Exploring the Physical-layer Identification of GSM Devices

Exploring the Physical-layer Identification of GSM Devices

Davide Zanetti
Institute of Information Security
ETH Zurich, Switzerland
zanettid@inf.ethz.ch

Vincent Lenders
armasuisse
Thun, Switzerland
vincent.lenders@armasuisse.ch

Srdjan Capkun
Institute of Information Security
ETH Zurich, Switzerland
capkuns@inf.ethz.ch

Abstract

In this work, we study the physical-layer identification of GSM devices. For our exploration, we build an ad-hoc acquisition setup that collects GSM signals during voice calls. We collect signals from a population of 18 mobile devices and build fingerprints by considering both the transient and the data parts of the acquired signals. Our results show that devices of different models and manufacturers can be identified with high accuracy (0% identification error) by exploiting transient-based fingerprints. Same model and manufacturer devices could also be identified by using transient-based fingerprints: we find an identification error between 0 and 8% depending on the considered device set. We also find that the built transient-based fingerprints are sensitive to the device transmission power, but only partially to the device position with respect to our acquisition setup antenna. This possibly enables defensive (e.g., access control) applications. Although with less accuracy with respect to transient-based fingerprints, data-based fingerprints could also be used to identify same model and manufacturer devices. However, these seem to be sensitive to the device position.

1 Introduction

In this report we present our exploration on the physical-layer identification of GSM devices. The report is organized as follows. In Section 2, we define our problem statement and provide a system overview. In Section 3, we present our acquisition setup, the performed experiments and summarize the collected data. We introduce our physical-layer identification techniques in Section 4 and present their performance results in Section 5. We discuss the obtained results in Section 6 and make an overview of the related work in Section 7. We conclude the report in Section 8.

2 System Overview and Problem Statement

The main goal of our work is to study the feasibility and the accuracy of the physical-layer identification of GSM devices.

Physical-layer device identification systems aim at identifying (or verifying the identity of) devices or their affiliation classes based on characteristics of devices that are observable from their communication at the physical layer. That is, physical-layer device identification systems acquire, process, store and compare signals generated from devices during communications with the ultimate aim of identifying (or verifying) devices or their affiliation classes.

The implication of applying physical-layer device identification techniques is twofold: they can provide additional security guarantees by enabling physical-layer-based identification (e.g., for an access

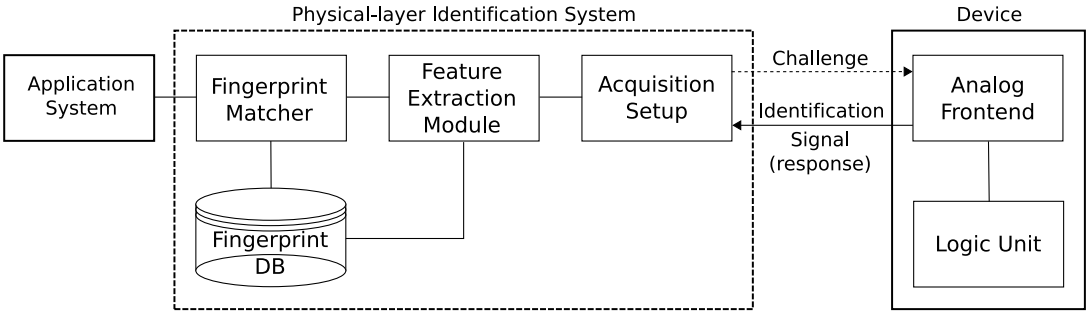


Figure 1: Entities involved in the physical-layer identification of wireless devices and their main components.

control application), but they can also invalidate privacy guarantees of protocols running at the upper layers of communication (thus enabling device tracking at the physical layer).

A physical-layer device identification system can be viewed as a pattern recognition system typically composed of (Figure 1): an acquisition setup to acquire signals from devices under identification, also referred to as *identification signals*, a feature extraction module to obtain identification-relevant information from the acquired signals, also referred to as *fingerprints*, and a fingerprint matcher for comparing fingerprints and notifying the application system requesting the identification of the comparison results. For a detailed introduction and thoughtful survey on physical-layer device identification, see Danev et al. [11].

