2022 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works. The definitive version of this paper has been published in NOMS 2022-2022 IEEE/IFIP Network Operations and Management Symposium, 25-29 April 2022 , 10.1109/NOMS54207.2022.9789901.]

Data Usage in IoT: A Characterization of GTP Tunnels in M2M Mobile Networks

Simon Raffeck*, Stefan Geissler*, Michael Krolikowski‡, Steffen Gebert‡, Tobias Hoßfeld*
*Chair of Communication Networks, University of Würzburg, Germany
Email: {firstname.lastname}@informatik.uni-wuerzburg.de
‡EMnify GmbH, Germany
Email: {firstname.lastname}@emnify.com

***Abstract*—Internet of Things (IoT) and Machine-to-Machine (M2M) devices have seen a significant growth in usage and deployment over the last years. Gaining insight into device and data usage behavior exhibited by the participants of mobile networks is elementary for Mobile Network Operator (MNO) and Mobile Virtual Network Operator (MVNO) to scale their networks and provide a reliable service. This work aims to make use of its first of a kind dataset, spanning multiple countries and MNOs, to provide a detailed characterization of GPRS Tunneling Protocol (GTP) tunnels and devices. To this end, general statistics are used to describe the observed data traffic focusing on the distribution of the tunnel duration and volume as well as periodic device behavior. An approximate metric is introduced to analyze the periodicity and synchronicity of IoT devices. Lastly, we publish the data investigated in this work and provide a large scale dataset on the data usage behavior of IoT devices to interested researchers.**

***Index Terms*—dataset, data analysis, mobile network, Internet of Things (IoT), GPRS Tunneling Protocol (GTP)**

I. Introduction

The IoT and M2M environments in general have seen impressive growth over the last years. Similarly, the number of different verticals and use cases has grown substantially and this increase in devices is expected to continue over the next decade [1]. To provide these new, heterogeneous devices with reliable, global network connectivity, a new type of IoT-focused mobile operators has emerged. Operating in the form of MVNOs, these operators leverage the dense infrastructure MNOs have been building over the years to provide global connectivity through international roaming.

This interconnection of globally distributed devices via the Radio Access Network (RAN) and core components of a multitude of MNOs, poses several challenges for operators. Ensuring system resiliency, proper network dimensioning, or the detection of anomalous or malicious devices are critical but challenging problems, especially, since MVNOs only control their own core network and are depending on functions provided by other operators.

In this context, understanding the behavior of this heterogeneous fleet of IoT devices is crucial for successful network operation. Establishing a baseline for the behavior of devices enables operators to identify misbehaving devices and develop accurate models of expected traffic and therefore system load. However, the traffic generated by IoT devices differs from conventional mobile network usage patterns [2]. These traffic patterns, however, are crucial regarding the operation of IoT-focused networks.

978-1-6654-0601-7/22/$31.00 © 2022 IEEE

To this end, we provide a first step towards understanding the data usage behavior of a large number of IoT devices in mobile networks. We present a characterization of a large scale dataset obtained at the ingress of an MVNO core network, where we monitored the establishment and destruction events of data tunnels in the a global 2G/3G deployment as well as the total amount of data exchanged in both receive and transmit direction over these tunnels. Our dataset contains tunnel data over 30 days in October 2021 and encompasses more than 500 000 unique devices that establish over 155 million data tunnels. We characterize the full set of observed tunnels regarding their data volume and duration. Further, we show that the time synchronous behavior of some devices leads to peaks in the creation of new tunnels and introduce an approximation for the periodicity of devices that allows the identification of these time synchronous devices.

The remainder of this paper is structured as follows. Related work is listed and discussed in Section II. Afterwards in Section III the system and network used to capture the data is introduced alongside a brief overview of the dataset itself. A short presentation of the captured data and its characteristics is given in Section IV. For a more detailed perspective, the innate behavior of the GTP tunnels is further analyzed in Section V. Afterwards, in Section VI the device behavior itself is investigated in more detail, with a focus on periodicity of the observed nodes. Lastly, in Section VII the observations and studies are brought together and conclusions are drawn.

II. Related Work

Related work in this area has a variety of focus points. Classification and characterization of IoT devices and traffic modeling are the two main fields of research, and while both have been investigated in a number of related works, these often lack a detailed and large scale dataset with a multitude of MNOs and global networks, limiting their applicability to real world scenarios.

