Chapter 15

Metrics for Broadband Networks in the Context of the Digital Economies

Salman M. Al-Shehri, Pavel Loskot,
Tolga Numanoğlu and Mehmet Mert

Additional information is available at the end of the chapter

http://dx.doi.org/10.5772/intechopen.72035

Abstract

In a transition to automated digital management of broadband networks, communication service providers must look for new metrics to monitor these networks. Complete metrics frameworks are already emerging whereas majority of the new metrics are being proposed in technical papers. Considering common metrics for broadband networks and related technologies, this chapter offers insights into what metrics are available, and also suggests active areas of research. The broadband networks being a key component of the digital ecosystems are also an enabler to many other digital technologies and services. Reviewing first the metrics for computing systems, websites and digital platforms, the chapter focus then shifts to the most important technical and business metrics which are used for broadband networks. The demand-side and supply-side metrics including the key metrics of broadband speed and broadband availability are touched on. After outlining the broadband metrics which have been standardized and the metrics for measuring Internet traffic, the most commonly used metrics for broadband networks are surveyed in five categories: energy and power metrics, quality of service, quality of experience, security metrics, and robustness and resilience metrics. The chapter concludes with a discussion on machine learning, big data and the associated metrics.

Keywords: digital transformation, metrics, measurements, performance, broadband networks

1. Introduction

The digital transformation of telecommunication industry alone will likely create $2 trillion new business opportunities and values for the industry as well as the society [1]. This transformation is already bringing profound changes to how telecommunication services are delivered and managed along with changes in the corporate organizations and cultures [2]. The digitalization will also require adoption of new policies and regulatory models. Today's hardware components provide sufficient computing and storage enabling to abstract many processes entirely in software. For instance, software-defined networks (SDN), network function virtualization (NFV), and network analytics provide unprecedented flexibility in configuring the communication services while optimizing the utilization of network resources. The future networks will be completely autonomous, that is, self-organizing, self-healing, self-secure, and self-optimizing. Thus, the broadband networks have become much more than just a telecommunication infrastructure. They are now the backbone of the digital economy, and are envisioned to be enabler of the new business models. The telecommunication industry is developing new solutions including [2]:

- **Application programming interfaces** (APIs) are offering a standardized, controlled, trusted, and secure access to telecommunication services. They support unified access and **over-the-top** (OTT) **services** for different types of users, and can be used for wholesale of connectivity and other applications.

- **Digital platforms** are universal marketplaces connecting digital producers with consumers. Examples use cases are smart city, autonomous vehicles, and ultra-high resolution video streaming services. They resemble operating systems, and are usually hosted in clouds.

- **Digital business models** are often cloudified and formed as XaaS (**anything as a service**) where X can be a platform, infrastructure, network, software, or anything else.

- **Digital ecosystems** are complete solutions and strategies for delivering digital services. They orchestrate architectures, infrastructures, interfaces, policies, and service definitions. They need to be trusted by the stakeholders, even while being highly autonomous and self-configuring.

- **Operations and business support systems** (OSS and BSS) are various, increasingly integrated, policy-driven autonomous systems supporting the key processes, and business models in the enterprises. They include systems for predictive analytics, business intelligence, and customer relationship management (CRM).

- **5G networks** aim to support different application areas (verticals) with vastly different requirements such as enhanced mobile broadband (eMBB), ultra-high reliability and low-latency (uRLLC) networks for the Internet of Things (IoT) devices, and massive machine-type communications (mMTC). The cyber-resilience of these networks is assumed from the onset. However, as of now, the 5G standards are still a work in progress.

- **Digital roadmap** is a digitalization strategy of an enterprise toward fully digital monitoring and control of its processes and operations.

- **Internet of Everything (IoE)** is interconnecting digital platforms, IoT and everything else within different service and industry verticals. The key driver is the customer experience and efficient utilization of the infrastructure and other resources.

- **Edge (fog) computing** distributes computing and digital content centers in the network edges, closers to the consumers in order to reduce latency and load in the core network.
- **Cyber-physical systems** intelligently exploit the connectivity and digitalization to significantly enhance efficiency of the underlying physical systems, and also to improve the business and customer experiences.

The share of revenues by communication service providers (CSPs) within the telecommunication industry has been constantly declining as evidenced by decreasing **average revenue per user** (ARPU) numbers [1]. Large portions of the voice and message revenues have been transferred to the digital content provides offering popular OTT applications. Thus, providing the connectivity and infrastructure as the legacy Internet service providers (ISPs) once did is no longer sufficient. CSPs today need to leverage the connectivity to offer services in new businesses and consumer markets (B2C and B2B). This may be considered to be much more a business transformation than a technology transformation. In fact, the value in connectivity is estimated to be an order of magnitude less than in the digital services [1]. This creates great opportunities for the CSPs to exploit connectivity, agility, cognition, and wealth of data to drive the innovation, customer experiences, and generate new revenues by becoming both digital service providers and enablers. Only then, the CSPs will be able to compete with the traditional content and application providers.

Winning and retaining the customers is and will be even more critical for the business survival. The interactions with customers are now omnichannel. Properly integrating and managing all the interaction channels is crucial for the superior customer experience. The agility and rapid prototyping of new applications (and, as a matter of fact, of the whole businesses) is achieved by modularization and microservices which are accessed via the published APIs. The microservices and APIs are fundamental in building digital platforms in the clouds. The digital platforms substantially reduce the barriers, costs, and times to market for the 3rd party producers to offer goods and OTT services in the web-scale economy as highlighted in **Figure 1**.

The digital transformation is non-trivial, but inevitable for CSPs to remain competitive next to the digital natives such as Google and Amazon who may possibly expand their future activities from computing to also provisioning communication services. The

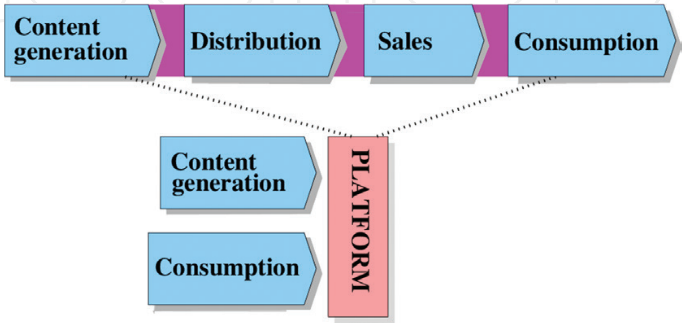

Figure 1. The legacy chain versus the centralized platform business models.

advantage of CSPs is their previous experience in building communication infrastructure, managing the connectivity, and analyzing large volumes of customer and network data. However, the rapid developments of telecommunication systems create many business and technological challenges. It is then important, more than ever before, to carefully consider how to efficiently evaluate, validate, optimize, and orchestrate rather than control these increasingly complex (eco-) systems. Choosing the right metrics and the measurements strategies is critical for this task. The need for standardized metrics for 5G systems is perceived by 21% of CSPs, and 33% of suppliers [2]. The metrics moderate interactions among different stakeholders including equipment manufacturers, subcontractors, infrastructure providers, service providers, content providers, network operators, end-users, governments, and regulatory bodies. The metrics enable to make informed decisions, and to define long-term strategies.

An overview of IT investments, productivity, staffing, and other key business data for enterprises in 21 vertical industries are provided in [3]. The reports such as [1, 3] clearly uncover the cultural changes in high technology companies as their primary focus is moving onto the needs of the customers whereas technology is leveraged for the business growth.

In general, it is desirable that the metrics and measurements exhibit these characteristics [4, 5]:

- **Accuracy:** the measurement errors and biases need to be within acceptable limits.
- **Validity:** the measurements and their evaluations need to be checked for correctness.
- **Feasibility:** the measurements have to be collected as often as desired.
- **Robustness:** the measurements quality must not be affected by changing conditions.
- **Efficiency:** the measurements should not consume too much of system resources.
- **Desirability:** the measurements collected are required for the design and operation.
- **Viability:** the measurements being collected can clearly provide measurable benefits.

