data encourage the necessity of robust dimensionality reduction methods before visualisation can be done.

Human vision limitation sets a boundary such that we visualise data in a two dimensions. Since the data from the network always has multiple variables, it is necessary for the algorithm used to select dimension reduction methods that avoid the loss of significant information as much as possible[15].

One of the most famous methods of dimensionality reduction used is principal component analysis(PCA)[13]. PCA implements dimensionality reduction by feature derivation, which allows feature identification and encourages feature combination. By using a matrix to the origin data matrix, transformations like moving and rotating and new coordinate system of the graph are given out[15]. The operation of PCA suggests a specific set of axes that allow the elimination of unnecessary coordinates or the those with little impact to reduce the dimension of the graph[15]. A principal component means a direction that entails the greatest variation. However PCA also has disadvantages, by reducing dimensions some attributes in the dataset could be lost, which may lead to weak analysis results[15].

6. Data analysis

A large amount of data is constantly produced by big networks everyday. In order to detect and observe patterns in this data, we need to clean it and analyse it.

Data analysis allows us to derive a meaning from the data that we collect from the network. Data analysis is normally used to detect anomalies in the network. An anomally defined by M Ahmed etal[1]] as an observation that differs so much from other observations as to raise suspicion that it was generated by a different process.

Anomalies are very crucial because they point out significant but uncommon events that can prompt important actions to be taken in multiple applications[1]]. These anomalies could be a cybersecurity threats or a technical fault in the network.

6.1 using data analysis for cyber security

The are three main methods used for cyber analytics and these are: misuse based, anomaly based and hybrid. Misuse based methods are sometimes called signature based. This is because misuse based methods are designed to identify known attacks through their signatures and they do so without raising a large number of false alarms[4].

However, misuse based methods are unable to detect zero day attacks. This is because they require frequent manual updates of the database and signature so the common attacks or the new attacks.

Anomaly based techniques model the normal network system behaviour, and detect anomalies as deviations from known behaviour. One of the most impressive parts about anomaly based methods is that they can detect zero day attacks. Another advantage is that the profiles of normal behaviour can be customised for each system and network[4]. This makes it very difficult for hackers to know which activities they are able to run without being caught[4]. The data on which anomaly based methods alert, can be used to define patterns for misuse based methods. The main draw back of anomaly based methods is that they have a high potential for false alarm rates[4]. This is because new unseen legitimate system behaviour might be treated as an anomaly.

Hybrid techniques employ both misuse and anomaly detection techniques.They are employed to raise identification rates for known intrusions and decrease the false positive rate for unknown attacks[4].

6.2 using machine learning to classify data

Different machine learning algorithms are used to extract patterns and derive meaningful insights from the collected data. Machine learning is a subset of a larger

field of artificial intelligence. It consists of a number of researches related to large scale data analysis that allows processing systems to learn from data examples to achieve optimisation in system's performance[9].

Supervised and unsupervised learning are some of the fields of machine learning among others. Given a labelled dataset, the task in supervised learning is to learn the relationship between the output and input so that on supplying a new input, the output is predicted accurately. In unsupervised learning however, given an unlabelled dataset, the task is to classify values in the data[9]. Machine learning can be used together with data science to analyse and detect anomalous behaviour in the network.

7. Conclusions

In this paper, literature in related to the use of network tools to characterise the internet using data analysis and visualisation.

Different metrics used to characterise the internet or other major networks were examined and studied. These involve the QoS and the QoE. One being focused mainly on the resources of the network and the later focused on the experience of the end user.

It was observed that the two are related in different ways and that QoS tends to influence QoE to a greater extent in some cases.

A number of prominent network measurement tools which are used in major networks in the world were also found in literature. Their impact in the developing world and in community networks is very minimal. Some of the major measurement tools are: pefSONAR, mobiperf, m-lab, RIPE ATLAS and LiveLab to mention a few.

The reason why some of these tools are not used even in large community networks is because community networks pose a lot of challenges to researchers. One example is that community networks are not standardised compared other bigger private networks.

Community networks are also not very secure to the user since the network is governed by the community. Hence this makes it hard to implement network measurement tool as this might lead to user's data being hacked and compromised.

After collecting data using network measurement tools, the analysis of data is done using different data science and machine learning techniques.

The paper also explored data visualisation and the challenges involved in visualising data from a large network. A number of challenges involve the diversity of packets in a large dataset from a network which makes it hard to derive meaningful patterns in the data. Another barrier to analysts is that some data in the network contains encrypted packets which are meant to protect data in the network.