Characterization of data plane traffic in M2M environments is investigated in [3], [4], however the datasets used are limited, either in scale or granularity or stem from emulated

traffic [5]. Further classification and characterization mechanisms concentrate on IoT devices using Wireless Local Area Network (WLAN) [6], [7] or on communication networks in general [8]. Signaling traffic is investigated on a comparable dataset in [9], however neglecting the data traffic. In [10] the authors provide a characterization of traffic patterns obtained from IoT networks and study the Poisson approximation for IoT traffic. Further traffic models for IoT networks are presented in [11] and for M2M traffic in [12]. To the best of our knowledge, this is the first large scale dataset containing real world data on the data usage behavior of IoT devices.

III. System Architecture and Dataset Description

The dataset discussed in this work has been obtained by monitoring the GTP create and delete events responsible for managing data tunnels in 2G/3G environments. The data has then been augmented with the total volume of data received and transmitted in each observed tunnel. For confidentiality reasons, specific details on the contents of the traffic are made unavailable.

Figure 1 shows a simplified structure of the system in which the dataset has been monitored. On the left, devices connect to the RAN of operators all over the world from where they perform inbound mobile roaming towards the home network on the right. The Serving GPRS Support Node (SGSN) and Gateway GPRS Support Node (GGSN) act as the two central components when it comes to establishing data tunnels. In between, dedicated signaling carriers transmit signaling messages between visited and home networks. As the specific signaling procedures are not instrumental to the contributions made in this work, we will omit details at this point. A more detailed description of the system as well as the roaming procedures can be found in [9].

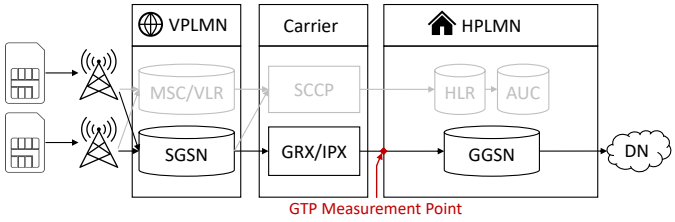


Figure 1: Schematic representation of the system architecture in which the data has been obtained.

Based on the information available at the GGSN, we obtain an extensive dataset containing one whole month of create and delete events as well as the total, received, and transmitted volume of devices. Table I shows the key characteristics of the dataset. We obtained data tunnel related events and volume values over 30 days in October 2021. In total, we observed over 500 000 unique devices and 150 million individual data tunnels. The dataset evaluated in this work was obtained in close cooperation with a global MVNO and contains information on the creation and destruction of GTP tunnels as performed by a large fleet of IoT devices from various verticals. The exact use cases of specific devices are unfortunately not available. The fields included in the dataset are briefly summarized in Table II.

The endpoint_id is a unique, anonymized identifier that allows the tracking of a single device over the total trace duration. time_create and time_delete provide timestamps for the creation and destruction of tunnels. The precision of these timestamps is one second. Hence, there exist a number of tunnels with duration 0, meaning that the duration was lower than one second (cf. Figure 6). The volume simply describes the amount of payload data that was sent and transmitted during the duration of the respective data tunnel in Megabyte.

Table I: Key characteristics of the dataset.

Scope			
Timeframe	1. Oct. to 31. Oct. 2021		
No. of Unique Devices	$> 500\,000$		
No. of Data Tunnels	$> 150\,000\,000$		
Key Parameters			
	Mean	Std.	Median
Tunnel Duration [s]	4183	32139	66
Tunnel Volume [MB]	0.2	51.3	0.0012
Tunnel TX [MB]	0.054	7.27	0.0006
Tunnel RX [MB]	0.146	50.1	0.0004

Table II: Fields contained in the dataset.

Datafield	Description	Format
endpoint_id	Anonymized identifier for specific devices. One device keeps the same identifier over the whole trace duration	string
time_create	Timestamp for tunnel creation in seconds	datetime
time_delete	Timestamp for tunnel destruction in seconds	datetime
duration	Tunnel duration in seconds	numeric
volume	Total transmitted data volume (RX + TX) in Megabyte	numeric
volume_rx	Received data volume in Megabyte	numeric
volume_tx	Transmitted data volume in Megabyte	numeric

In this work, we examine the duration and volume of tunnels in both upstream and downstream directions. The table shows the mean, standard deviation and median for each of the parameters. The values immediately show the large range of values for all four metrics with coefficients of variation of up to 343 for the received volume. Further, in all cases the median is significantly smaller than the mean, highlighting the existence of extreme outliers on the high end. Interestingly, the mean suggests that devices, receive more data than they transmit. However, the median suggests otherwise. This is further investigated in Section V.

