

User Group Behavioural Pattern in a Cellular Mobile Network for 5G Use-cases

Gábor Soós, Dániel Ficzer, Pál Varga
Dept. of Telecommunications and Media Informatics
Budapest University of Technology and Economics
Budapest, Hungary
{soos, ficzer, pvarga}@tmit.bme.hu

Abstract—When it comes to user needs, 3G and 4G cellular mobile systems cover the mass needs for mobile broadband quite successfully. Answering the demands of critical IoT (Internet of Things), and mass IoT application users – beside lifting mobile broadband to the next level – remains the challenge for 5G. While generic, high level targets for KPIs are widely communicated, it is not yet well-understood how the various demands can affect the traffic mixture. Both the radio- and the core-domains of the cellular network have to cope with traffic peaks, and have to obey various QoS (Quality of Service) guarantees. In order to do this, traffic-related characteristics should be determined, and this knowledge should be used during network planning, optimization and service shaping.

This paper aims to provide insights to user behavioral patterns for these three key application areas: mobile broadband, critical IoT and mass IoT. Since traffic volume- and burst-related user behaviour is not expected to change suddenly, current, targeted data collection on 4G links would provide a good basic insight for future, 5G usage – at least as traffic patterns. We collected live 4G network data then analyzed throughout this paper in order to show traffic patterns – and their distinguishing features – for the three key 5G application areas.

Keywords—Communication Systems, Cellular Mobile Network, Internet of Things, Cybersecurity, Digital Twin, User profiling, 5G

I. INTRODUCTION

Along the rapid development of mobile networks, devices and use-cases, the need for information in general is also rising. In 2015 the average [1] data need on a 2G and 3G [2] network was around 1 GB per month, however in 2022 on 4G [3] and possible 5G [4] network this will be approximately 8 GB per month. This significant difference does not mean that users utilize the same applications more often, but the general user needs changed during the years. The higher data volume results in interactive applications getting more popular where users require faster response. It is the service providers' (SP) major interest to know their users' behavior and main properties. First, to gain more in general, secondly, to build higher functioning, more reliable network and provide higher user experience. SPs compete with each other every year to get the best rating from independent organizations which are measuring network performance and user experience. These methods are also developing, nowadays these are very complex measurements,

where technical parameters take into consideration less and less and in favour to user experience as the key factor.

It is clear that a different network architecture is effective for massive file-download (FTP/torrent) than for a IP based voice call or text based communication based on over the top (OTT) application. In case of the next generation networks the different user requirements could be served with prompt and dedicated responses by the cellular networks, and also the architecture and standards shall be suitable to fulfill these requirements.

In the beginning, Erlang was the metric reflecting the wired circuit-switched (voice) networks' transmission capability. This actually means how many parallel calls can be handled by a certain connection or transmission technology or media. In data networks, latency and throughput are similar key measurement parameters, which are typically given in 'ms' and 'Mbps'. However, in future 5G networks data transmission needs will be more diversified [5]. To measure new use-cases' main characteristics such as eMBB (enhanced Mobile Broadband), critical IoT and massive IoT, new metrics will be needed. To find these new metrics the first step should be to properly examine current, pre-5G use-cases. For SPs, a further crucial question is to serve the hunger for more devices and more data. Therefore network development directions shall be well aimed.

In order to support better understanding of the context, the next chapter discusses relevant traffic analysis methods, afterwards the subscriber grouping and clusterization of the three 5G use-cases are shown. In section IV, based on an arbitrary chosen method we show the differences of the use-cases focusing on deep packet analysis. In section V we describe these traffic patterns with mathematical formulas and show one possible future use-case effect regarding the traffic. Section VI concludes the paper.

II. ANALYZING USER-TRAFFIC GROUPS

In order to properly plan cellular data network services [6] and to dimension required size of a serving system it is necessary to know the possible users and to define their most relevant parameters [7]. The parameters can be the required average or peak data throughput or the latency of data

transmissions, others can be based on higher level requirements that are related to more complex applications.

It is almost impossible to understand these needs well on the individual level, but with a group of users the analysis can be very effective. The SPs main interest was always to serve first the interactive services and in the background the less critical ones. As OTT (Over-the-top) services expanded and competition generated, eventually it had begun to use ports for non-critical applications which should have higher priority, such as OTT providers' image transfer on the HTTP port. However, there are cases where best-effort traffic are treated as critical ones. Typical examples are sending bank ID numbers with short message service, or voice over data traffic. Furthermore, there are a lot of different possibilities how to measure the user groups – one of the easiest method is to counter the transmitted data, or it can be based on Deep Packet Inspection (DPI) where even the application of the group is measured individually. Based on the complexity of measurement, the results can be represented on detailed timelines. The methodologies are discussed in the following subsections. The different type of analysis methods are summarized in Table I, where we show the basis of recognition, with examples about the strengths and weaknesses of the used methodology.