The rest of this chapter is organized as follows. Section 2 reviews metrics for digital platforms and ecosystems, websites, and computing systems. Section 3 provides metrics for broadband networks and 4G/5G systems, lists the metrics which have been standardized and which are used for the Internet measurements. Section 4 covers other commonly used metrics for telecommunication networks. Section 5 discusses big data, machine learning, and associated metrics. Finally, Section 6 concludes the chapter.

2. Measuring the digital economy

One of the key objectives in designing technology systems in order to deliver services to end-users is performance. The key measures for evaluating the system performance are: revenues and profits, customer experience, and operational efficiency.

A digital maturity model assesses readiness and effectiveness of the enterprise on its digital journey [2]. It evaluates the digital strategy, understanding of customers, human resources and other assets, processes and operations, and the availability of required technology. It is usually given a score between 1 (initial, ad-hoc improvements) and 5 (a highly optimized digital enterprise) in each of these dimensions. Since the cost of reaching the highest score in all dimensions may be prohibitive, prioritization of objectives, and balancing the costs against the benefits is important. TM Forum [6] developed a sophisticated digital maturity model evaluated over 5 main dimensions (customer, strategy, technology, operations, and organization) with 28 sub-dimensions, and additional 175 criteria questions.

2.1. Metrics for computing systems

Many computing systems are implemented in clouds, and their access is governed by security and demand policies as well as admission rules. There are three main groups of shareholders in this space: the cloud infrastructure and application providers; the 3rd party application and content providers; and the service consumers. The following metrics can be used to measure the technological and business performance of computing systems [7].

Service and system availability is the percentage of time the system is operational, so it can deliver services without degradation. It can be equivalently expressed as the average downtime over a given time period such as month, or year, as the average outage, or as the average time between failures. When the failure occurs, the average **time to recovery** may be useful.

Response reliability is a fraction of the satisfactorily handled requests or service outcomes.

Response time is the average time until the response is received after generating a request. Since the response time may be greatly increased during high demand conditions, the load balancing is critical to provide sufficient scalability of the service provisioning. A similar measure is concerned with the delay to create and configure a new computing instance.

Security threats and incidents detected per a unit of time, for example, in a month, are the indication of both the service attractiveness for an unauthorized use as well as the level of security detection and prevention mechanisms deployed in the system.

Throughput or bandwidth is the number of transactions or requests handled per unit of time, usually a second. It is particularly important for systems and services operating in real-time or at large scale. For real-time services, the average **latency** for repeated requests is also useful.

Capacity or maximum utilization is capability of the system to concurrently handle all or most of the workload requests without a delay, or it is the maximum available computing power or storage space for a single user workload. It can be also expressed as **scalability**, that is, the maximum number of requests served at any given time. On the other hand, **system elasticity** allows scaling the resources to match the total current workload and service demand.

Computing and storage capacity is measured either as the number of processor cores and the memory size available, or at the level of computing units such as the number of virtual servers.

Cost per request, per workload unit, or per user accounts for all supporting, operational, and business processes and any other recurring costs required to provide the agreed services to users. For a well-designed system, this cost is decreasing over time as the system scales up, so the revenues and profits are sustained or improved.

Return on invested capital (ROIC) can be expressed as the number of years until the total profit generated by the offered services exceeds all costs accumulated from the capital investments and the operational expenditures (OpEx).

Market share growth can be indicative of the business viability. If it is declining, the business is normally unsustainable over long-term horizons.

Furthermore, technical metrics for Google Cloud and Amazon Web Services monitoring are listed in [7]. Google also developed the corresponding API to access these clouds and collect the metric values from running application instances. Although the users can define their own metrics to observe, the data can only be collected for the user private projects. The main metric attributes included are the metric name, type, value type, units, and description.

2.2. Metrics for websites

The web analytics provide indication how the website content is perceived by online visitors. It measures a success rather than performance of a website. It plays important role in effectively disseminating information, online marketing, and optimizing traffic and web hosting [8].

Website traffic indicates the trend of online visits, whether it is growing, stagnant, or declining. It can be used to evaluate recent changes in the website content and its efficacy to attract the visitors. It is also useful to breakdown the visitors as new, repeated, returning, and unique ones.

Traffic sources reveal where the visits are coming from. They can arrive via search engines, from another referral, social or other websites, or directly. This metric is often important to evaluate the search engine optimization (SEO) strategy.

Bounce rate is the percentage of visitors only seeing a single page, and *not* exploring other pages on the website except the initial or landing page.

Number of shares on social media is an indirect indication of the page or posted article popularity.

Conversion rate is a ratio of the unique visitors to the number of conversions, that is, those visitors performing a desired action such as visiting a recommended site, subscribing to a service, or purchasing a product. It is therefore one of the most important measures of the website usefulness. Tracking the conversions allows us to evaluate other metrics such as **value per visit** and **cost per conversion.**

Many other more detailed metrics are provided by the website analytics engines, for example, by Google. For instance, **visit duration** is calculated as a time difference between the first and last activity of the visitor, **click through** is the number of times a link was clicked, **exit page rate** tracks the last page visited on the site, and so on. More detailed description of the metrics used for website analytics can be found in [8].

2.3. Metrics for digital platforms and ecosystems

Traditionally, Zachman framework has been very popular to manage the complexity of modern enterprises since the late 1980s [9]. It enables a systematic and consistent approach to model complex enterprises from the perspective of different stakeholders. For a set of five principal viewpoints representing different stakeholder interests, there are six metric or model attributes as shown in **Figure 2**. The model of enterprises is then represented as a two-dimensional matrix.

The complexities of emerging digital ecosystems are overwhelming. The number of metrics which need to be considered for complex systems is usually very large. It is then crucial to develop a management system to systematically record, categorize, update, search, and otherwise maintain these metrics. A comprehensive framework covering business processes, applications, and information management is being developed by TM Forum [6]. It is a complete suite of standards and best practices to assess and optimize the performance of digitalized businesses. It is a service-oriented framework which strives to support extensive automations of business processes. It is built on two cornerstones: almost 3000 standardized metrics embraced by the industry, and open-source APIs to support the integration across platforms. This approach to digital ecosystems drives innovation while reducing the risks and shortening time to markets. The improvements in system maturity are directly transformed to a better customer experience, and the reduced costs. The framework metrics are organized in several categories: business, customer experience management, cyber operations, fraud management, and cable operations. The business metrics categories are summarized in **Figure 3** [6]. Note that some metrics have additional attributes, for example, the shopping awareness under the customer experience has the attributes access, time, and quality.

The Frameworx digital ecosystem by TM Forum defines rich metadata for each metric assuming many attributes. The attributes are organized in several sections, and each section contains a number of attribute fields. Examples of the attributes provided for each metric are:

- Overview section gives a summary of the main attributes such as the metric ID, business value driver, capability, reporting details, accuracy, responsible entity, capture period, full name, value type, value range, and metric type.
- Description section is a textual summary of the metric whereas general comments are inserted into a separate section.

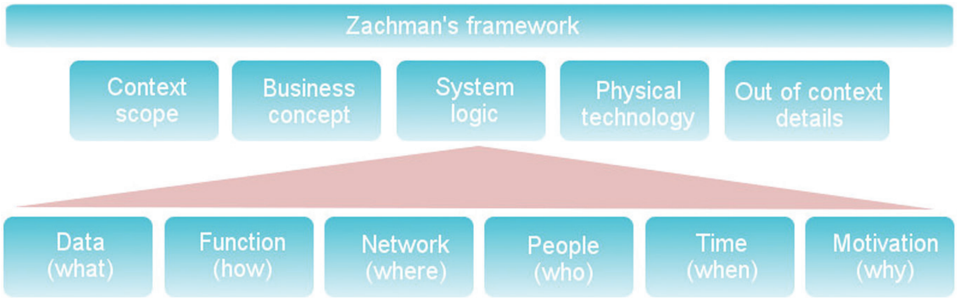

Figure 2. The Zachman modeling framework of enterprises.