Note that due to the large number of devices present in the system over the monitoring duration and due to confidentiality reasons, we only provide a sample of 500 000 devices. We believe, however, that even the reduced dataset is of great value to the community. Hence, we provide a subset of the data discussed in this paper to interested researchers. The dataset is provided as open access via the Zenodo platform and can be downloaded from there [13].

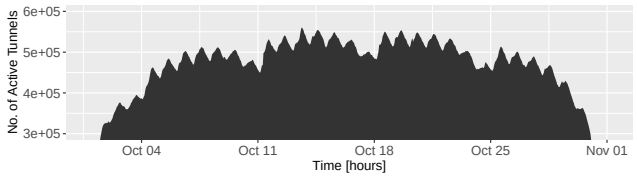


Figure 2: Number of active GTP tunnels over time.

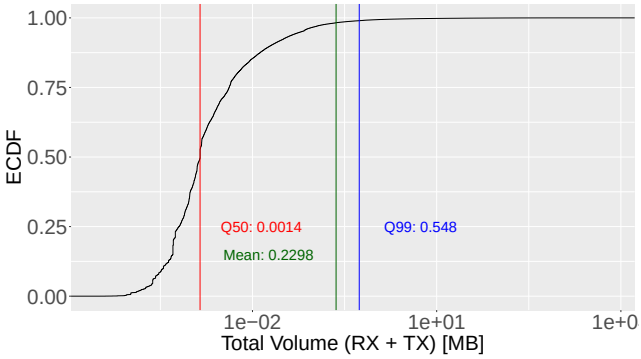


Figure 3: ECDF of total data volume (RX + TX) transmitted over GTP tunnels.

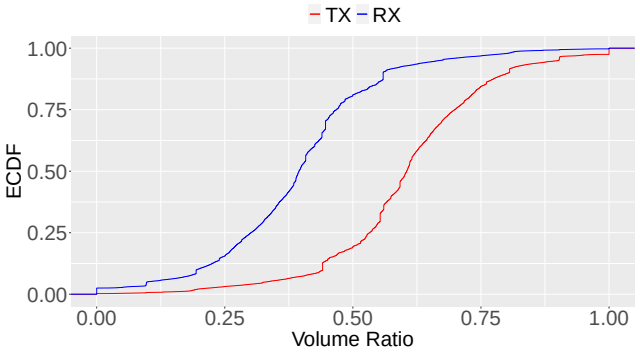


Figure 4: ECDF of ratio RX/Volume and TX/Volume over GTP tunnels.

IV. Dataset Overview

To analyze the behavior of devices and GTP tunnels, the dataset is investigated on a general level in this section. Firstly, the amount of opened tunnels throughout the observed timespan is looked into, and their behavior over the recorded days is described.

Figure 2 illustrates the number of active tunnels over the time in hours during the month of October, with the number of active GTP tunnels in 100 000 on the y-axis. The peaks presented by the figure indicate the individual days. Weekdays, Monday to Friday, exhibit a larger number of active tunnels than Saturday and Sunday. Furthermore, the midday peaks are indicative of a day-night cycle in the device behavior.

To further investigate the data usage of the devices, the Empirical Cumulative Distribution Function (ECDF) of the total data volume of all tunnels is shown in Figure 3. As indicated by the red line 50% of all tunnels report a data volume of less than 0.0014 MB. Additionally, the 90%-quantile of GTP tunnels exhibits 0.548 MB of rx- and tx-data volume usage. The mean over all tunnels is at 0.023 MB.

A more detailed look into the volume and the influence of RX and TX on its composition is given in Figure 4 as a ECDF of the RX and TX percentage of the total volume over all tunnels. The blue line represents the downlink traffic and the red line the uplink. As anticipated all tunnels exhibit more uplink traffic than downlink, with 50% of all tunnels contributing 39.48% for downlink and 60.52% for uplink of the total volume.