A. Data traffic

Measuring the transmitted data of a users' group for a couple days with arbitrary resolution [8]. Transmitted amount of data can be measured at the packet core or at the connecting IP routers to the user's groups. The measurement results shall be the same as the Call Data Record files originating from the mobile packed core 'Ga' interface [9].

B. Recognition based on standard ports

Some applications' server work with fixed ports which are specified by international standardization organizations such as IANA [10]. Based on the standardized recommendations, different applications traffic can be easily separated. For example, HTTP for 80, HTTPS for 443, FTP for port 21 or the extremely popular P2P applications with for port 6346-6347. However, many newer applications do not have own, dedicated ports. Thanks to the rapid development of applications, ports allocation organizations can not always or can not fully properly track these changes. Application developers have a free choice on what ports they want to use for their application, they can freely decide to use the 80 and 443 ports for a peer to peer (P2P) application or starting HTTP services on port 21. In many cases new applications use unpublished protocols with a port which is used for a whole other purpose compared to the standard. Port-based traffic content recognition give us just a general picture from the actual content categories, however it can be extremely effective. From other aspect, in a closed group communication the used port of an application or the actual role is not important, nevertheless the size and frequency of the messages are more significant aspects. It means also that

the L4 protocol-based application detection is only usable for scaling the type of communication. To measure this is more than easy: from any part of the mobile packet core or connecting IP network, we can get individual IP or group level information, by well known monitoring services such as NetFlow [11].

C. File extension type

In case the traffic is not encrypted, the transmitted traffic content can be recognized. One method for that is to recognize the HTTP field, and there the name of the file. It can be read from the extension what kind of file is that without any problem. In Table I we show some easily recognizable image and application file types. The process is similar in case of video files or other kind of applications, as well.

D. Deep Packet Inspection

As we see, port based recognition is ambiguous. To identify an application based on traffic, it is needed to examine and search unique fields in the higher layers of OSI model; this methodology is often called as Deep Packet Inspection (DPI) [12]. An example for this method is recognizing HTTP SYN and SYN_ACK messages, or FTP port commands. Knowing the most popular protocols, traffic can be examined not only based on ports, more examining packets' header or a couple bytes of the traffic applications can be recognized also, even though they operate on other ports.

E. DPI with machine learning

It is hard to deal with the rapid development and fast change of applications. Often some social media application use different protocol and used ports depend on used versions or language of customer application. In this case manually configured static DPI recognition is not effective at all. With the help of machine learning the success rate can be increased [13]. With machine learning the already known marks of the applications can be improved by using the standards as a basic and using adaptive algorithm to recognize applications from network traffic. The success rate can be increased with generated application traffic, after teaching and giving feedback to the algorithm via labeling the traffic with known applications' IDs.

F. Statistical analysis

In most cases nowadays, the end-to-end data transmission layer is encrypted, hence content identification is getting a really tough task. Above the IP layer all data content looks like randomly filled bits, therefore any port or DPI based recognition is impossible. Only from source and destination IP addresses and timing or other behaviour patterns of the transmitted data can the traffic can be identified. Naturally this method also can be supported by machine learning to increase precision.

TABLE I
TYPE OF USER BEHAVIOURAL ANALYSIS

Type	Basics of recognition	What to recognize	Unknown and bad recognition
Data only	IP packet data	only the size of transmitted data	no details about traffic type
Port based	standards of IANA	HTTP(S), FTP, Telnet, ssh, some p2p	not standardized protocol usage
File extension type	file/video/program name open database	exe, bat, jpg, gif, png, txt, 3gpp, mpeg, mp4, stream, javascript, json	if URL not contains extension
DPI	standardized applications even on non standardized ports	HTTP(S), FTP, Telnet, ssh, some p2p	when the application is not standardized
DPI with Machine Learning	applications based on closed protocols	skype, facebook, viber, p2p	in case of fast changing applications
Statistical analysis	behaviour analysis	applications inside encrypted traffic	in case of changing applications
With the help of OTT	IP address, port, protocol IDs	OTTs sharing protocols with SP	OTTs not sharing protocol type

G. Recognition with help of OTT

From all recognition methods this is the most accurate one, where the OTT application developer gives the exact details and parameters for the application to the SP. This could be a simple IP-based recognition, when the destination IP address and port pool of the servers will define the application traffic. Naturally these can not be fully open in case of P2P connections, or when the application should be controlled within some kind of data center group. In other cases the OTT developers share the exact protocol description with the SP. Then the provider is able to detect the presence of the OTT application precisely, without knowing the IP pool of servers or ports. The advantage of this method is to detect even P2P traffic between subscribers. However it is necessary to frequently exchange information between the SP and OTT, and also the legal contracts with national regulation shall support this, as well.

