Identification of Signaling Patterns in Mobile IoT Signaling Traffic

Viktoria Vomhoff*, Stefan Geissler*, Tobias Hossfeld*
*Chair of Communication Networks, University of Würzburg, Germany
Email: {firstname.lastname}@informatik.uni-wuerzburg.de

I. Introduction

The increasing acceptance of the Internet of Things (IoT) has made connected devices an everyday occurrence and created many application areas. The broad spectrum of verticals present in modern IoT deployments lead to an extremely heterogeneous environment. A temperature sensor has vastly different requirements in comparison to a connected car. This leads to significantly different traffic patterns within the network [1]–[3].

This, in combination with the need for global connectivity, has led to the emergence of Machine-to-Machine (M2M) focused platforms and the expected increase of the number of devices will lead to new challenges regarding the scalability, resiliency, and overall performance of all involved systems. To this end, we need to further our understanding of the behavior of IoT devices in cellular networks. Connecting these devices using networks that have been designed for human use poses several challenges. Operators have to deal with signaling traffic of a vast number of globally distributed devices whose behavior differs significantly from human generated traffic. Therefore, a good understanding of such IoT devices is essential. This includes the knowledge of traffic patterns, especially when it comes to their signaling behavior. As many devices only transmit negligible amounts of payload data, the overhead induced through mobile signaling is significant and induces significant cost for operators.

To this end, we attempt to identify sequences of signaling dialogs, to strengthen our understanding of the signaling behavior of IoT devices by examining a dataset containing over 270.000 distinct IoT devices whose signaling traffic has been observed over a 31-day period in a 2G network [4]. We propose a set of rules that allows the assembly of signaling dialogs into so-called sessions in order to identify common patterns and lay the foundation for future research in the areas of traffic modeling and anomaly detection.

II. Background

In this section the architecture of a 2G/3G network is provided and relevant core components are briefly introduced. Furthermore, we cover the signaling procedures performed by devices.

A. Network Architecture and Mobile Roaming

Unlike classic Mobile Network Operators (MNOs), Mobile Virtual Network Operators (MVNOs) operate their own core network, but no Radio Access Network (RAN). Therefore, the MVNO we get the data from, maintains roaming agreements with more than 300 MNOs worldwide to cover the whole globe. The architecture of the system evaluated in this work is shown in Figure 1. Starting on the left-hand side, exemplary IoT devices, equipped with a SIM card from the MVNO connect to the RAN of a local operator. The most important components are the Mobile Switching Center (MSC), Visitor Location Register (VLR), and Serving GPRS Support Node (SGSN). The VLR is a database located at the MSC and contains every device connected to the visited network and especially to the current MSC. While MSC and VLR are responsible for circuit switched connectivity, such as telephony and Short Message Services (SMS), the SGSN provides a similar functionality for data connectivity.

Via dedicated carrier networks, the visited network can then interact with the home network, operated by the MVNO. Here the main components are the Home Location Register (HLR), Authentication Center (AUC), and Gateway GPRS Support Node (GGSN). Similar to the visited network, the home network core components are responsible to manage authentication (HLR, AUC) as well as data connectivity management (GGSN) [5].

As indicated by the blue and red markers in Figure 1, we capture signaling interactions of both the MAP and the GTP protocol. Specifically, we capture request-response pairs, called dialogs, for authentication and mobility as well as the creation, update and deletion of data tunnels using GTP.

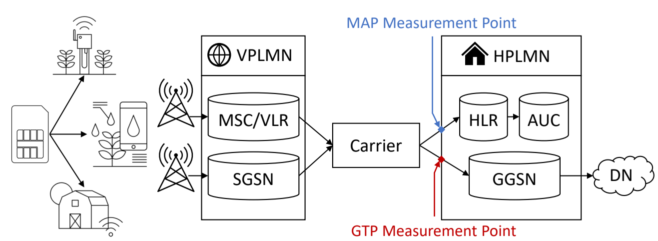

Figure 1: Network architecture overview.