In our study, we use a single experimental setup for the examination of device identification. Our setup consists of two main components: a signal acquisition setup (Section 3.1) and a feature extraction and matching module (Section 4). Our acquisition setup captures (Section 3.2) device signals during the communication between a GSM device and a GSM network basestation related to a voice call. Our feature extraction module then extracts specific characteristics, or *features*, from the device signals and builds device fingerprints. We explore features of both the data part and the transient part of the device signals. The considered device population is composed of different model and manufacturer devices, as well as same model and manufacturer devices (Table 2, Appendix B). we also explore several factors that may affect the device identication accuracy and therefore the applicability of our physical-layer identification techniques (e.g., for access control application and device tracking). In particular, we investigate the impact of the device position with respect to the acquisition setup and the device transmission power. We additionally evaluate the applicability of our physical-layer identification techniques by exploiting two different GSM networks, a non-controlled and a controlled (from the point of view of the entity performing the device identification) networks. The former is a local Swisscom network, while the latter an ad-hoc GSM network based on the OpenBTS project [1]. In summary, in this work we address the following questions:

1. Is it possible to identify GSM devices using physical-layer identification techniques?
2. What is the identification accuracy of our setup, within our device population?
3. What is the impact of factors like the device position wrt the acquisition setup and the device transmission power on the identification accuracy?
4. What are the implications of the proposed techniques for GSM users' privacy and on GSM security?

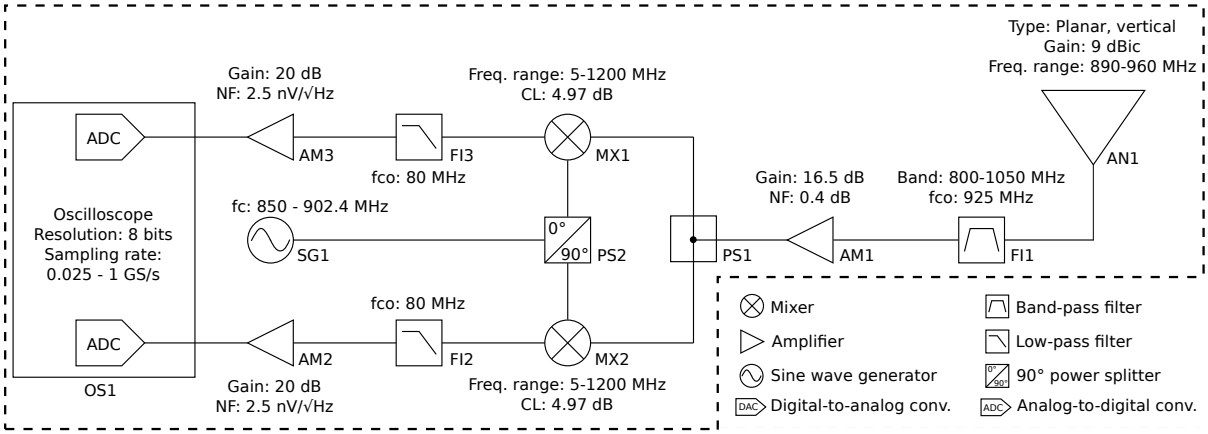


Figure 2: Block diagram of the acquisition setup.

3 Experimental Setup and Data

In this section, we first describe our signal acquisition setup. We then detail the different types of experiments we performed and present the collected datasets.

3.1 Acquisition Setup

Our acquisition setup is shown in Figure 2. It is mainly composed of a receiving antenna (directional, to better target the device under identification and limit the perturbations due to other electromagnetic emissions), a downmixing circuit to bring the device signal from the GSM carrier frequency to an intermediate frequency (IF, to reduce the necessary sampling rate during signal digitalization), and two analog to digital converters (ADC, 8-bit resolution). Each acquired signal s is stored as complex in-phase (I) and quadrature (Q) components s_I and s_Q. In our experiments, we vary both the IF and the ADC sampling rate. In order to prevent (limit) any possible signal perturbations (e.g., noise) during the signal acquisition phase, i.e., to preserve the signal characteristics then deployed in the feature extraction phase, our acquisition setup is composed of low-noise and high-quality equipment, components and cabling (listed in Table 1, Appendix A). During all our experiments, the acquisition setup antenna is placed at 1.25 m from the ground.

3.2 Performed Experiments

Our experiments are based on the interaction between a GSM device and a GSM basestation (BTS) during a voice call. More specifically, our acquisition setup collects GSM Normal Burst (NB) [13] transmitted by the GSM device under identication during a voice call. A GSM NB is used to carry voice and it is composed of 148 bits divided as follows: 6 tail bits, 114 bits of payload (the actual voice information, possibly encrypted), 26 training sequence (TS) bits and 2 stealing flag bits. In addition, a NB presents a guard period of 8.25 bits at its end. The total length of a NB is 0.577 ms. Given the 156.25 bits composing the NB, the gross bit rate is 270.833 kbps. The modulation in GSM is Gaussian Minimum Shift Keying (GMSK) [12]. Figure 3(a) shows the GSM Normal Burst (NB) structure. In our experiments, we consider both the data-related part of the Normal Burst, as well as the transient parts of it, i.e., the turn-on and turn-off transients. In particular, for the data-related part we focus on the TS bits. This was done to not introduce any data-dependent bias in our identification, since the TS is imposed by the BTS and fixed for all devices (while we do not have control on the other bits in the Normal