III. USER GROUPS FOR THE USE-CASES

Currently most cellular networks' benchmarks are based on voice services and peak data traffic throughput [14]. This approach is reasonable, since it does not matter which inner elements of the network are processing and routing which users' data. The main point is to accomplish the transmission uniformly for every user, and to transport data as fast as the serving network elements can [15]. The three main use-cases of 5G networks (eMBB, cIoT and mMTC) [16] [17] [18] need more distinct radio and core network resources. Microservices and slicing [19] are big promises to offer elastic services for user needs. To be prepared for this challenge, existing user traffic in 4G networks shall be separated to the distinct service needs and treats to create more user-group specific description.

In our previous work [20] we classified users based on their content nature into three categories. These categories already exist on 4G networks, as some kind of forerunner of future 5G use-cases. Massive Broad Band – or as many 5G article refers to it, enhanced Mobile Broad Band – is where users' main interest high up- and downlink speed. The second one is the Massive Internet of Things (mIoT) scenario, where lots of devices would like to connect and transmit at the same time. The last one, to transmit messages under a critical period of time is the Critical Internet of Things (cIoT) scenario.

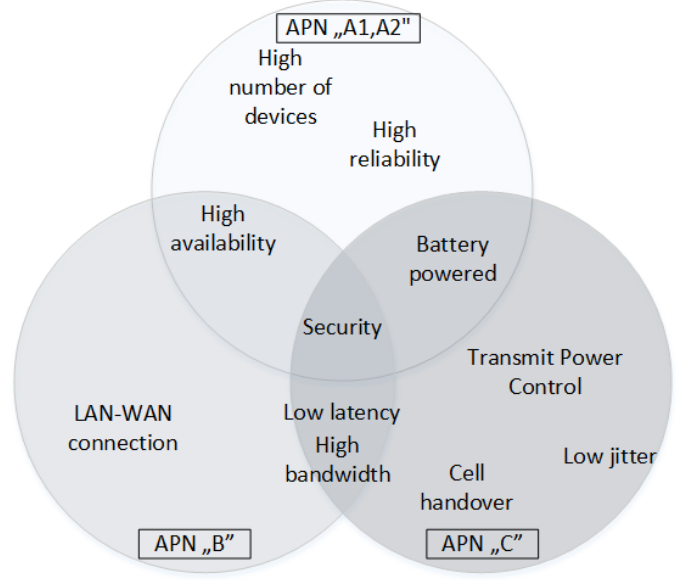


Fig. 1. Mapping 5G Use-case characteristics to APN traffic scenarios (marking some distinguishing features in this diagram)

We described through 10 different features (see Figure 1) to which group a certain use-case belong to, and then identified these groupings within a live mobile network, where the subscription were bought by a service partner, because their main interest are these kind of use-cases. With the help of Access Point Names (APNs), we examined these well-defined user groups without their individual user identification.

Although the exact borders of the three APNs can not be drawn exactly, the distinguishing features shown by Figure 1 are more than enough for our examination.

Nevertheless, strictly speaking, these forecast 5G use-cases are not existing in current 4G networks; there are only groups with similar purpose can be found.

Parts of the following brief description of APN scenarios are from our previous work [20].

1) *M2M communication*: APN A1 and A2 serves mainly Machine to Machine type communication. These are the forerunners of critical or massive IoT type use-cases. There are lot of subscriptions, with very-low-cost devices. The

main business-case for the owners of such APNs are companies working with sensors of public services, or alarm devices of houses and cars. The UEs send keep-alive messages regularly, asking for status update in a planned interval to one or more central server.

2) *More subscribers behind Cellular routers*: APN B is a network segment connected by cellular routers [21]. Companies or individuals using these subscriptions to utilize one connection to the SP and then via network address translation (NAT) connect more local users via cable or wifi. Main use-cases include surfing (web), communicating (e.g., facebook, skype) or watching online videos (e.g., youtube). The owner of these subscriptions can use IP data tunneling between end subscriptions and centralized servers. Here the data consumers are mainly humans, but the operator of the devices connecting to a cellular network can be a company, not allowing the unnecessary reboot cycles.

3) *Smartphone*: APN C is utilized by average cellular mobile subscribers: mainly smartphones, USB sticks used by humans. These customers are also called mass-market. SPs are selling for anyone entering to a customer representative shop.