B. Signaling Procedures

In order to successfully attach to a network and be able to send data, devices have to go through two separate procedures. The first procedure, called IMSI attach, is responsible for authenticating a device with the VLR and establishing connectivity for circuit switched services (telephony, SMS) [6]. The first dialog of this procedure is called Send Authentication Information (SAI). A request is sent from the VLR to the HLR in order to initiate device authentication. At the HLR the request is checked. If the device is allowed to register, a corresponding response containing one or several authentication vectors is sent. After this an Update Location (UL) dialog follows. In this dialog the location of the device is sent form the VLR to the HLR. Note that location in this context does not describe a devices geographical location, but contains information on which VLR a device is currently connected to. If a device is not newly attaching to the system, but changed the VLR, the MVNO can send a Cancel Location (CL) dialog to the old VLR and deregister the device there. After this procedure has been successful, the device is registered for telephony and SMS.

This procedure is done during initial registration, when a device moves to another location (another VLR), or may even be triggered periodically. Whether a device exhibits this periodic behavior depends on the Base Transceiver Station (BTS), a part of the RAN of the visited network.

In order to be able to send data, a second procedure, called GPRS attach, has to be performed. The process is very similar to the IMSI attach. The communication here is between the SGSN and the HLR, instead of the VLR, and the UL dialog is replaced with the Update GPRS Location (UL_GPRS) dialog. After the procedure is successful the device is allowed to open a data connection to access the Data Network (DN).

The explained dialog types all belong to the Mobile Application Part (MAP) protocol. In order to open a data tunnel the following GPRS Tunneling Protocol (GTP) dialog types are needed. The dialog exchanged between the SGSN and GGSN are Create Packet Data Protocol (PDP) Context (PDP_CREATE), Update PDP Context (PDP_UPDATE), and Delete PDP Context (PDP_DELETE). The first is to open a data tunnel, to allow the device the sending of data, the second is to update an existing tunnel, e.g. after changing the location, and the last one is to close the tunnel, e.g. after data transmission is completed.

In the following, we attempt to automatically match multiple dialogs (e.g. SAI, UL, PDP_CREATE) that occur in close temporal proximity, as explained in Section IV. We assemble such dialogs into sessions with the goal to capture the intent of devices and identify sessions that occur with higher frequency and identify devices that behave abnormally.

III. Dataset Description

The dataset used to develop the first version of our session detection algorithm is a 31-day trace from January 2020. It contains more than 270 000 devices which produce more than 600 million dialogs. For this work, we use 38 of 61 available data fields present for each dialog. Note that we are using the same dataset that has already been described in the past [7]. The most important fields for this work are shown in Table I.

The *start* and *end* columns give the unix timestamp of the first request and the last response of the corresponding dialog, respectively. The fields *calling* and *called* determine the specific VLR, SGSN, or HLR the dialog is sent to or received from and the *ci* is the cell identifier which contains the identifier from which mobile cell (i.e. base station) the dialog is received. In the *type* field, the dialog type is given, the *typeReason* gives canonical information about why this dialog type has been assigned, and the *superType* defines whether a dialog is successful, rejected, or an error. Rejected dialogs have actively been denied by the core network, e.g. devices that are not allowed to authenticate, errors encompass actual technical errors or aborted or incomplete dialogs. Furthermore, the *contextIdentifier* matches PDP dialogs to the same context, hence allows the mapping of PDP_CREATE to its corresponding PDP_DELETE. The last field is the *simId*, which is a unique identifier for the device.

Table I: Most important dataset fields in the trace.