The data in network also needs to be cleaned before sent to a visualisation tool. The first thing to be done is to reduce the dimensions of data through dimensionality reduction.

In conclusion collection, analysis and visualisation of data in networks allows one to practice data driven networking. Data driven networking involves using data from the past behaviour of the network to influence the future behaviour of the network. In the long run this will improve the QoS of the network and in turn improve the QoE for the user.

References

[1] Ahmed, M., Mahmood, A. N., and Hu, J. A survey of network anomaly detection techniques. *Journal of Network and Computer Applications 60* (2016), 19 – 31.

[2] Bajpai, V., and SchÃűnwÃĎlder, J. A survey on internet performance measurement platforms and related standardization efforts. *IEEE Communications Surveys Tutorials 17*, 3 (thirdquarter 2015), 1313–1341.

[3] Braem, B., Blondia, C., Barz, C., Rogge, H., Freitag, F., Navarro, L., Bonicioli, J., Papathanasiou, S., Escrich, P., Baig Viñas, R., Kaplan, A. L., Neumann, A., Vilata i Balaguer, I., Tatum, B., and Matson, M. A case for research with and on community networks. *SIGCOMM Comput. Commun. Rev. 43*, 3 (July 2013), 68–73.

[4] Buczak, A. L., and Guven, E. A survey of data mining and machine learning methods for cyber security intrusion detection. *IEEE Communications Surveys Tutorials 18*, 2 (Secondquarter 2016), 1153–1176.

[5] Fiedler, M., Hossfeld, T., and Tran-Gia, P. A generic quantitative relationship between quality of experience and quality of service. *IEEE Network 24*, 2 (March 2010), 36–41.

[6] Fiedler, M., Hossfeld, T., and Tran-Gia, P. A generic quantitative relationship between quality of experience and quality of service. *IEEE Network 24* (05 2010).

[7] Ford, M., and Eggert, L. Report on the workshop on research and applications of internet measurements (raim). *ACM SIGCOMM Computer Communication Review 46* (07 2018), 1–4.

[8] Ganjam, A., Jiang, J., Liu, X., Sekar, V., Siddiqi, F., Stoica, I., Zhan, J., and Zhang, H. C3: Internet-scale control plane for video quality optimization. In *Proceedings of the 12th USENIX Conference on Networked Systems Design and Implementation* (Berkeley, CA, USA, 2015), NSDI'15, USENIX Association, pp. 131–144.

[9] Hussain, B., Du, Q., and Ren, P. Semi-supervised learning based big data-driven anomaly detection in

mobile wireless networks. *China Communications 15*, 4 (April 2018), 41–57.

[10] Jiang, J. Enabling data-driven optimization of quality of experience in internet applications.

[11] Jiang, J., Sekar, V., Stoica, I., and Zhang, H. Unleashing the potential of data-driven networking. pp. 110–126.

[12] Jiang, J., Sun, S., Sekar, V., and Zhang, H. Pytheas: Enabling data-driven quality of experience optimization using group-based exploration-exploitation. In *Proceedings of the 14th USENIX Conference on Networked Systems Design and Implementation* (Berkeley, CA, USA, 2017), NSDI'17, USENIX Association, pp. 393–406.

[13] Kaspi, O., Yosipof, A., and Senderowitz, H. Visualization of solar cells libraries space by dimension reduction methods. *Journal of chemical information and modeling* (2018).

[14] Kilkki, K. Quality of experience in communications ecosystem. *J. UCS 14* (01 2008), 615–624.

[15] Ruan, Z., Miao, Y., Pan, L., Xiang, Y., and Zhang, J. Big network traffic data visualization. *Multimedia Tools Appl. 77*, 9 (May 2018), 11459–11487.

[16] Shepard, C., Rahmati, A., Tossell, C., Zhong, L., and Kortum, P. Livelab: Measuring wireless networks and smartphone users in the field. *SIGMETRICS Perform. Eval. Rev. 38*, 3 (Jan. 2011), 15–20.

[17] Staheli, D., Yu, T., Crouser, R. J., Damodaran, S., Nam, K., O'Gwynn, D., McKenna, S., and Harrison, L. Visualization evaluation for cyber security: Trends and future directions. In *Proceedings of the Eleventh Workshop on Visualization for Cyber Security* (New York, NY, USA, 2014), VizSec '14, ACM, pp. 49–56.