In our previous work [20] we presented that mobile network users' behaviour can be measured and it is rewarding to examine the effect to the signalling network of mobile networks. It can be seen even from the most simple Peak to Mean (PMR) counters, that the three APN types affected the mobile network differently. These results have been confirmed with further analysis as well.

Still, it is clear that end-user behaviour does not only affect the signalling part of network. Currently, mobile networks could become loaded most likely due to the high volume of users' data. Data traffic measurements almost never examine users separately, not even in groups – which was right for this point –, but in 5G there are cases, when examining user traffic guarantees is a necessity: think of slicing. This also means that the analysis carried out in our previous work [20] with signalling, is worth to repeat with user traffic.

The analysis of user data transmission and the categorization of users is quite a challenge. Necessarily, there are highly detailed measurements and even protocol layer examination shall be required.

Users' behaviour is mostly measured on time segments, meaning how many and what type of signal or data transmission are generated during a period of time. Similarly, it can be determined how many and which kind of ports have been used. The mixture of the above mentioned application identification methods should be applied for a highly-performing, reasonably accurate solution.

IV. RESULTS OF THE MEASUREMENTS

Cellular networks are planned to serve the subscribers data transmission needs [14]. Therefore the most important parameter to know on a daily or monthly basis, is the required transmission of data. Our measurements took place

on four APNs in few randomly chosen days. Afterwards, we calculated the average of these days.

All traffic graphs from 2 to 5 show one day of traffic, where the time line resolution is 5 minutes. Table II shows the aggregated results of the different user groups on the well known traffic describing values [22] data as Peak To Mean Ratio (PMR), Squared Coefficient of Variation (SCV), skewness and the average user throughput in user level. One of the main differences can be seen at the PMR values, where the IoT based user groups shows significantly higher loads than the other groups, where the users are probably humans. It is worth to mention that APNs which are probably used by humans, have negative skewness, however, machine used APNs such as A1 and A2, have positive skewness. Beside the main statistical data, we presented the user number, up- and downlink average traffic as well, on Figures 2 – 5. Our diagrams provide some explanation regarding when and why are some significant diversion experienced between the different applications' traffic.

TABLE II
BASIC COMPARISON OF THE APN DATA TRAFFIC CHARACTERISTICS
(DOWNLOAD TO UE/UPLOAD FROM UE)

APN	"A1"	"A2"	"B"	"C"
PMR	24.2/2.85	2.24/1.76	1.44/2.02	1.56/1.62
SCV	2.93/ 0.0487	0.00618/ 0.00266	0.226/0.321	0.179/0.219
Skewness	10.7/5.34	13.7/11.6	-1.02/-0.555	-0.727/-0.556
Average user throughput [kbps]	3.28e-4/ 2.76e-4	0.00257/ 0.00334	98.4/14.4	15.7/1.35

In Figure 2, the number of connected users are shown with straight line, commented as "nr session curr". The number of connected users are almost constant for the whole period of the examined time; it was around 33200. However, transmitted traffic had notable bursts: there are 3 high peaks on the uplink and downlink traffic. The aggregated group level average transmission speed is around 9-10 kbps with 100-260 kbps during the high peaks. These high traffic time periods will result in very high PMR values, up to 24.

Regarding IoT traffic we chose one more user group, the APN "A2", and found similar characteristics. Measurement results are shown in Figure 3. The number of subscribers during the measurement was closely constant around 7300. User group A1 and A2 show different transmission rate characteristics. APN "A1" had more than one traffic peak, and between the peaks the data rate was very low. At APN "A2", there is only one high data throughput peak and then the traffic is almost constant. The reason of this phenomena could probably be that the connecting IoT devices synchronize to the central server, besides that, only keep-alive messages are sent by these subscribers with random distribution. The value of the PMR in case of APN "A2" is only 2, which requires significantly more steady traffic handling service from the network.