V. Tunnel Characteristics

To fully understand the GTP tunnel characteristics recorded within the dataset, a close look into distinctive features exhibited by the tunnels is taken. To begin, the tunnel duration is analyzed and used to classify the connections into representative groups. Figure 5 depicts the ECDF of how long a GTP tunnel was open in seconds. The tunnel duration ranges from 0 s up to 2 656 966 s, with the x-axis of the Figure being limited to 25 000 s for readability. The 50%-quantile is at 66 s and the 90%-quantile at 3637 s. The results are significantly different than GTP tunnel durations of human and machine generated traffic from a mobile operator, e.g., 90%-quantile at 11 094 s, see [14]. The majority of the tunnels contained in our dataset are thus open for less than an hour. These key datapoints are used to classify the tunnels into four color-coded classes:

Class 0 Tunnels opened for less than 1 s in red.
Class Q50 Tunnels open between 1 s and 66 s in blue.
Class Q90 Tunnels open between 67 s and 3637 s in yellow.
Class Q100 Tunnels opened for longer than 3637 s in green.

Class 0 is left out of the annotation in Figure 5 to maintain a more reader-friendly picture.

For a more in-depth investigation of the different classes Figure 6 illustrates the ECDF of the total data volume (solid line), the RX data volume (dotted) and the TX data volume (dashed) in MB for each of the classes, color-coded as described above. Class 0 (red) is the only class that exhibits more RX volume than TX for 50% of the tunnels. When it comes to overall volume, the classes act according to their

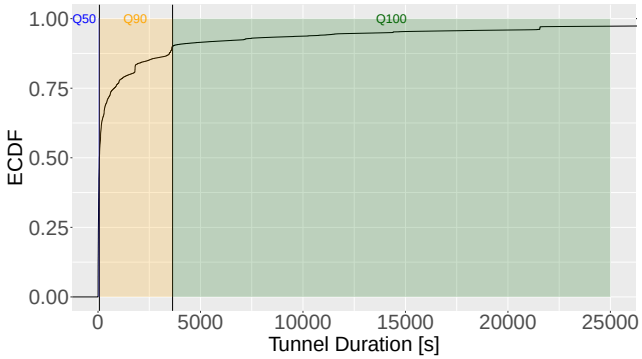


Figure 5: ECDF of the duration of GTP tunnels, with subdivision into classes

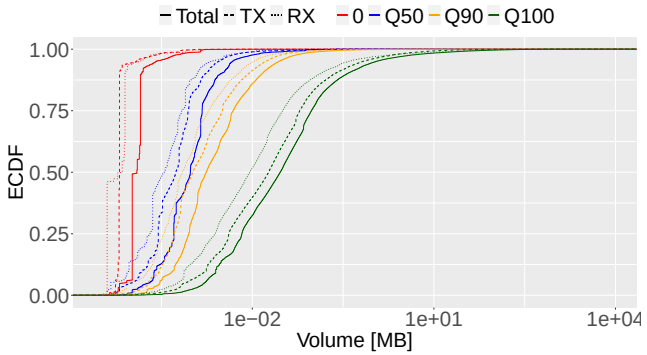


Figure 6: ECDF of total data volume, RX and TX transmitted over GTP tunnels per duration class.

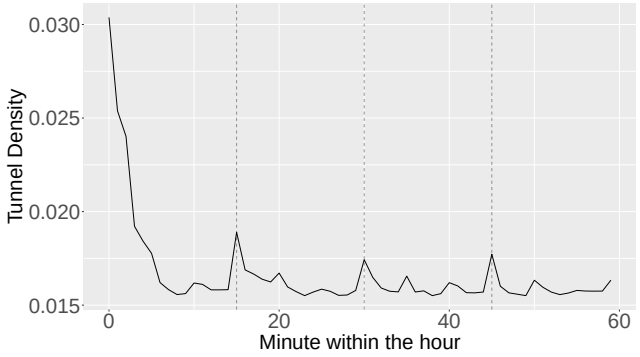
tunnel duration, exhibiting higher overall volume with larger tunnel durations. The Q50 and Q90 classes show comparable data volume values. Both these classes being relatively close together in their tunnel durations compared to the outliers of the Q100 class, this further collaborates the aforementioned correlation.

Lastly, the GTP tunnels are examined in regard to their synchronicity. To this end, the messages responsible for opening up a data connection are further analyzed. Investigating whether or not devices tend to open up GTP connections in a synchronized, and therefore bursty, manner is crucial for a deeper understanding of the system as a whole.