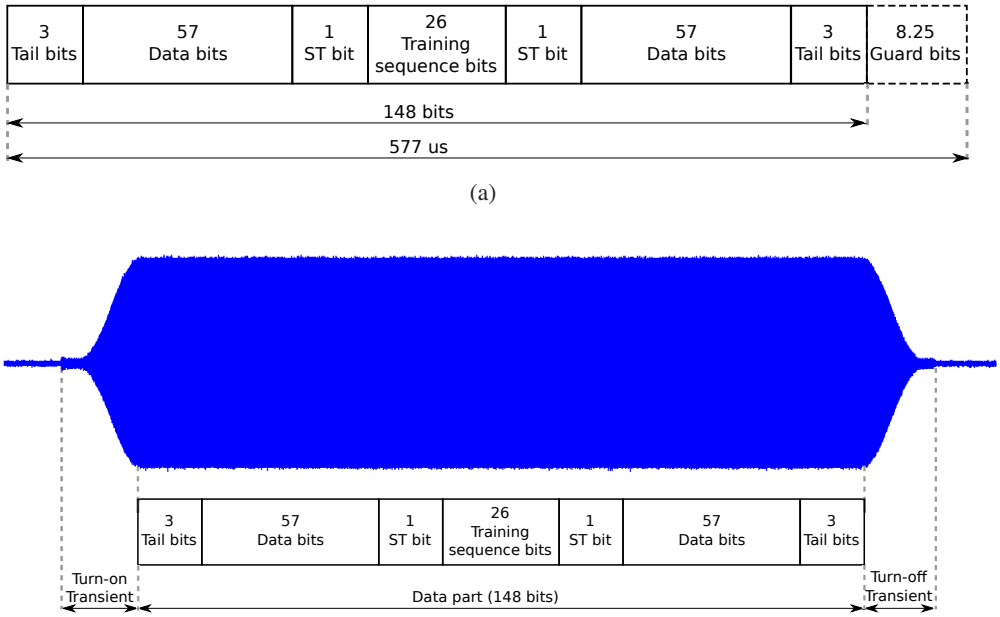


Figure 3: GSM Normal Burst: (a) data structure and (b) RF signal. ST stands for STealing flag.

Burst)[1]. Figure 3(b) shows a collected NB and its data and transient parts. The GSM specifications are available from the European Telecommunications Standards Institute (ETSI [2], the 05 Series provides the specification of the GSM physical layer). Additional references on GSM can be found in [14, 17].

In our study, we deploy two different GSM networks: a local Swisscom network and an ad-hoc GSM network based on the OpenBTS project [1]. OpenBTS provides an open-source implementation of the GSM protocol stack. The GSM air interface is built on top of a software-defined radio, while calls are connected using a SIP softswitch or PBX service. In our GSM implementation, we use an Ettus USRP (Universal Software Radio Peripheral [3]) as radio interface and Asterisk [4] as PBX service to forward calls. Figures 23(a) and 23(b) (Appendix D) show the basic blocks that compose our GSM network implementation and the actual implementation. Operating our own GSM network gives us the possibility to control some of the parameters affecting the Normal Bursts transmitted by the GSM devices under identication. In particular, the carrier frequency, the content of the training sequence and the device transmission power (all of them imposed on the devices by the GSM network). Being able to control those parameters allows us, on the one hand, to collect consistent signals, while, on the other hand, to diversify our exploration in a controlled setup.

Our device population is composed of 18 devices of 5 different models and 4 manufactures. Table 2 (Appendix B) lists the considered devices.

In our experiments, we acquire NB bursts from the devices under investigation by considering different:

- GSM networks: a local Swisscom network and our ad-hoc GSM network.
- The position of the devices with respect to the acquisition setup antenna. Figure 4 shows the considered positions.

[1]The training sequence is selected by the basestation among 8 different code sequences of 26 bits [13]. A BTS always uses the same configured TS code for all devices. Ideally, being able to control the NB data payload, i.e., the voice information, would provide a larger signal information. However, without device manipulation, it seems not practical to control the voice information.