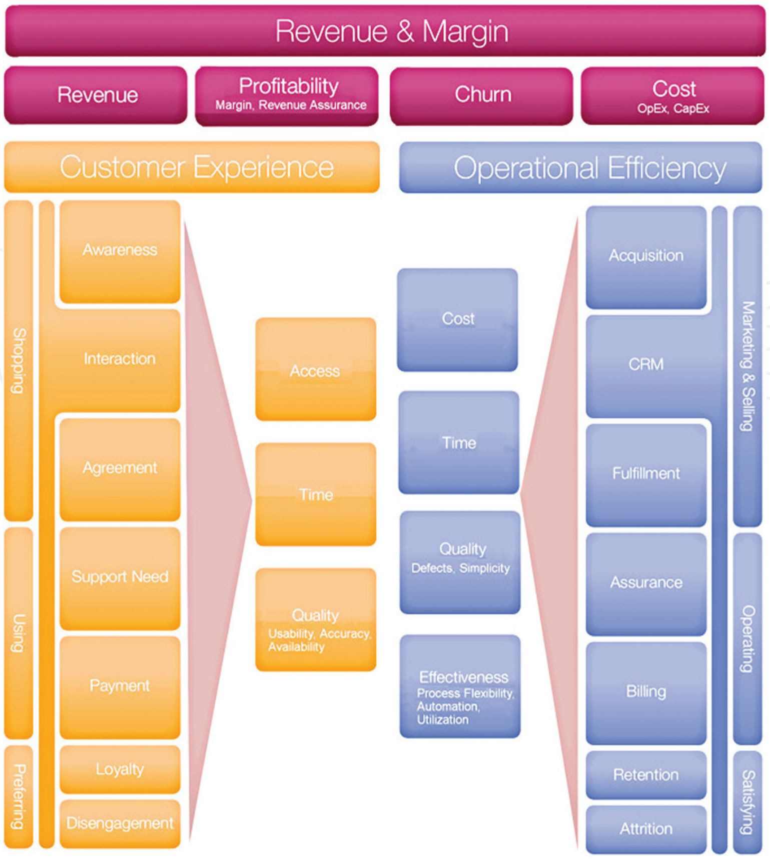

Figure 3. The business metrics categories defined within the Frameworx digital ecosystem by TM Forum.

- Category & Topic section classifies the metric according to its main type, and then three sub-categories depending on the metric objective, specific type, and purpose. Other attributes recorded in this section are the metric level, state, and topic.
- There are other sections to capture the metric mathematical formula and the symbols used.
- Associations section gives details about where the metric is primarily being used. This includes diagrams, other metrics, domains, and documents.

3. Metrics for broadband networks

OECD defines a **broadband service** as having the baseline speed of at least 256 kbit/s [10]. This value has been selected to provide a minimum acceptable quality of service (QoS) for typical broadband applications such as web browsing and VoIP. It is a loose definition which may be less appropriate to compare different broadband technologies, and to improve network performance characteristics. For instance, many countries are introducing mandatory minimums for the broadband access (e.g., 1 Mbit/s in Finland, and 600 kbit/s in downlink and 100 kbit/s in uplink in Switzerland). In practice, broadband measurements provide other data than the access speed, so the definition of broadband may be modified in the future [11]. It is generally agreed that IoT and machine-to-machine traffic is excluded from broadband network measurements, since their traffic profiles are very different from consumers driven traffic, and their traffic is normally restricted and processed locally, for example, within the IoT platforms, so it does not traverse the Internet core or larger parts of the access networks [11, 12].

The roll-out of broadband networks has a direct and measurable impact on the economic development of countries and regions [10]. It stimulates innovations, and has other social impacts such as improved level of the economic productivity, public administration, business practices, health and education. For these reasons, OECD carefully observes developments in the broadband coverage and penetration. OECD defined the broadband checklist including the items directly related to the broadband metrics and measurements such as [10]:

- define broadband services by speed tiers while reflecting national specificities;
- measure the deployment of broadband networks by exploiting the interactive Internet mappings;
- measure the investments in broadband infrastructure, market share, competition among the broadband providers, and also compare the broadband pricing;
- develop a harmonized methodology to measure the broadband speeds, coverage, and capacity;
- explore reliability of the Internet-based statistics to infer traffic flows and web usage patterns;
- develop indicators of the mobile broadband uptakes based on traffic and usage patterns;
- develop new indicators of the broadband demands and of intensity and sophistication of the broadband technology usage patterns;
- develop automated data mining methods to improve learning form the collected broadband statistics; and
- develop appropriate metrics and improve reporting procedures to monitor issues of the security, privacy and consumer protection.

The **speed tiers** of broadband assumed by OECD are: less than 1.5/2 Mbit/s, 1.5/2–10 Mbit/s, 10–25/30 Mbit/s, 25/30–100 Mbit/s, 0.1–1 Gbit/s, and above 1 Gbit/s. Other important actions driven by OECD include measuring the technical and other skills which are required in the digital economy. Moreover, OECD advocates development and use of analytical frameworks and statistical approaches to assess the issues and impacts of the broadband networks on the digital economy and society. In particular, the security and privacy should be assessed across many dimensions including threats, vulnerabilities, incidents, impacts, prevention, and responses. In addition to security and privacy, data on the Internet-related activities incur the costs in order to be of sufficient statistical quality.

In the 2012, OECD workshop on broadband metrics [11], it was recommended to consider the following four categories of metrics for the broadband networks:

- broadband availability metrics and mappings;
- broadband infrastructure investment metrics;
- broadband performance metrics; and
- broadband competition metrics.

We will focus mainly on the broadband performance metrics in the sequel of this chapter. The key performance indicator (KPI) for the broadband Internet access is a **connection speed**. The connection speed affects the quality of experience (QoE), usefulness of applications, and also impacts the broadband policies. However, measuring the connection speed is not straightforward, and common methodologies and best practices to measure the broadband access quality are still subject to many discussions [12, 13]. For now, it has been agreed to classify the connections as wireline and wireless rather than fixed and mobile, and consider whether the broadband users also use or not voice services while their monthly data allowances are less than 500 MB, less than 1GB, less than 5GB, and being more than 5GB. It is further recommended to distinguish between the demand-side and supply-side metrics, and between households, individual consumers, and businesses.

The **demand-side metrics** are obtained from surveys among the regulators and other governmental organizations, and from the data provided by the mobile service providers and other industry stakeholders. From surveys, one obtains **penetration or adoption of broadband services**, applications used, their frequency and usage patterns, socio-economic profile of users (age, gender, education, and income), and the usage issues (e.g., security, pricing, and performance). CSPs can provide data on the number of connections, traffic volumes, usage patterns, and quality of service (QoS) whereas industry stakeholders (e.g., Akamai, Cisco, and Alexa) collect various web statistics. However, the number of subscribers may not be a good indication of the actual broadband usage. Especially for wireless access, the subscribers can have data usage plans which may not be fully utilized. The pricing, tariff plans, and service bundles such as monthly allowances, flat-rates or pay-per-use have significant impact on the broadband usage [14]. It is also possible to exploit crowdsourcing measurements, for example, by downloading a specialized application [15, 16].

The **supply-side metrics** report on the broadband capacity, availability/coverage, speed, and competition. More specifically, **broadband coverage** reflects either the whole region with all broadband providers considered, or it is evaluated for each provider separately. **Broadband network capacity** is the total communication spectrum available, possibly averaged over the regions, or the population while conditioned on the air interface (e.g., 3G/UMTS, long-term evolution (LTE), HSPA, and WiMAX) the technology used (fiber to the premises/cabinet/home, coax, twisted copper cable), and the duplexing method and frequency band used. **Access speed** is one of the most commonly reported metrics on the quality of broadband networks, so we discuss it here in more detail. Similar discussion is generally valid also for other types of performance metrics.