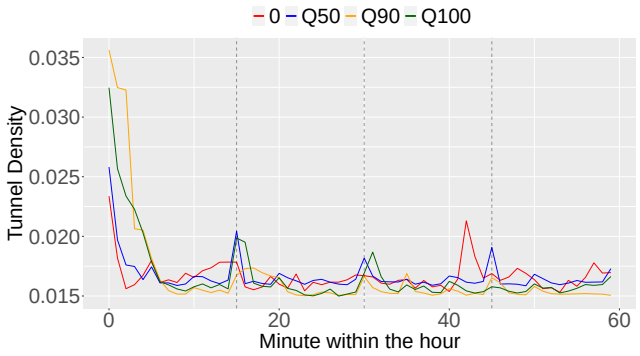
In Figure 7 the density function of the probability that a GTP tunnel is created at a specific minute within any hour is depicted. To this end, the probability that a PTP CREATE is send at a specific minute is calculated and normalized. The x-axis displays the minutes within an hour and the y-axis the probability density. The dotted vertical lines are drawn to visualize every $15\,\mathrm{min}$.

Figure 7a shows this metric over every tunnel within the dataset. The illustration shows a significant peak at the start of every hour, implying that devices will create tunnels in a bursty manner, and smaller peaks at every $15\,\mathrm{min}$ after that. Furthermore, this implies that the devices are synchronized and the interarrival times of their tunnel creation messages are not negative exponentially distributed. Non-synchronized devices exhibit memorylessness as described by the characteristics of a Poisson process and will therefore, present uniformly distributed interarrival times.

This behavior is further analyzed in Figure 7b. The tunnel creation probability density is drawn for each of the duration classes defined above and color-coded accordingly. All of the classes show the distinctive peak at the start of every hour followed by minor peaks occurring in what appears to be a $15\,\mathrm{min}$ interval. Class 0 exhibits a somewhat larger peak right before the $45\,\mathrm{min}$ mark, but the smaller amount of tunnels within this class, dampen it's effect on the overall density. It can be stated however, that the tunnel duration has no effect on the seemingly synchronized behavior shown within the observed data.



(a) Density function of PDP CREATE dialogues for the probability that tunnels are opened at a specific minute within any hour



(b) Density function of PDP CREATE dialogues for the probability that tunnels are opened at a specific minute within any hour for each duration class

Figure 7: Tunnel creation probability density per minute within any hour, gathered from the probability of a PTP CREATE.

VI. Time Synchronous Device Behavior

In this section, the device behavior is analyzed in more detail. To this end, a metric to approximate the periodicity of nodes in large datasets is introduced in Subsection VI-A. After establishing a working framework to investigate if devices are synchronized, the same approach is applied to the dataset and used to evaluate the device behavior in Subsection VI-B.

A. Degree of Periodicity in Large Datasets

In datasets like the one examined in this work, the computation of device periodicity is a complex task, as large parts of the analysis is done in Apache Spark to handle the number of data points. Due to the technical properties of the applied map-reduce mechanisms, the computation of e.g. the autocorrelation is not efficiently possible using frameworks like Apache Spark. The same is true for other approaches based on transform methods of the time series data like periodicity transform [15] searching the best periodic characterization in the dataset. The approaches in [16], [17] require Fourier transform and autocorrelation computation. [18] provides a mechanisms for periodicity detection based on convolution. [19] provides a method for detecting transmission periodicity for IoT data based on histograms and a threshold of the standard deviation of the histogram.

In this paper, we introduce a simple measure of the periodicity of time series based on histograms that can be efficiently computed in map-reduce environments. *The degree of periodicity a^* is defined as the probability of the mode of the interarrival times (IATs) of a time series.* Formally, A is a discrete random variable (RV) reflecting the IATs of a time series with distribution $a(k) = P(A = k)$ for $k = 0, 1, \ldots$. The mode m is the value that is most likely to occur. Then,

$$a^* = a(m) = P(A = m) \quad \text{with } m = \arg\max_k a(k) \; . \tag{1}$$

The assumption is that a^* is sufficient to approximate the periodicity of the underlying time series. Thereby, a value of $a^* = 1$ describes a perfectly periodic time series with only a single occurring IAT. The minimal value is assumed for a time series with uniformly distributed IATs which is $a^* = \frac{1}{n}$ for a time series of $n+1$ time stamps and n IATs. Note that we may normalize a^* accordingly: $\widehat{a} = \frac{a^* - 1/n}{1 - 1/n}$. This is however negligible for large datasets as in our case.