Field	Content	MAP	GTP
start	timestamp of first request	✔	✔
end	timestamp of last response	✔	✔
countryName	country name	✔	✔
operatorName	operator name	✔	✔
calling	source VLR/SGSN of dialog	✔	✘
called	destination VLR/SGSN of dialog	✔	✘
ci	cell identifier	✘	✔
type	dialog type	✔	✔
typeReason	explanation of dialog type	✔	✔
superType	definition of whether the dialog is successful, rejected, error or unknown	✔	✔
contextIdentifier	identifier to match PDP contexts	✘	✔
simId	SIM card identifier	✔	✔

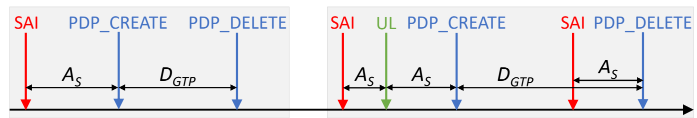

Figure 2: Schematic representation of exemplary sessions.

Throughout the dataset, different sequences of dialogs can be seen that losely correspond to the signaling procedures introduced earlier. However, not all patterns that can be observed behave exactly like the IMSI attach and GPRS attach procedures, indicating device, VLR or operator specific behavior that deviates from the standardized signaling procedures. Because of that we developed the session detection algorithm to identify sequences of dialogs, called sessions, with the goal of analyzing and comparing them to the procedures as well as identify sessions that occur regularly as well as identify outliers or even malicious devices.

IV. Session Detection Algorithm

In order to identify sessions in our dataset, multiple processing steps are performed. At first the dataset is filtered and only successful dialogs are kept in the trace. This is optional and depends on what the goal is. For now, we are just interested in seeing how devices behave in comparison to the expected procedures. However, taking erroneous dialogs into account is planned for future work. In the next step, we examine the inter arrival times between dialogs of each device, respectively. It

Table II: Extract of the session library.

Index	Session	No. of Occurences	Pct. of Occurences	Cum. Pct. of Occurences
1	PDP_CREATE PDP_DELETE	39 538 615	0.23	0.23
2	SAI	38 759 766	0.22	0.45
3	SAI PDP_CREATE PDP_DELETE	13 155 091	0.075	0.52
4	SAI SAI	10 392 775	0.059	0.58
5	UL	7 913 284	0.045	0.63
6	PDP_CREATE PDP_UPDATE PDP_DELETE	7 742 440	0.044	0.67
7	SAI SAI PDP_CREATE PDP_DELETE	7 457 510	0.043	0.72
8	PDP_CREATE SAI PDP_DELETE	5 881 758	0.034	0.75
9	SAI UL	4 207 436	0.024	0.77
10	UL_GPRS	4 097 077	0.023	0.80

can be seen that a lot of dialogs exhibit inter arrival times in the range of less than one up to a few seconds of time between each other, whereas the others show inter arrival times of many minutes or even hours. Therefore, it is assumed that some dialogs belong together in the sense that these are triggered by the same signaling intention, e.g. updating the HLR after a device has moved to a new operator. To examine this assumption we designed a session detection algorithm that matches dialogs into sessions based on the following rules. Exemplary sessions are depicted in Figure 2, as indicated by the gray boxes.

Sessions are assembled by checking each of the following rules until a currently open session is finished:

- MAP dialogs are attached to their successor if the inter arrival time A_S is smaller than 30 seconds
- The PDP_CREATE, PDP_UPDATE and PDP_DELETE dialogs of a respective PDP tunnel always belong to the same session
- A PDP_DELETE dialog always terminates the current session

Each dialog marked as a session start is then assigned a session number. As a next step, all dialogs which are not marked as a session start, are assigned to the session of the previous dialog. The result is a set of signaling sessions for each device that can in the following be analyzed to identify commonly occurring sessions.

V. Preliminary Results

In order to obtain preliminary results, the session detection algorithm is applied to the full dataset. We then count the occurence of each type of session, meaning sessions containing the same sequence of dialogs, independent of their exact inter arrival time. The resulting rates are summarized in a session library that can be seen in Table II. The table shows the top 10 most occurring sessions and includes the index of the corresponding session in the library, the session itself, the number of occurrences, and the percentage of session specific as well as cumulative occurrences.