The **access speed** can be either the actual speed measured during the tests, delivered in a day to day use, or it is the advertised (headline) peak or average speed. The advertised and delivered speeds can be vastly different, and each of these speeds can have large variations across the regions, even when the same technology is used. There are obvious speed differences for wireline and wireless access. For the latter, the speed varies greatly as the devices can use one of their wireless interfaces (WiFi and 3G/4G) depending on the context such as mobility. The measurements should be segmented based on the device portability and device type. A typical household has multiple devices sharing the same outgoing connection to the broadband network. The advertised speeds tend to be the theoretical peak vales (the capacity) whereas the measurements are more likely to be the average values. Thus, it is not sufficient to just know the broadband speed, but one has to know what exactly is being reported, that is, peak versus average value, mean versus median average, theoretical versus measured value, end-to-end (Internet) versus the first router (access) speed, when the measurement was performed, and so on. More sophisticated measurement methods can be adopted to average out the measurement noise, for example, using long-term averages of the short-term peaks. Whereas the download speeds were traditionally much larger than the upload speeds, these speeds are becoming more balanced as the users are generating a lot more of their own contents [12]. The speed measurements are usually done with the TCP protocol which can be setup to use one or multiple simultaneous or parallel connections, since a typical webpage generates about 90 requests for content including HTML, CSS, javascript, images, and advertising [17]. However, many of these requests are small pieces of data which are unlikely to reach the full transmission speed of the connection, unlike the transfer of large files over longer time durations which are much more likely to reach the full capacity speed. Thus, the access speed can vary for different applications being used. The broadband speeds for a certain region are typically the values averaged over selected subscribers. How to choose a representative set of these subscribers is another important issue. For instance, sharing of broadband lines between residential customers and businesses significantly influences the speeds observed. The broadband speeds are also strongly affected by the traffic management and traffic shaping policies of CSPs. The fair use policies are especially enforced in the wireless environment. The policies vary the capacity of broadband networks throughout the day, and so they also affect the access speeds. The collected broadband data are often used to compare the offerings of different CSPs, and to formulate the broadband policies, so a consistency in reporting the broadband data is important [16, 18].

Broadband availability in a region is a geographical mapping of the broadband service levels to mainly capture the service providers, the broadband technology in place, and the advertised download and upload speeds. The data can be expressed in different granularity, for example, from whole regions to local municipalities. The most important regional differences in broadband availability are among the urban, sub-urban, and rural areas due to their vastly distinct densities of broadband subscribers. However, the European Commission in its Digital Agenda envision complete (100%) broadband coverage in Europe at 30 Mbit/s or higher by the year 2020.

In order to assess usage of a specific application or service, the user-defined metrics appear to be more common. For mobile internet applications, the following metrics have been defined in [17] to understand the service adoption within a population:

- **Service penetration rate** (SPR) is a fraction of service users among all users in a given time period.
- **Busy hour service attempt** (BHSA) is a fraction of service users during the busy hours among all service users in a given time period.
- **Concentration factor of service attempt** (CSA) measures a concentration of service uses throughout the day.
- **Monthly service activity** (MSA) is a concentration of service uses within days over a month.
- **Service holding time** (SHT) is the average time duration of each service use.
- **Service throughput per usage** (STPU) is the average traffic volume generated during each service use.
- **Time interval of service attempts** (TISA) is the average time interval between two consecutive service attempts by the same user.
- **Net data rate** (NDR) is the average data rate of a service measured at the application layer.

3.1. Metrics for 4G/5G systems

The optimization of broadband networks in 4G/5G systems is driven by an agreed set of KPIs. The KPI monitoring is used both for real-time management of the network as well as for longer term planning of the capacity. The network optimization is dependent on the operator strategy, and the number of systems and sites involved. It targets traffic management, the user experience, and the capital and operational costs. The user experience includes uplink/downlink data rates, and **connectivity** in terms of the coverage, connection setup time, and connection outage or rejection rate. The network planning involves the network coverage and accessibility, **level of congestion** and **traffic volume or density**. The LTE (long-term evolution) standard recognizes at least the following three categories of the KPIs.

Radio-frequency (RF) KPIs are assumed especially during the network roll-out and initial optimizations to achieve the desired coverage with the planned levels of the RF signal strength. These KPIs are usually measured as distributions of the received reference signal strength.

Service KPIs are used to ensure the long-term quality of service and quality of experience targets for different data and voice services as well as to attract and retain the subscribers. These KPIs are usually groups depending on the specific network service such as radio channel access mechanism and type of control messages. The **subscriber retainability** is affected by the handover rate, call drop-off rate, call rejection rate, and other.

Operation KPIs are continuously observed to fine tune the network performance for the current service or traffic demands. These KPIs include the measures of service quality such as data rates, packet loss rates, and packet delays, and the measures of **utilization of the network resources** such as the fraction of resource blocks allocated, module and signaling loads, **cell and channel occupancy rate**, scheduling rates, and other.

The KPIs for 5G systems are defined by the 3GPP standardization body. The aim is to achieve the following improvements against the existing 4G networks: 1000× larger traffic volumes per geographical area, up to 100× more connected devices, up to 100× higher data rates, 10× smaller energy consumption, end-to-end latency at most 1 ms, and ubiquitous coverage also in areas with low density of users. More specifically, the KPIs for 5G networks are defined in three main categories in accordance with the main design goals of the 5G networks.

For eMBB services, the main KPIs are **peak data rate** (20 Gbps in downlink and 10 Gbps in uplink), **expected data rate** (100 Mbps in downlink and 50 Mbps in uplink), and **spectral efficiency** (30 bps/Hz in downlink and 15 bps/Hz in uplink).

For uRLLC services, some of the main KPIs are **maximum latency** (10 ms in control plane, and 0.5 ms in user or data plane), **reliability of packet delivery** (1 lost packet per 100 million transmitted packets), and **connection interruption time** due to mobility (0 ms).

For mMTC services, the important KPIs are **area traffic capacity** (10 Mbits/m^2), **connection density** (1 million/km^2), **energy efficiency** (90% reduction of energy consumption compared to the 4G), **coverage** in terms of the received signal strength (−164 dBm), and the user equipment **battery lifetime** (15 years).

Other metrics for 5G networks which are under development are related to advanced network functions such as network security and network virtualization.

3.2. Standardized metrics for measuring quality of broadband networks

In practice, what really matters is the QoS of broadband networks for CSPs and the QoE for the consumers [19]. We will discuss QoS and QoE metrics more generally in the next section.

ITU-T Y.1540 standard assumes the following metrics to measure QoS over the end-to-end heterogeneous connections:

- **IP packet transfer delay** (IPTD) is the time difference between the ingress and egress packet events when such packet is successfully delivered without errors.
- **IP packet delay variations** (IPDV) are affected by the TCP retransmission mechanisms and may cause undesirable overflow and underflow of packet buffers.
- **IP packet loss ratio** (IPLR) is a fraction of lost packets.
- **IP packet error rate** (IPER) is a fraction of erroneously received packets.
- **IP packet reordered ratio** (IPRR) is a fraction of reordered but otherwise successfully received packets.
- **Spurious IP packet ratio** (SIPR) is a number of spurious packets observed during a specified time interval.
- **IP packet severe loss block ratio** (IPSLBR) is a fraction of the severe loss block outcomes.
- **IP packet duplicate ratio (IPDR)** is a ratio of duplicated packets to the successfully received packets minus the number of duplicated packets.

- **Replicated IP packet ratio** (RIPR) is a ratio of replicated packets to the successfully received packets minus the number of replicated packets.
- **Service availability** is IPLR < 0.75 for at least 5 min duration.