To show the validity of the assumption, we calculate a^* for different time series and show that its highly correlated to the Jensen-Shannon-Divergence (JSD) D_{JS} when comparing A to the IAT distribution S of a perfectly periodic time series with period m. Then, S is deterministic with $s(m) = 1$ and $s(k) = 0$ for $k \neq m$.

To this end, we introduce both the JSD as well as the Kullback-Leibler-Divergence (KLD) which the latter is based on. Both provide measures of similarity between two probability distributions. The KLD is defined as

$$D_{KL}(P, Q) = \sum_{k=0}^{\infty} p(k) \cdot \log_2 \left(\frac{p(k)}{q(k)} \right) \; , \tag{2}$$

whereas P and Q are discrete RVs with probability mass functions $p(k)$ and $q(k)$, respectively. $\log_2$ is the base 2 logarithm. Hence, D_{KL} describes the weighted sum of logarithmic differences between P and Q. Based on that, the JSD for two probability distributions is defined as

$$D_{JS}(P, Q) = \frac{1}{2} D_{KL}(P, M) + \frac{1}{2} D_{KL}(Q, M) \tag{3}$$

with $M = \frac{1}{2}(P + Q)$. The advantage of D_{JS} over D_{KL} is that the JSD is both symmetrical and bounded as $0 \leq D_{JS} \leq 1$ holds true for all P and Q. For easier comparability, we define

$$D(P, Q) = 1 - D_{JS}(P, Q) \; . \tag{4}$$

From here, we now calculate $D(S, A)$ for different distributions of A. With S being defined as mentioned above and after some algebraic transformations, D_{JS} can be simplified with the probability a^* of the mode:

$$D_{JS}(S, A) = 1 + \frac{1}{2} \left(a^* \log a^* - (1 + a^*) \log(a^* + 1) \right) \; . \tag{5}$$

Hence, $D(S, A)$ is only depending on a^* and we can simply calculate it for various values of a^*. Figure 8 shows the resulting $D(S, A)$ values against a^*. The values result in a Spearman correlation of 0.98, indicating the close approximation of our proposed a^* metric.

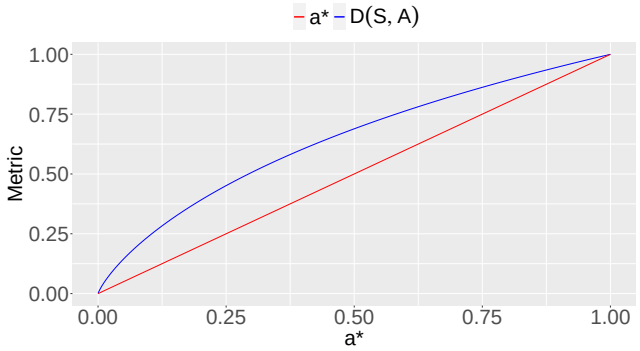


Figure 8: Comparison of a^* and $D(S, A)$.

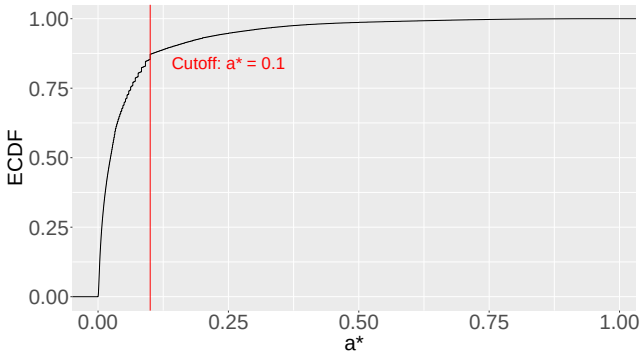


Figure 9: ECDF over a^* for all 368 787 devices with at least 10 observed tunnels.

B. Identification of Periodic Devices

We now compute a^* for the interarrival times observed for data tunnels in our dataset. Figure 9 shows the CDF over all values obtained for devices with at least 10 tunnels that have been observed over the monitoring period of 30 days. These include 368 787 devices or about 73% of the total population. The remaining 27% of devices are, due to their low activity, only responsible for 0.3% of data tunnels and are hence neglected to investigate further. Instead these devices are considered non-periodic.