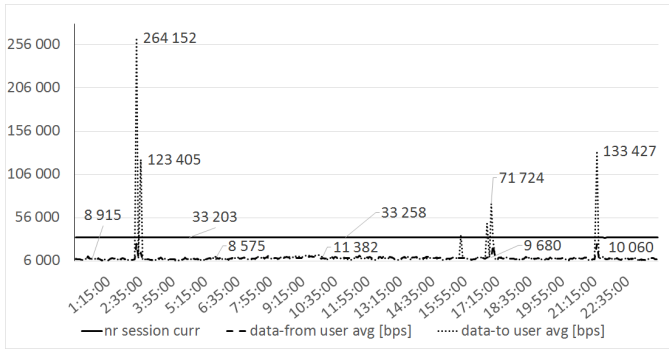


Fig. 2. Number of sessions and data transmission of APN "A1"

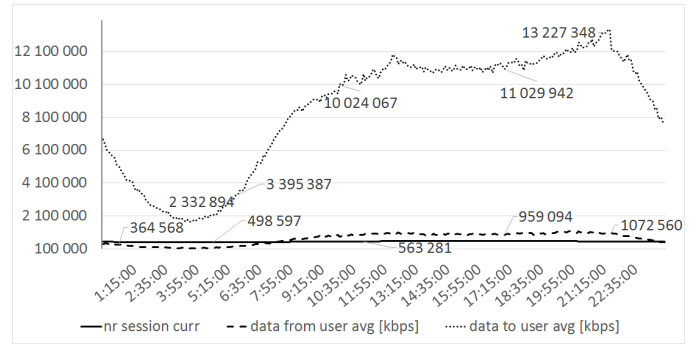


Fig. 5. Number of sessions and data transmission of APN "C"

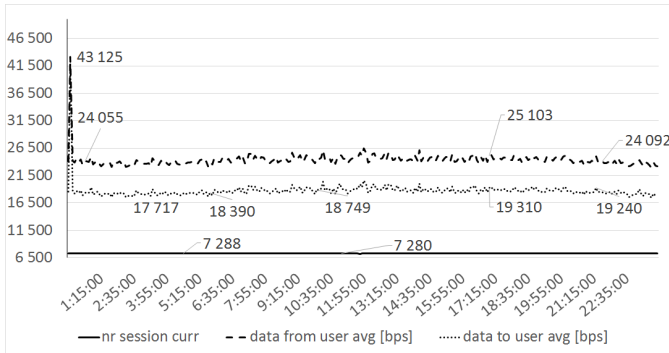


Fig. 3. Number of sessions and data transmission of APN "A2"

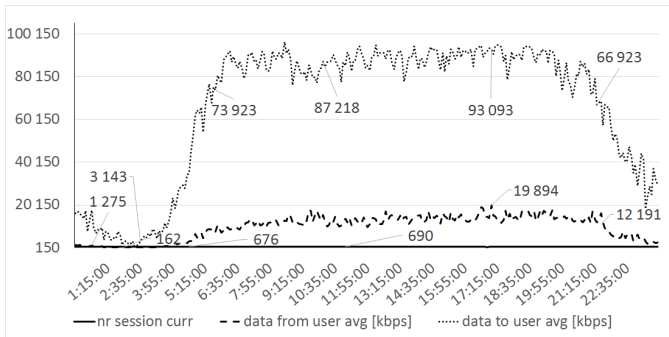


Fig. 4. Number of sessions and data transmission of APN "B"

Figure 4 presents the number of subscribers and average data throughput of user group "B" with 5 minute resolution during one day. The number of connected subscribers was quite constant – around 680 –, while the average throughput changed dynamically during the day. From 21:00 in the evening to 5:00 in the morning the traffic is relatively low, but outside this time frame we can see some huge traffic. It is interesting that maybe the traffic has some upper limit. The PMR ratio here is very low, the traffic is balanced, probably it is shaped in busy-hours.

APN "C" marks the general users who generate traffic with smartphones or USB sticks. In Figure 5 the number of corresponding users is also constant during the measurement period, but the curve describing their data transmission has a

well known shape [23]. The PMR value is relatively low, there are no rapid high peaks or drastically high transmission values. Other mentioned feature is the average transmitted data per subscriber, which is not the highest from the APN "C". On APN "B" probably there are multiple actual active users behind one subscription, so they generate more data.

Our initial assumption has been confirmed during this analysis: it is important to identify when and how much are the users transmit data, not just the magnitude of that.

A. Service usage characteristics

Simple statistical methods and diagrams about the data transmission on APNs can be valuable and clarify some issues about data traffic characteristics. In order to understand users' behaviour and model their APNs, we run server destination-port based traffic content recognition with sampling. At first, 10 second samples, with 20 second pause on every user-group for one day period. With the help of netflow and openflow protocols, we make queries to which port on the server was opened and closed and how many times during our measurement. For example one of the simplest scenario is when a user generates DNS queries, therefore the counter of 53 ports was generated by one user. Results of the measurement are depicted by Figure 6, which has some unexpected results.