IETF proposes the following five metrics for the end-to-end QoS reflecting the TCP retransmission mechanisms:

- **Link/path bandwidth capacity** (RFC5136) is the overall link/path bandwidth capacity.
- **Bulk transport capacity** (RFC3138) is the bandwidth capacity at the transport layer.
- **One-way and two-way packet losses or connectivity** (RFC2680) is simply the number of packets lost.
- **Packet one-way and two-way delay** (RFC2679, RFC2681) is the end-to-end packet delay.
- **Delay variation** (RFC3393).
- **Packet reordering** (RFC4737).
- **Duplicated packets.**

ITU-T defines six service classes corresponding to the specific values of the metrics listed above. These classes can be mapped to named classes defined in IETF as follows: Class 0/1: telephony, real-time interactive, and multimedia conferencing services; Class 2: signaling; Class 3: low-latency data and high-throughput data; Class 4: broadcast video, multimedia streaming, and low-priority data; and Class 5: standard services. Note that both ITU-T and IETF standards are operator oriented.

The subscriber-oriented QoS may assume additional metrics such as [15, 18]:

- upload and download speed;
- round-trip time (RTT) delay/latency;
- delay jitter;
- packet loss;
- DNS failure rate is a proportion of failed translations of a website name to the IP address;
- DNS resolution is a delay to translate a website name to the IP address;
- web browsing speed is a time it takes to fetch a complete content of a website;
- average daily disconnection is a number of interrupted broadband services per day lasting more than 30 s; and
- distance from the digital exchange indicates the anticipated delays and access speeds.

More importantly, Ofcom evaluates not only the absolute values, but also statistically the probabilities that these metrics are above or below a given threshold:

- the probability of download/upload speed greater than 2 Mbit/s;
- the probability of web browsing loading speed below 1 s; and
- the probability of latency less than 0.1 s.

In addition, Ofcom regularly performs a series of video streaming tests (Youtube, Netflix, and BBC iPlayer) displayed in the standard definition, high definition, and ultra-high definition in order to assess the quality of broadband networks by different CSPs in the UK. In determining the average broadband speeds, Ofcom published the statistical methodology it uses for processing data including the weighting factors to account for different broadband technologies, rural versus urban locations, and varying distances from the network exchange.

Finally, FCC evaluates the broadband networks in states and cities in the US by deploying measuring equipment and using SamKnows methodology [16, 20].

- **Download/upload speed** is throughput in Mbit/s utilizing three concurrent TCP connections.
- **Web browsing** reports the times to fetch a webpage and all its resources from a popular website.
- **UDP latency** is the average RTT of a series of randomly transmitted UDP packets distributed over a long time frame.
- **UDP packet loss** is a fraction of UDP packets lost during the UDP latency test.
- **Video streaming test** measures the initial time to buffer, the number of buffer under-runs and the total time for buffer delays.
- **Voice over IP test** measures the upstream packet loss, downstream packet loss, upstream jitter, downstream jitter, and RTT latency.
- **DNS resolution** is the time for CSP recursive DNS resolver to return a record for a popular website domain name.
- **DNS failures** are a fraction of DNS requests performed in the DNS resolution test that failed.
- **ICMP latency** is RTT of five regularly spaced ICMP packets.
- **ICMP packet loss** is a fraction of packets lost during the ICMP latency test.
- **Latency under load** is the average RTT for a series of regularly spaced UDP packets sent during the sustained downstream/upstream tests.
- **Consumption** is a simple record of the total bytes downloaded and uploaded by the router.

The measurements are obtained for both IPv6 and IPv4 protocols separately. FCC details their statistical data processing methodology including treatment of outliers, adjustment of peak hours to local time, testing setup to avoid congestion and traffic shaping effects, and accounting for the speed-enhancing services.

3.3. Metrics for measuring internet traffic

Measuring Internet traffic is one of the key monitoring tasks for managing and monitoring broadband networks [21]. It is used by CSPs in real-time operations as well as for long-term planning to optimize the network resources, identify anomalies and security issues, and establish traffic control policies, and set the correct levels of service pricing. The processing of traffic measurements is used to classify traffic type, extract more detailed characteristics, and evaluate the statistics [22]. The accuracy and, in some cases, also completeness of such information is critical aspect of CSP business intelligence to remain competitive. There are many challenges in measuring particular traffic. The measurements can be done at or across the flows, or at the level of individual packets, and the measurements can be partially, fully or not at all aware of the underlying protocol used. Unless the measurements are done at the end-points, the router collecting data may not see all packets from the flow as some packets are likely to be routed through a different path. Similarly, many applications use multiple connections to deliver content. The measurements to be meaningful need to check whether more than one connection exists, and then identify which connections belong to the same traffic flow. Moreover, it may be also important to identify different sessions which stemmed from the same application. At a deeper level, examining control information of protocol packets enables to track the protocol state which significantly improves the traffic identification accuracy. Some applications rely on the protocol encapsulation and tunneling, for example, the IPv6 protocol routed through IPv4 sub-network. In this case, the packet inspection needs to look at the payload of the encapsulation protocols. Other challenges in measuring Internet traffic are traffic encryption, for instance, there is increasing preference for using the HTTPS protocol, and traffic is also affected by the deployed proxies.

Some of the **Internet traffic attributes** which are extracted during the deep packet inspection are [21, 22]:

- service tier, content provider, operating system, browser, website;
- IP addresses, MAC addresses, client device, client device type;
- application protocol, media stream type, session protocol, transport protocol;
- video codec, audio codec, media container, video resolution;
- over-the-top application; and
- control versus data content.

4. Other metrics for telecommunication networks

There are many sources of metrics for telecommunication networks [5]. The largest pool of metrics can be found in technical literature. Some of these metrics are much more widely adopted than the others. There are many advantages to create metrics standards in order to ensure consistency and fair comparison of products and services. The metrics standardization is usually driven by industry consortia and telecommunication regulators. In this section, we will review the most commonly used metrics for telecommunication networks. In general, there are often trade-offs between different metric values, so the metrics have to be selected carefully when they are used as KPIs, for instance, to achieve fairness. At a system level, **fairness** evaluates how the network resources are shared and the network capacity utilized among multiple users. We can also evaluate whether a single user is provided a fair access to the network resources and capacity. The most popular measures of fairness are:

- **Jain's index** is independent of the network size, and independent of the measure quantifying how the resources are used by the individual users [23].
- **Max-min fairness** does not allow to increase the resource utilization of one user, if that user has larger utilization of resources than other users.
- **Proportional fairness** is useful in scenarios which incorporates utilization of multiple resources.

In the following subsections, we will review five categories of the most commonly used metrics for telecommunication networks [4].

4.1. Energy and power metrics

The main driver for reducing the energy consumption in telecommunication network is to reduce the operational costs, and to increase the battery lifetime of handheld devices. The measurement procedures including exact location of the measurements, time interval, and conditions such as network load, QoS constraints, and applications are the key factors influencing the measured values of energy consumption.

- **Total energy consumed** is a sum of operational and embodied energies.
- **Operational energy** is the energy consumed during the operation, and it corresponds to the RF power and the overhead power. The overhead power accounts for the baseline circuit consumption at a zero load.
- **Embodies energy** summarizes the energy over the whole life-cycle of the equipment. It includes the energy for manufacturing, transport, installation, decommissioning, and disposal.
- **Energy consumption rating** (ECR) is a ratio of the expended power and the maximum data throughput.
- **Variable-load ECR** is measured as a ratio of weighted averages of the power and the data rates at several values of network load.
- **Energy efficiency rate** (EER) is the inverse value of ECR.
- **ECR for radio access networks** (ECR-RAN) is a ratio of the total expended power in the cell to the cell surface area.

- **Power ratio** of equipment is simply a ratio of the output power to the input power.
- **ATIS energy metrics** are defined as ratios of logarithm of the expended power to the capacity or throughput.
- **ITU metrics** are ratios of the expended power and the product of throughput and distance, for wireline networks, and throughput and area, for wireless networks, respectively.
- **Key power** (not performance) **indicator** (KPI) is a ratio of coverage for rural areas or the number of subscribers for urban areas to the total cell site power, respectively.
- **Transceiver energy consumption** is given by the powers used in transmitting, receiving, scanning, idle, and sleep modes.