The figure shows a clear cutoff point at $a^* = 0.1$. Based on this, in combination with the results already obtained for comparable data of IoT devices in [9], we assume devices with a^* values higher than the cutoff point to be periodic. Remember that the a^* value describes the relative frequency of the interarrival time observed most often for a respective device. Hence, $a^* = 0.1$ means that 10% of the observed interarrival times fall on the same value.

Finally, Figure 10 shows two exemplary devices drawn from the dataset that exhibit a large a^* value of 0.89 and a small value of 0.01, respectively. We show a zoomed in version of the first 10 minutes of the time series for each of the devices. Thereby, the figure shows an on-off-phase diagram in which active tunnels are indicated by on phases. Hence, tunnels of longer duration are shown as wider bars in the plot.

The non-periodic device shown on the top exhibits very

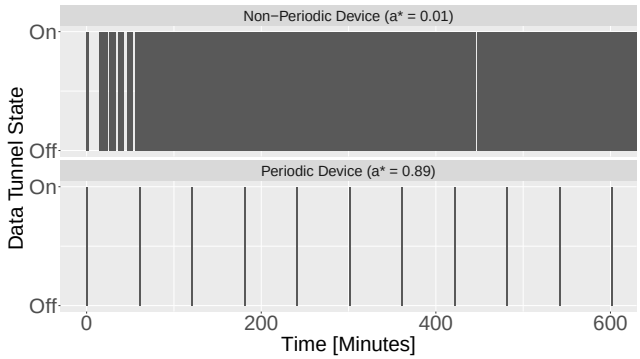


Figure 10: Time series of data tunnel activity for the first 10 minutes of two example devices from both classes with a^* values of 0.01 (non-periodic) and 0.89 (periodic)

irregular behavior with tunnel creation events having uneven spacing. In addition, the duration of tunnels varies significantly over the shown 10 minute period.

The periodic device shown in the bottom half of the figure, as opposed to before, behaves very regularly with evenly spaced tunnel creation events that show a constant interarrival time of 10 minutes. Similarly, the tunnel duration is alike for all tunnels observed in the 10 minute period. Closer inspection shows that the device deviates from an a^* metric of 1 as it starts to miss single intervals, leading to interarrival times of 20 minutes, hence reducing the degree of periodicity.

VII. Conclusion

In this work, we present a large scale dataset containing data usage information of over 500 000 IoT devices. We provide an overview of the key characteristics contained in the dataset and establish basic facts on the behavior of devices. We show the existence of a day-night cycle as well as weekend-workday differences over the full duration of the dataset. We have shown that it is possible to classify GTP tunnels by means of their duration. These classes have been further investigated and we have shown a correlation between the tunnel duration and the transmitted data volume. Furthermore, we have shown that tunnels are created in a synchronized manner, regardless of the tunnel duration. This behavior has been observed throughout all classes and leads to load spikes at specific time intervals. Specifically, devices tend to create new tunnels at every full hour and in 15 minute intervals. In order to identify these devices, we introduce an approximation of device periodicity that can be efficiently computed using Apache Spark or other map-reduce applications. We show that our approach is able to differentiate two classes of devices, periodic and non-periodic. This work provides a first insight into the data usage behavior of IoT devices. However, the numerous insights through detailed analysis of the included dataset are far from exhausted and remain for future work.

Acknowledgment

This work is funded by the Bavarian Ministry of Economics, Regional Development and Energy within the project 5CALE as part of the R&D program for information and communication technology in the field of 5G mobile communications. The authors alone are responsible for the content.

References

[1] P. Cerwall, A. Lundavall *et al.* "Ericsson mobility report". (accessed 2022-02-11). [Online]. Available: https://www.ericsson.com/4ad7e9/assets/local/reports-papers/mobility-report/documents/2021/ericsson-mobility-report-november-2021.pdf

[2] I. Cvitić, P. Zorić, T. M. Kuljanić, and M. Musa, "Analysis of network traffic features generated by iot devices," *Future*, 2021.

[3] B. Finley and A. Vesselkov, "Cellular iot traffic characterization and evolution," in *2019 IEEE 5th World Forum on Internet of Things (WF-IoT)*. IEEE, 2019, pp. 622–627.