The measurement results have shown that not only the impact of different user characteristics on the data transmission and signaling system is distinct, but also, unexpectedly, other ports are used, so other services are also likely to be used. Taking these features into account, we can say that bringing these services closer to the customer – either physically or at service level – will result in a better customer experience and better service. Figure 6 shows a special feature of APN "A1", where the used ports on the server side is almost uniformly distributed. All of the different ports handle nearly 12% of connections. This is probably a server-side solution of sharing the load with different clients opening different ports. The APN "A2" has a different characteristics. It is clear that the clients are mainly using port 5001, since the rest of the ports are getting negligible requests. For APN "B", port 67, 0 and 44772 receives high traffic. Port 67 based on IANA

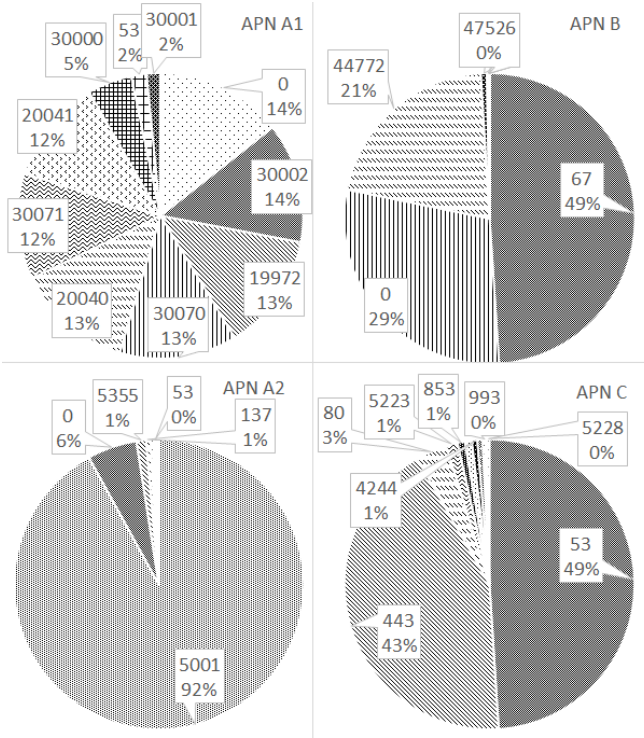


Fig. 6. Used port number/usage ratio[%] on APNs "A1,A2,B,C"

standards is typically used for DHCP request, while port 0 is used for some other application. Surprisingly, for APN "C", port 53 opening and closing was one of the most common thing. This typically means a DNS query. Since this is an open-to-use APN, this is understandable. The second, 443, probably covers HTTPS queries.

We have to mention that the interpretation of these results are based on IANA public port description and it can be misleading, however we are not quite interested in the exact application type, rather on the characteristics of the traffic.

V. NETWORK LOAD FORECAST

Regarding our user group level model, we used the results of the measurement. We determined their grouping depending on what traffic demand they showed as the function of the time variable. It has been found during the function creation that "smoother" traffic, such as the distribution of APN "B" and "C" can be approximated by polynomial functions, but equations of at least 5 dimensions are recommended [24]. In contrast, for APNs "A1" and "A2", traffic can only be approximated by more complex functions. For our current measurements, the polynomial functions approximating the data traffic of APN "B" and "C" are shown in Table III where "x" is selected as a unit of the 5 minute measurement period and calculated for 500 and 500k concurrent users, respectively.

The APN "A1" and "A2", which represent mainly IoT traffic, are described by a quasi-constant function which must be supplemented by a logical formula. Although this

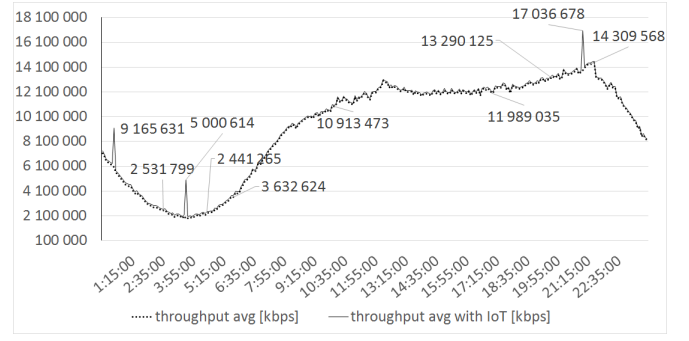


Fig. 7. Data transmission of APN "C" with forecasted IoT traffic

formula is unable to describe the high data transmission peak periods, we introduced a logical function. The goal here was to represent the randomly additional traffic. Therefore we checked the graphs of APN "A1" and "A2", and found that in case of APN "A1", in every 100 measurement period there is one high peak with additional 2.5 Gbps data rate and in case of APN "A2", in every 200 measurement period there is an additional 22000 kbps load. The formula is based on a random number that can take any value between 0 and 100 or 200 in case of APN "A2". In case the random value is equals with 1, the traffic calculated with the function shall be supplemented with the high peak data as written. In all other cases of the random number, this supplement is 0.