4.2. Quality of service

CSPs do not explicitly sell QoS to the subscribers and businesses, but it is included in service packages as the service level agreements (SLAs) at different costs. CSPs may change or update the performance indicators, and still target the same QoS. Guaranteeing QoS is, in general, difficult due to dynamic channel allocation, dynamic routing, energy saving, and fault tolerance mechanisms used. Both passive and active traffic monitoring can be used to assess the level of QoS provided. Since the network resources are shared among many traffic flows, traffic prioritization, and engineering is a dominant method to manage QoS in broadband networks. In both wired and wireless networks, the QoS metrics can be classified as **application-oriented QoS** (AQoS) and **network-oriented QoS** (NQoS). The former is concerned with end-to-end QoS as required, for example, by real-time applications while the latter is concerned with optimizing a core network of routers and switches. Hence, the AQoS metrics can be used to assess the user satisfaction with applications, whereas the NQoS metrics measure the network capability to deliver services while efficiently utilizing the network resources. The application requirements are usually translated to corresponding network characteristics, and they often vary over time.

Most QoS metrics considered in the literature are NQoS metrics such as:

- **Throughput** usually refers to a single flow, and is expressed in bits/s. The throughput can be determined for a single hop, end-to-end connection or aggregated for the whole network.
- **Computing or service throughput** is the ability of a system to process requests and to deliver the work in a given amount of time.
- **Packet delivery ratio** (PDR) is a ratio of the successfully delivered packets to the total number of generated packets. However, measuring the end-to-end packet losses is not straightforward, so the packet losses are usually inferred indirectly.
- **Packet latency** is normally defined as the average end-to-end delay.
- **Delay jitter** is the variance of random end-to-end packet delays. It can be measured for delays in one direction only, or the delays are considered as RTTs. Alternatively, the jitter can

be calculated as the difference between the maximum and minimum RTT values. The jitter can be classified as random/deterministic, correlated/uncorrelated, and constant/transient/short-term.

From the user point of view, **availability** is one of the most important QoS metrics. The users expect that the network is resilient to failures and can provide the agreed services most of the time. More precisely, CSPs standardly aim to achieve 99.999% ("five nines") of the service uptime. Evaluating the availability is not straightforward, since the reliability of many components, systems, and their interactions is at best estimated. Therefore, SLAs usually specify the acceptable downtime and outage periods within a given time interval. The availability can be assumed end-to-end, or at network level. The most commonly used availability metrics are:

- **Mean time to failure** (MTTF) is the expected time to the next failure.
- **Mean time to repair** (MTTR) is the average time to return to operational state after a failure.
- **Mean time between failures** (MTBF) is the average time between two successive failures.
- **Impacted user minutes** (IUM) is a product of the number of users affected by the failure and the failure duration in minutes.
- **Defects per million** (DPM) is a measure of defects of a component or equipment.
- **Point availability** is the probability the system is operational at some future time given the last repair time.
- **Average uptime availability** is a proportion of time the system is ready to deliver the service.
- **Steady-state availability** is expressed as a long-term probability for given rates of failure and repair.
- **Inherent availability** is the steady-state availability considering only corrective downtime.
- **Achieved availability** is the availability assuming only the planned shutdowns.
- **Operational availability** is the average availability assuming all expected downtimes.

4.3. Quality of experience

The QoE metrics evaluate the user satisfaction with the provided level of service. Among challenges to define QoE metrics are: non-linear perception processing by the human senses, lack of accurate models of the human perception, and fast-pace of development of new technologies and services. As the new networks such as the 5G are transforming from the network-centric to user-centric designs, there is a shift from QoS-oriented to QoE-oriented network management. The QoE can be used to determine the required QoS of the network, and how to set adequate pricing levels. However, the relationship between QoS and QoE is complicated, since the improvement in QoS does not guarantee any improvement in QoE. In practice, QoE is evaluated using either subjective or objective metrics. The **subjective QoE** metrics take the human perspective on perception of quality differences through measured statistics, and mainly through the user surveys. However, the surveys are laborious and slow to obtain. Even though the subjective QoE metrics are not generally considered by standardization bodies such as ITU and ETSI for new real-time applications, they are becoming popular among CSPs to accurately forecast the consumer satisfaction.

- **Mean opinion score** (MOS) is a numerical QoE index evaluated through subjective tests, but it ignores some other important aspects such as applications interactivity.
- **Double stimulus continuous quality scale** (DSCQS) is index of video quality which is less sensitive to context, but it is also inefficient for real-time evaluations.
- **Single stimulus continuous quality evaluation** (SSCQE) is more representative for quality monitoring of real-time applications.
- **Absolute category rating**, also referred to as **single stimulus**, optionally with **hidden reference removal** (HRR) is efficient, reliable, and standardized method permitting a great number of test conditions during a single test period.
- **Double stimulus impairment scale** (DSIS) is a paired evaluation of an unimpaired reference video against the impaired video.
- **Single stimulus continuous quality evaluation** (SSCQE) uses a slider device and no standard video.
- **Just noticeable difference** (JND) is a scale obtained by a series of comparison tests on two samples while intensity in one sample increases or decreases.
- **Maximum likelihood difference scaling** (MLDS) measures a relative difference in quality to represent the utility of the tested parameter on visual quality.

The **objective QoE** utilize algorithms, data, and mathematical models to infer the user satisfaction. The data are often QoS measurements which is attractive, since they can be used adaptively and in real-time. The objective QoE can rely, to a different degree, on a reference signal such as a video or an image. The **full-reference** (FR) metrics calculate deprivation of the encoded and subsequently decoded signal pixel-by-pixel. The **reduced-reference** (RR) metrics restrict the comparison to some parts of the signal. In order to completely remove the dependence on a reference signal, the **no-reference** (NR) metrics relies on the ability of human observers to determine the quality of the observed images. The challenges in devising the objective QoE metrics is an unknown dependence on the system parameters, unknown non-linear nature of the human perception, and varying satisfactions of users over time requires that QoE is monitored and updated regularly. The selected QoE metrics for objective evaluation of quality are:

- **E-model** estimates MOS in real-time by computing a so-called R-factor.
- **Perception evaluation of speech quality** (PESQ) model estimates MOS by comparing the observed signal with a reference.

- **Application performance index** (APDEX) evaluates consumer satisfaction on a scale between 0 (no users are satisfied) to 1 (all users are satisfied).
- **Peak signal-to-noise ratio** (PSNR) measures similarity between two different images assuming **mean square error** (MSE).
- **Moving picture quality metric** (MPQM) is a video quality index obtained using a mix of content dependent factors and the network impairments such as packet losses and delays.
- **Motion-based video integrity evaluation** (MOVIE) evaluates video impairments jointly in space and time.
- **Structural similarity index** (SSIM) measures degradation of structural information in video or image such as luminance and contrast.
- **Video quality metric** (VQM) detects human perceivable artifacts in images and video for given codec type, block, and color distortions.
- **Pseudo subjective quality assessment** (PSQA) is a real-time evaluation of quality of video or audio communications over packet-based networks.
- **User satisfaction index** (USI) exploits rigorous analysis of the network level QoS metrics during the call duration.

4.4. Security metrics

The security metrics are ill defined due to lack of sufficiently accurate mathematical models of security. Unlike QoE metrics which can be inferred from the objective QoS measurements, there are no such established baseline metrics which can be objectively measured to infer the security of a system. This is also the reason why there are many more user-defined security metrics than commonly used or even standardized security metrics. Even if the standardization bodies recommend some security metrics and security assessment frameworks, they do not specify any security protection or detection methods, and it is difficult to predict how effective these methods would be. If broadband networks can be made more secure by adopting security policies and procedures, then the security metrics can indicate a relative difference of the perceived security rather than providing the absolute measures. Hence, it is useful to consider a baseline system to evaluate the effectiveness of the implemented security mechanisms, to compare various security strategies, and to decide whether the security policies should be updated. However, comparing security vulnerabilities of the IT technology involving human behavior is challenging, and there are currently no established security metrics combining these two perspectives. A large body of research work considers how to identify the most appropriate security metrics.