In this evaluation, a total of 174 712 239 sessions have been identified, which are grouped into 721 565 unique session types. Out of these 721 565 unique sessions, there are 579 120 sessions which only occur once. This means that 80% of identified sessions only have a single occurrence in the dataset. On the other hand, the 10 most occurring sessions are listed in Table II. These top 10 sessions contribute 80 % of the total number of occurring sessions, so the Pareto principle is observed and needs to be further investigated. The most common session, with a percentage of 23 %, is “PDP_CREATE PDP_DELETE”, representing the establishing and closing of a data tunnel. The second most observed session is a single “SAI” with 22 %. This is particularly interesting, as a single, standalone SAI has no immediate use for both the visited network as well as the corresponding device. It merely prepares the system for future signaling dialogs, like UL or UL_GPRS.

VI. Discussion and Outlook

In order to extend our understanding of the behavior of the signaling traffic induced by IoT devices, we developed an algorithm that allows the identification of signaling sessions that encompass multiple dialogs. Due to respecting both their temporal proximity as well as their meaning in the context of mobile signaling, these sessions are assumed to represent a full signaling intention, meaning a full interaction with a specific goal. In the preliminary results presented here, we have shown that the resulting sessions contain only few dialogs and that a small fraction of unique sessions contributes the majority of total session volume. Similarly, more than 80% of sessions only occur once in the whole dataset, even when not taking into account erroneous dialogs.

With this session detection algorithm in combination with a deeper understanding of the behavior of specific devices, e.g. a source traffic model, datasets can be analyzed in more detail and regular devices can be distinguished from misconfigured or malicious devices. Furthermore, the insights gained through session detection can be used to develop model driven simulation tools. This will in the future help to conduct research without being reliant on large scale datasets through the generation of realistic signaling load based on established session libraries. In this context the session detection library is used to determine which traffic should be generated.

However, the session detection in its current form is based on assumptions that should be validated by means of investigation of additional datasets. Additionally, the threshold of 30 seconds, that is used by the algorithm, worked for our example but may need to be configured differently or dynamically for other environments or datasets. Finally, a more detailed distinction between sessions is required and correlation between sessions need to be looked at. We have seen that roughly 22% of sessions consist of a single SAI dialog that has no immediate use for the system. In order to understand why this is happening, a more detailed analysis is required. These research questions are critical in order to understand the behavior of mobile IoT devices and will provide interesting challenges in the future.

REFERENCES

[1] 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*, 2020.

[2] F. Metzger, T. Hoßfeld, A. Bauer, S. Kounev, and P. E. Heegaard, "Modeling of aggregated iot traffic and its application to an iot cloud," *Proceedings of the IEEE*, vol. 107, no. 4, pp. 679–694, 2019.

[3] M. Laner, P. Svoboda, N. Nikaein, and M. Rupp, "Traffic Models for Machine Type Communications," in *10th International Symposium on Wireless Communication Systems*. VDE, 2013.

[4] A. Lutu, B. Jun, A. Finamore, F. E. Bustamante, and D. Perino, "Where Things Roam: Uncovering Cellular IoT/M2M Connectivity," in *Internet Measurement Conference*, 2020.

[5] N. Vallina-Rodriguez, S. Sundaresan, C. Kreibich, N. Weaver, and V. Paxson, "Beyond the radio: Illuminating the higher layers of mobile networks," in *Proceedings of the 13th Annual International Conference on Mobile Systems, Applications, and Services*, 2015, pp. 375–387.

[6] A. Lutu, B. Jun, F. E. Bustamante, D. Perino, M. Bagnulo, and C. G. Bontje, "A first look at the ip exchange ecosystem," *ACM SIGCOMM Computer Communication Review*, vol. 50, no. 4, pp. 25–34, 2020.

[7] S. Geissler, F. Wamser, W. Bauer, M. Krolikowski, S. Gebert, and T. Hoßfeld, "Signaling Traffic in Internet-of-Things Mobile Networks," in *IFIP/IEEE International Symposium on Integrated Network Management*. IEEE, 2021.