TABLE III
CURVE FITTING FOR APN TRAFFIC (DOWNLOAD TO UE)

APN	f(x)=	peak load of IoT
A1	$-0.0013x^3 + 0.693x^2 - 113,6x + 15645$	$\text{rand}(1;100)*2.5*10^6$
A2	$-0.0007x^3 + 0.256x^2 - 24.77x + 24792$	$\text{rand}(1;200)*22000$
B	$3.54*10^{-8}x^6 - 3.42*10^{-5}x^5 + 0.0126x^4 - 2.202x^3 + 179x^2 - 4909x + 38482$	-
C	$-2.49*10^{-6}x^6 + 1.74*10^{-3}x^5 - 0.386x^4 + 15.75x^3 + 3969x^2 - 313406x + 8*10^6$	-

Based on the use-case projection, the formulas have been used to determine what traffic characteristics and peaks to expect, when there will be about 10 times as many IoT devices as there are the current smartphone subscribers. The comparison of the results with the current average traffic is shown in Figure 7. As this figure shows from the quasi-random extra traffic, IoT devices can randomly generate high traffic peaks, even when the network is in busy-hour load. This can put an extra strain on the entire service chain, from the radio, through the packet core to the destination IP network. This may even create secondary effects such as traffic congestion anywhere, which can cause further fluctuations in unexpected transients.

All in all, it is basically almost irrelevant for mobile networks what type of traffic and when they transfer, but the load shall be as balanced as possible. Network components

are generally scaled to meet peak traffic demands. However, it can be concluded from the measurements that equipment that generates random rush hours may require extra planning. Instead of investing into extra capacity, it would be better to have a standardized solution from the network side to indicate towards the users when the network load is low, that is, when network resources are easier to access. This could basically be part of different resource reservation auctions [25] [26].

VI. CONCLUSION

The three main use-cases of 5G networks are based on the needs of civilian and industrial use-cases. The eMBB use-case as a broadband connection, together with cIoT and mIoT that are targeted for IoT scenarios, are already partly available on the current 4G and also on 2G and 3G networks. If we observe the features and traffic demand characteristics of the current end-devices, we can infer the needs of mass-marketed devices in the future. Knowing this will enable us to provide better and more reliable services. The devices connect to the cellular network via signaling and data plane; these will become a bit more separated in the future to serve better the user demands. The effect of different types of users on mobile network signaling has already been investigated in our previous article and now we have compared data usage and distribution characteristics of different user groups. Based on the results, we have determined which use-case may have larger impact on the network, and then illustrated these threats through future examples.

Our results include applying polynomial functions to the data transfer curves obtained through some examples to determine the extreme loads to be expected in future use cases. In addition to data transfer, we examined with Deep Packet Inspection what major server-side services they use, which can be an important parameter in the design of a microservice-based 5G network.

Based on the results we suggest to define standard ways on how these quasi-random, but significant load peaks could be effectively handled within the 5G network functions.

ACKNOWLEDGEMENTS

Many thanks to Ákos Sonkoly, Dorottya Balogh and Rebeka Hordós for review comments and their valuable suggestions regarding ways to improve this paper.