[4] M. Z. Shafiq, L. Ji, A. X. Liu, J. Pang, and J. Wang, "A first look at cellular machine-to-machine traffic: large scale measurement and characterization," *ACM SIGMETRICS performance evaluation review*, vol. 40, no. 1, pp. 65–76, 2012.

[5] F. Malandra, S. Rochefort, P. Potvin, and B. Sansò, "A case study for m2m traffic characterization in a smart city environment," in *Proceedings of the 1st International Conference on Internet of Things and Machine Learning*, 2017, pp. 1–9.

[6] A. Sivanathan, D. Sherratt, H. H. Gharakheili, A. Radford, C. Wijenayake, A. Vishwanath, and V. Sivaraman, "Characterizing and classifying iot traffic in smart cities and campuses," in *2017 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*. IEEE, 2017, pp. 559–564.

[7] A. Sivanathan, H. H. Gharakheili, F. Loi, A. Radford, C. Wijenayake, A. Vishwanath, and V. Sivaraman, "Classifying iot devices in smart environments using network traffic characteristics," *IEEE Transactions on Mobile Computing*, vol. 18, no. 8, pp. 1745–1759, 2018.

[8] H. Tahaei, F. Afifi, A. Asemi, F. Zaki, and N. B. Anuar, "The rise of traffic classification in iot networks: A survey," *Journal of Network and Computer Applications*, vol. 154, p. 102538, 2020.

[9] S. Geissler, F. Wamser, W. Bauer, M. Krolikowski, S. Gebert, and T. Hoßfeld, "Signaling traffic in internet-of-things mobile networks," in *2021 IFIP/IEEE International Symposium on Integrated Network Management (IM)*. IEEE, 2021, pp. 452–458.

[10] T. Hoßfeld, F. Metzger, and P. E. Heegaard, "Traffic modeling for aggregated periodic iot data," in *2018 21st Conference on Innovation in Clouds, Internet and Networks and Workshops (ICIN)*. IEEE, 2018, pp. 1–8.

[11] F. Wamser, P. Tran-Gia, S. Geißler, and T. Hoßfeld, *Modeling of Traffic Flows in Internet of Things Using Renewal Approximation*. Cham: Springer International Publishing, 2019, pp. 483–492. [Online]. Available: https://doi.org/10.1007/978-3-030-34960-8_42

[12] M. Laner, P. Svoboda, N. Nikaein, and M. Rupp, "Traffic models for machine type communications," in *ISWCS 2013; The Tenth International Symposium on Wireless Communication Systems*. VDE, 2013, pp. 1–5.

[13] S. Raffeck, S. Geißler, M. Krolikowski, S. Gebert, and T. Hoßfeld, "Anonymized gtp tunnel trace in mobile iot," Feb. 2022. [Online]. Available: https://doi.org/10.5281/zenodo.6045708

[14] F. Metzger, C. Schwartz, and T. Hoßfeld, "Gtp-based load model and virtualization gain for a mobile network's ggsn," in *2014 IEEE Fifth International Conference on Communications and Electronics (ICCE)*. IEEE, 2014, pp. 206–211.

[15] W. A. Sethares and T. W. Staley, "Periodicity transforms," *IEEE transactions on Signal Processing*, vol. 47, no. 11, pp. 2953–2964, 1999.

[16] M. Vlachos, P. Yu, and V. Castelli, "On periodicity detection and structural periodic similarity," in *Proceedings of the 2005 SIAM international conference on data mining*. SIAM, 2005, pp. 449–460.

[17] T. Puech, M. Boussard, A. D'Amato, and G. Millerand, "A fully automated periodicity detection in time series," in *International Workshop on Advanced Analysis and Learning on Temporal Data*. Springer, 2019, pp. 43–54.

[18] M. G. Elfeky, W. G. Aref, and A. K. Elmagarmid, "Periodicity detection in time series databases," *IEEE Transactions on Knowledge and Data Engineering*, vol. 17, no. 7, pp. 875–887, 2005.

[19] R. Tolas, R. Portase, A. Iosif, and R. Potolea, "Periodicity detection algorithm and applications on iot data," in *2021 20th International Symposium on Parallel and Distributed Computing (ISPDC)*. IEEE, 2021, pp. 81–88.