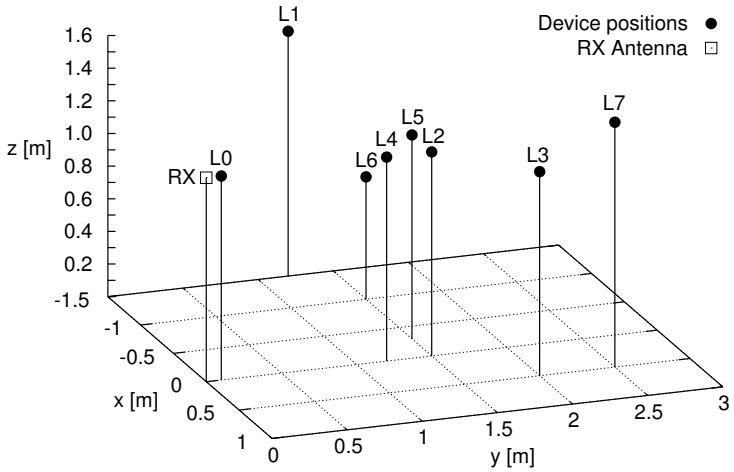


Figure 4: Considered positions of the acquisition antenna and of the GSM devices. In our experiments, the acquisition antenna (RX) is fixed, while Normal Bursts are acquired from different positions (L0-L7).

- The transmission power of the devices (when attached to our ad-hoc GSM network).
- The training sequence code (when attached to our ad-hoc GSM network).

3.3 Collected Data

Using our acquisition setup, we performed the experiments described in Section 3.2 and collected GSM Normal Bursts. In Table 4 (Appendix E), we summarize the data that we collected, represented in a form of datasets. Data collection was performed over several months, one device at the time, in an indoor, RF noisy environment with active Wi-fi and GSM networks and with other objects nearby. Unless otherwise indicated, the burst acquisitions for each device (within a dataset) are performed in a row and during the same call.

4 Feature Extraction and Matching

The goal of the fingerprinting features is to obtain distinctive fingerprints from the signals collected in the proposed experiments. Here, we detail the extraction and matching procedures of features extracted from the Normal Burst transient part (Section 4.1) and data part (Section 4.2). We define the bounds between the Normal Burst transients and data part at the beginning of the first bit for the turn-on transient, and at the end of the last bit for the turn-off transient, as shown in Figure 3. The feature extraction and matching is performed on the acquired signals in the digital domain, using MathWorks Matlab [5]. Table 3 (Appendix C) lists the signal features we consider in our exploration.

4.1 Transient-based Features

We explored 3 diffent signal features in both the turn-on s_{ON} and turn-off s_{OFF} signal transients: the instantaneous phase ϕ, the instantaneous frequency f and the signal power envelope e. With respect to the complex in-phase (I) and quadrature (Q) components s_I and s_Q of an acquired signal s, we define

them as follows:

$$\phi[n] = \begin{cases} \phi_{ON}[n] & = tan^{-1}\left(\frac{s_{Q,ON}[n]}{s_{I,ON}[n]}\right) \\ \phi_{OFF}[n] & = tan^{-1}\left(\frac{s_{Q,OFF}[n]}{s_{I,OFF}[n]}\right) \end{cases} \quad (1)$$

$$f[n] = \begin{cases} f_{ON}[n] & = \frac{\phi_{ON}[n]}{dn} \\ f_{OFF}[n] & = \frac{\phi_{OFF}[n]}{dn} \end{cases} \quad (2)$$

$$e[n] = \begin{cases} p_{ON}[n] & = |(s_{Q,ON}[n], s_{I,ON}[n])| \\ p_{OFF}[n] & = |(s_{Q,OFF}[n], s_{I,OFF}[n])| \\ e_{ON}[n] & = 10 \cdot log_{10}(10^3 \cdot p_{ON}[n]) - \ max(10 \cdot log_{10}(10^3 \cdot p_{ON}[n])) \\ e_{OFF}[n] & = 10 \cdot log_{10}(10^3 \cdot p_{OFF}[n]) - \ max(10 \cdot log_{10}(10^3 \cdot p_{OFF}[n])) \end{cases} \quad (3)$$

4.1.1 Feature Combination and Matching

For each of the defined features, we build (and evaluate) fingerprints by considering each transient as an individual signal part. Additionally, for each feature, we combine both turn-on and turn-off extracted features. For example, for the feature ϕ, we extract ϕ_{ON} and ϕ_{OFF} from the turn-on and turn-off transient respectively, as well as the combination (vector concatenation) of them; we denote this feature combination as (ϕ_{ON}, ϕ_{OFF}). For evaluation, reference and testing, device fingerprints are built from a number N of acquired Normal Bursts. Each device fingerprint F is the value of a selected feature x (e.g., ϕ_{ON}) averaged over N:

$$F_x[k] = \frac{1}{N} \cdot \sum_{i=0}^{N-1} x_i[k],\ 0 \leq k \leq L-1 \quad (4)$$

where x_i is the feature extracted from an acquired signal i and L the length of the considered signal feature x. For matching two fingerprints, i.e., computing the similarity score between reference and testing fingerprints, we used Euclidean distance.