Attack graphs are a common tool for modeling system vulnerabilities [24]. They visualize possible progression of the attack from one vulnerability to another. As the more vulnerabilities exist in the system, the more opportunities the attackers have to devise and launch an attack. Due to the size of attack graphs, they can be formed automatically, and they are usually generated for a given host in the network which needs to be protected.

Common vulnerability scoring system (CVSS) is a universal language to describe system vulnerabilities, their urgency, and then prioritize the response and defenses [24]. More importantly, it can be considered as industry standard on defining and accessing the security of systems and products. However, CVSS does not score threats, real-time attacks, or it can manage the security risks. Instead, it combines base, temporal and environmental metrics, and formulas to produce a single security score for the whole system. The base metrics are: access complexity, authentication, and confidentiality, integrity and availability (CIA). The temporal metrics consider time dependency of vulnerabilities, and the environmental metrics are concerned with implementation issues leading to vulnerabilities. The base and temporal scores reflect the severity and urgency, respectively. They are computed and published by equipment vendors whereas the environmental score is computed by users. There are also attempts to further optimize the CVSS scoring to specific systems being considered. Since there are, generally, no widely adopted user-defined security metrics in the literature, we provide a brief list of those which are used somewhat more frequently.

VEA-bility metric (vulnerability, exploitability, and attackability) is a 3D score assessing the network security [25]. It combines impact and temporal assessment of vulnerability expressed as CVSS scoring with exploitability, network topology, and possible attack paths from the attack graph. The scores are evaluated for each network host, and then combined into one final value.

Mean time-to-compromise (MTTC) is the average time required by the attacker to compromise the network [26]. The network compromise event is defined by a set of conditions. The security modeling in this framework assumes attack graphs and probabilities of security-related events.

Relative cumulative risk (RCR) of vulnerability is evaluated as a score combining the individual and neighboring network risks, and measuring the proximity to the untrusted hosts [27].

Hazard metric evaluates the security risks of a network by assessing the network maturity level, frequency of exploits, exploitability impacts, and amendment and authentication levels. The values are then combined into one final score [28].

Security of intelligent electronic devices (IED) calculates susceptibility to each known threat given its countermeasures. The values for each threat are combined into single final score [29].

Critical Vulnerability Analysis Scale Ratings (CVASR) by SANS institute is based on collecting security data using questionnaires [30]. The data are then processed to produce a final 3-level ranking of the potential security threat.

Weakest link security is a popular industrial methodology to evaluate the system security.

There are many other user-defined security metrics such as **Mean-Time-To-Problem-Report** (MTTPR), **Mean-Time-To–Problem-Correction** (MTTPC), problem exposure rates, problem correction rates, problem exploits rates, and so on. The security metrics and the underlying measurements are currently the most active areas of research among all other metrics.

4.5. Robustness and resilience metrics

Robustness is ability of a network to withstand failures, that is, it is a level of **fault tolerance**. For broadband networks, it often means the ability to reroute traffic in case of topology changes or congested links. In general, robustness is achieved by an appropriate network design to create topology having a rich connectivity, and by traffic engineering to utilize this connectivity effectively. The failures can be occasional and random, or targeted and at large scale. For large scale attacks, one may consider the network **survivability**. The most common type of failure dynamics are cascading failures and over-loading attacks. The ability of a network to recover from these adverse events can be quantified by **quality of recovery** (QoR) as an indication of the outage duration.

Resilience is ability of a network to provide the acceptable level of service despite failures. The failures here are either structural related to interactions of the network components or functional which is related to dysfunction of components. The network resilience is intended to be a long-term measure whereas robustness is concerned with short-term conditions. Interestingly, self-organization and autonomy of networks increase the network complexity but also their vulnerability, so their robustness and resilience decrease. Hence, the network robustness and resilience can be also used to infer the level of the network security.

In general, the broadband networks are designed to deliver the desired QoS, and more recently also QoE, and their robustness and resilience are addressed as a subsequent issue. Many resilience metrics are based on the graph-theoretic measures of networks [31]:

- **Node connectivity** is either the smallest number of paths between any two nodes, or the smallest number of nodes whose removal will disconnect the network.
- **Average neighbor connectivity** is the average degree of neighbors of a k-degree node.
- **Heterogeneity** is a measure of robustness of the network topology.
- **Average node degree** is another measure of robustness of the network topology.
- **Symmetry ratio** is a measure of the network functionality response to various attacks.
- **Clustering coefficient** is a measure of the network density as the number of triplets.
- **Average hop-count** is the average shortest paths between all pairs of nodes.
- **Radius** is the length of the shortest path among all shortest paths in the network.
- **Closeness** is measure of node centrality as the mean distance from node to all other nodes.
- **Betweenness** is defined as the number of the shortest paths through a node or a link.
- **Diameter** is the longest of all the shortest paths between all pairs of nodes.
- **Average shortest path length** (ASPL) is the average of all the shortest paths between all node pairs.

- **Algebraic connectivity** is the maximum number of node or link failures a network can tolerate before it becomes disconnected.
- **Natural connectivity** is the redundancy of alternative paths.
- **Weighted spectrum** can be used to identify geographically vulnerable links and nodes.
- **Network criticality** is the surviving ability of the network against topology changes.
- **Effective graph resistance** depends on the presence and quality of backup paths between a given pair of nodes.
- **Path diversity** is the number of disjoint alternative paths between two communicating nodes.
- **Assortativity coefficient** is the correlation of the node degrees.

It should be noted that these graph-based metrics assume a static topology, which may not be the case even for fixed broadband networks, particularly with dynamic route assignment, function virtualization, and slicing of resources.

5. Big data and machine learning metrics

Management of complex heterogeneous telecommunication networks utilizing advanced techniques such as virtualization and network slicing requires more sophisticated strategies to devise the appropriate metrics. The key objective is to automate decision-making in real-time supported by a deluge of data. The big data requires machine learning to enable data analytics. Big data are sourced from many different sub-systems into a common data pool to produce insights which can be utilized by whoever stakeholders need them. Big data is also an enabler of **deep learning**, the most powerful machine learning strategy developed so far. Deep learning is particularly effective for tasks which are difficult to clearly define such as security auditing, business analytics, predicting faults, revenue maximization, configuration and performance optimization, and other. The models of telecommunication networks in machine learning tasks are not explicitly defined, but they are learned and evolve through in-flow of data. Ultimately, the network can forecast faults and correct them before they occur, making the broadband network completely self-healing. Another appealing application is the network self-configuration to optimize the performance and utilization of resources.

The popular **5V's** measures for big data are:

- **Data volume** is the amount of data generated per a unit of time.
- **Data velocity** is the speed at which the data are being generated and moved around.
- **Data variety** refers to different sources and types of data.
- **Data veracity** is a level of trustworthiness of data.
- **Data value** is the potential monetary or other valuation of data.

In most tasks, the machine learning algorithms perform prediction from previously learned cases. The quality of these predictions can be evaluated using these metrics:

- **Estimator variance and bias, mean squared error, and scoring function** are the average measures of the estimator quality, provided that the estimator is being used repeatedly.
- **Classification metrics** evaluate loss, score, and utility functions. For instance, **accuracy score** measures the proportion of correct identifications.
- **Binary classification metrics** are usually concerned with false-positives (false alarm, type I error) and false-negatives (type II error). There is usually a trade-off between these two types of error, that is, improving one will deteriorate the other and vice versa. **Sensitivity** (probability of detection) is the proportion of correctly identified positive outcomes whereas **specificity** is the proportion of correctly identified negative outcomes.
- **Regression metrics** measure the performance of regression algorithms such as **mean absolute error**, and **r2 score**.
- **Clustering metrics** measure the performance of clustering algorithms. In particular, they measure whether the clustering defines separations of data similar to some ground truth such that members belonging to the same class are more similar than members of different classes assuming some **similarity metric**.
- **Distance metrics** measure the distances of objects. However, the true distance metrics such as the Euclidean norm must satisfy certain basic properties, which is not always the case.
- **Kernels** are measures of similarity of objects. They are less restrictive, that is, more general, than the distance metrics.