REFERENCES

- [1] Ericsson. Future Mobile Data Usage and Traffic Growth. [Online]. Available: <https://www.ericsson.com/en/mobility-report/future-mobile-data-usage-and-traffic-growth>
- [2] 3GPP. Technical Specifications and Technical Reports for a UTRAN-based 3GPP System. [Online]. Available: <https://www.3gpp.org/specifications/releases/77-release-1999>
- [3] 3GPP TS 21.101. (2008-12) Technical Specifications and Technical Reports for a UTRAN-based 3GPP system.
- [4] 3GPP. 3GPP 5G Briefing for Evaluation Groups. [Online]. Available: https://www.3gpp.org/news-events/3gpp-news/1987-imt2020_workshop
- [5] P. Rost, C. Mannweiler, D. S. Michalopoulos, C. Sartori, V. Sciancalepore, N. Sastry, O. Holland, S. Tayade, B. Han, D. Bega, D. Aziz, and H. Bakker, "Network Slicing to Enable Scalability and Flexibility in 5G Mobile Networks," *IEEE Communications Magazine*, vol. 55, no. 5, pp. 72–79, May 2017.
- [6] D. Kozma, G. Soós, and P. Varga, "Supporting LTE Network and Service Management through Session Data Record Analysis," *Infocommunications Journal*, vol. 71, no. 2, pp. 11–16, 2016.
- [7] M. Needham and J. Harris, "Traffic and Network Modeling for Next Generation Applications," in *2008 IEEE International Symposium on Broadband Multimedia Systems and Broadcasting*, March 2008, pp. 1–18.
- [8] M. Slanina, L. Klozar, and S. Hanus, "Practical Measurement of Data Throughput in LTE Network Depending on Physical Layer Parameters," in *2014 24th International Conference Radioelektronika*. IEEE, 2014, pp. 1–4.
- [9] 3GPP TS 32.295, "Charging Management; Charging Data Record (CDR) Transfer," 3rd Generation Partnership Project, Version 15, 2008-06.
- [10] IANA. Service Name and Transport Protocol Port Number Registry. [Online]. Available: <https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml>
- [11] Cisco, "NetFlow 9 - Technical Support and Documentation," Cisco IOS NetFlow, 2019.
- [12] X. Lu, W. Cao, X. Huang, F. Huang, L. he, W. Yang, S. Wang, X. Zhang, and C. Hongsong, "A Real Implementation of DPI in 3G Network," 12 2010, pp. 1–5.
- [13] B. Yang and D. Liu, "Research on Network Traffic Identification based on Machine Learning and Deep Packet Inspection," in *2019 IEEE 3rd Information Technology, Networking, Electronic and Automation Control Conference (ITNEC)*, March 2019, pp. 1887–1891.
- [14] W. Sun, D. Miao, X. Qin, and G. Wei, "Characterizing User Mobility from the View of 4G Cellular Network," in *2016 17th IEEE International Conference on Mobile Data Management (MDM)*, vol. 1, June 2016, pp. 34–39.
- [15] M. Laner, P. Svoboda, S. Schwarz, and M. Rupp, "Users in Cells: A Data Traffic Analysis," in *2012 IEEE Wireless Communications and Networking Conference (WCNC)*, April 2012, pp. 3063–3068.
- [16] Q. Zhang and F. H. Fitzek, "Mission Critical IoT Communication in 5G," in *Future Access Enablers of Ubiquitous and Intelligent Infrastructures*. Springer, 2015, pp. 35–41.
- [17] J. Du, L. Zhao, X. Chu, F. R. Yu, J. Feng, and I. Chih-Lin, "Enabling Low-Latency Applications in LTE-A based Mixed Fog/Cloud Computing Systems," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 2, pp. 1757–1771, 2018.
- [18] M. Condoluci, R. Trivisonno, T. Mahmoodi, and X. An, "mIoT Connectivity Solutions for Enhanced 5G Systems," in *2018 IEEE International Conference on Communications (ICC)*, May 2018, pp. 1–7.
- [19] T. Taleb, B. Mada, M. Corici, A. Nakao, and H. Flinck, "PERMIT: Network Slicing for Personalized 5G Mobile Telecommunications," *IEEE Communications Magazine*, vol. 55, no. 5, pp. 88–93, May 2017.
- [20] G. Soós, F. N. Janky, and P. Varga, "Distinguishing 5G IoT Use-Cases through Analyzing Signaling Traffic Characteristics," in *2019 42nd International Conference on Telecommunications and Signal Processing (TSP)*, July 2019, pp. 562–565.
- [21] H. Matsue, S. Kubota, H. Hojo, K. Watanabe, T. Saito, S. Aikawa, and A. Sato, "Future Systems and Technologies for Broadband Wireless Access Services," 11 2003, pp. 156 – 157.
- [22] A. Adas, "Traffic Models in Broadband Networks," *IEEE Communications Magazine*, vol. 35, no. 7, pp. 82–89, July 1997.
- [23] Nan E, Xiaoli Chu, Weisi Guo, and Jie Zhang, "User Data Traffic Analysis for 3G Cellular Networks," in *2013 8th International Conference on Communications and Networking in China (CHINACOM)*, Aug 2013, pp. 468–472.
- [24] H. Yang and S. S. Lam, "Real-Time Verification of Network Properties Using Atomic Predicates," in *2013 21st IEEE International Conference on Network Protocols (ICNP)*, Oct 2013, pp. 1–11.
- [25] M. Jiang, M. Condoluci, and T. Mahmoodi, "Network slicing in 5G: An Auction-based Model," in *2017 IEEE International Conference on Communications (ICC)*, May 2017, pp. 1–6.
- [26] L. Liang, Y. Wu, G. Feng, X. Jian, and Y. Jia, "Online Auction-Based Resource Allocation for Service-Oriented Network Slicing," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 8, pp. 8063–8074, Aug 2019.