A good overview of various machine learning algorithms with the corresponding performance metrics can be found in the documentation for the Python machine learning library *scikit-learn* [32].

In general, the most powerful machine learning algorithms such as deep learning do not provide justification or explanation for their outcomes. Hence, the network operators are left in the dark to either trust these algorithms or reject their decisions. A partial remedy to this problem is to visualize and evaluate the intermediate outcomes of these algorithms. Development of reliable machine learning algorithms which are provably trustable is a subject of very active research. It is possible that the designers will need to use some machine learning algorithms to validate other machine learning algorithms and their decisions, preferably in real-time.

6. Discussion

In this chapter, we reviewed many different metrics how to evaluate the technical and business performance of broadband networks and the associated technologies. It is clear that the subject of metrics and sensing for the next generation broadband networks has become rather complex. The situation further complicates that broadband networks are a backbone of the digital economy, and that the broadband networks can now rarely be considered separately form the underlying and overlaying technologies. Even though many metrics have been proposed in the literature, only some of them are used much more frequently than the others, so they can be considered de-facto standards. The actual standardization of metrics is mainly driven by large industry consortia. The digital platforms in a production (users-facing) environment require to define and maintain thousands of various metrics which is a managing challenge beyond the resources available even at large university laboratories.

The most active areas of research on metrics for broadband networks and other systems are:

- The digital transformation of broadband networks and CSPs is happening fast. The legacy metrics are often insufficient while new metrics are being introduced at unprecedented speed. The systems and processes are needed for the management of thousands of metrics including maintenance, validation, updating, defining reference values, and so on.
- The broadband network design and management is transiting from the QoS-based metrics to the QoE-based metrics to better align the performance objectives with a customer-centric focus.
- The next generation networks will exploit advanced techniques such as virtualization, softwarization, and network slicing for the maximum flexibility. Furthermore, the mobile broadband access and heterogeneous nature of the next generation broadband networks will require new metrics and management strategies. The traditionally used metrics must be updated to remain relevant, since the underlying assumptions of their use have changed.
- There are a few complete security frameworks while many researchers are proposing their own security metrics to quantify the vulnerabilities and security risks of systems. With better availability of data on threats and vulnerabilities, a set of established simpler security metrics can be expected, for example, as it occurred with the QoS metrics.
- Machine learning algorithms are very powerful, and are being trialed for automated management of broadband networks, and even customer interactions and management. However, the concern is that machine learning algorithms do not justify or explain their outcomes. Active research is ongoing to develop machine learning algorithms which can indicate how their decisions were reached.
- More generally, there is also a need for high performance processing systems for big data analytics.

Author details

Salman M. Al-Shehri[1], Pavel Loskot[1]*, Tolga Numanoğlu[2] and Mehmet Mert[2]

*Address all correspondence to: p.loskot@swan.ac.uk

1 College of Engineering, Swansea University, Swansea, United Kingdom

2 Communications and IT Division, Aselsan A.S., Ankara, Turkey

References

[1] Digital transformation initiative: telecommunication industry [white paper]. World Economic Forum; 2017. 44 p

[2] TM Forum. https://www.tmforum.org/

[3] IT key metrics data. 2017: executive summary. Gartner. URL: https://www.gartner.com

[4] Al-Shehri SM, Loskot P, Numanoğlu T, Mert M. Common metrics for telecommunication networks. Technical Report. June 2016. 65 p

[5] Eusgeld I, Freiling FC, Reussner R, editors. Dependability Metrics. Lecture Notes in Computer Science, Springer; 2008. 300 p. ISBN: 978-3-540-68947-8

[6] TM Forum. Frameworx. https://www.tmforum.org/tm-forum-frameworx/

[7] Google. Google Cloud Platform Monitoring. https://cloud.google.com/monitoring/api/metrics

[8] Burby J, Brown A, WAA Standards Committee. Web Analytics Definitions. 2007. 34 p. https://www.digitalanalyticsassociation.org

[9] Zachman JA. A framework for information systems architecture. IBM Systems Journal. 1987;**26**(3):276-292. DOI: 10.1147/sj.263.0276

[10] OECD. Measuring the Digital Economy: a New Perspective. OECD Publishing; 2014. 161 p. DOI: 10.1787/9789264221796-en

[11] OECD. Workshop on broadband metrics. Summary of Recommendations. London, June 2012. 88 p

[12] Loskot P, Hassanien MA, Farjady F, Doran N, Payne DB, Ruffini M, Nesset D, Seton J. Long-term socio-economical drivers of traffic in next generation broadband networks. Annals of Telecommunications. 2015;**70**(1-2):10 p. DOI: 10.1007/s12243-014-0424-9

[13] Sundaresan S, Donato W, Feamster N, Teixeira R, Crawford S, Pescapè A. Measuring home broadband performance. Communications of the ACM. 2012;**55**(11):100-109. DOI: 10.1145/2366316.2366337

[14] Ofcom. UK Home broadband performance: A consumer summary of fixed-line broadband performance provided to residential consumers. Research Report. 2016. 18 p

[15] Ofcom. Measuring mobile broadband performance in the UK. Research Document. 2015. 66 p

[16] FCC. Measuring broadband America. Fixed broadband report. Technical Report and Appendix. 2016. 78 p

[17] Li K, Xu X, Swamy MNS. Modelling and analysis of regional service behavior properties of mobile internet applications. IEEE Access. 2017;**5**:4795-4807. DOI: 10.1109/ACCESS.2017.2684135

[18] Ofcom. UK Home broadband performance: The performance of fixed-line broadband delivered to UK residential consumers. Research Report. 2017. 82 p

[19] Lehr W, Smith-Grieco T, Woo GR. Broadband metrics best practices: Review and assessment. Technical Report. 2008. 89 p

[20] Samknows. UK Broadband Availability. https://www.samknows.com/

[21] Sandvine. Identifying and measuring internet traffic: Techniques and considerations. White Paper. 2015. 20 p

[22] Sandvine. Internet traffic classification. White Paper. 2015. 17 p

[23] Jain R, Chiu D, Hawe W. A quantitative measure of fairness and discrimination for resource allocation in shared systems. Technical Report. DEC-TR-301. 1984. 38 p

[24] Mell P, Scarfone K, Romanovsky S. A Complete Guide to the Common Vulnerability Scoring System Version 2.0 [Report]. NIST; 2007. 23 p

[25] Tupper M, Zincir-Heywood AN. VEA-Bility Security Metric: A Network Security Analysis Tool. In: Proceedings of ARES, Barcelona, Spain; 2008: 8 p. DOI: 10.1109/ARES.2008.138

[26] Suh-Lee C, Jo J. Quantifying security risk by measuring network risk conditions. In: Proceedings of ICIS, Las Vegas, USA; 2015. 6 p. DOI: 10.1109/ICIS.2015.7166562

[27] Singh UK, Joshi C. Quantifying security risk by critical network vulnerabilities assessment. International Journal of Computer Applications. 2016;**156**(13):26-33. DOI: 10.5120/ijca2016912426

[28] Premaratne U, Samarabandu J, Sidhu T, Beresh R, Tan JC. Security analysis and auditing of IEC61850-based automated substations. IEEE Transactions on Power Delivery. 2010;**25**(4):2346-2355. DOI: 10.1109/TPWRD.2010.2043122

[29] Anbalagan P, Vouk M. An empirical study of security problem reports in Linux distributions. In: Proceedings of ESEM, Florida, USA; 2009:481-484. DOI: 10.1109/ESEM.2009.5315985

[30] SANS Institute. Implementing a vulnerability management process. Technical Report. 2013. 24 p

[31] Cholda P, Mykkeltveit A, Helvik BE, Wittner O, Jajszczyk A. A survey of resilience differentiation frameworks in communication networks. IEEE Communication Surveys and Tutorials. 2007;**9**(4):32-55. DOI: 10.1109/COMST.2007.4444749

[32] Scikit-learn. Python machine learning library documentation. http://scikit-learn.org/stable/