4.2 Data-based Features

We explore 3 different features based on the phase and frequency errors of the signal data part. Phase and frequency errors are computed with respect to the *ideal* phase and frequency trajectories given a specific data (bit) pattern. We extracted signal features (fingerprints) from the fixed training sequence (TS) of the Normal Burst. This was done to not introduce any data-dependent bias in our identification, since the TS is fixed for all devices. Figure 5 shows the phase and frequency extracted from an acquired Normal Burst (transient sequence part), the correspondent ideal trajectory, as well as the computed phase and frequency errors (for device M4, Table 2). We define the phase and frequency extracted from the training sequence of the acquired signals as $\phi_{TS,REAL}$ and $f_{TS,REAL}$, while their corresponding ideal trajectories as $\phi_{TS,IDEAL}$ and $f_{TS,IDEAL}$. We note that the phase and frequency errors are computed by aligning the phase and frequency extracted from the training sequence of the acquired signals and their corresponding ideal trajectories at bit $i = 3$ of the training sequence $(0 \leq i \leq 25)$. This is done to not introduce any dependency from the pre-TS bits, which cannot be controlled[2]. The first features we

[2]Due to the GMSK/GSM modulation, the phase and frequency of those first TS bits are affected by the value of their predecessor bits, which cannot be controlled. From bit 3 on, the effect of pre-TS bits is considered negligible.

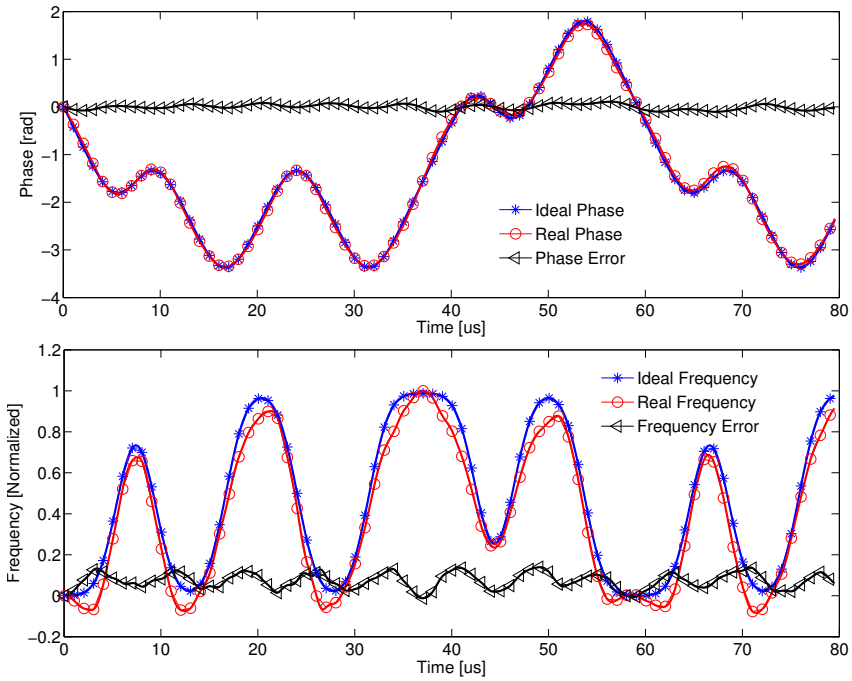


Figure 5: Extracted phase, ideal phase and phase error for the transient sequence part of an acquired Normal Burst (upper plot). Extracted frequency, frequency phase and frequency error for the transient sequence part of the same acquired Normal Burst (lower plot). Considered device: Wondex ST100 (M4, Table 2)

.

consider correspond to the phase and frequency errors themselves:

$$\epsilon_{\phi}[n] = \phi_{TS,IDEAL}[n] - \phi_{TS,REAL}[n] \tag{5}$$

$$\epsilon_{f}[n] = f_{TS,IDEAL}[n] - f_{TS,REAL}[n] \tag{6}$$

The second features we consider are based on the spectral components of each bit of the training sequence. Those components are obtained after Fourier transformation and the actual extracted feature is the concatenation of the extracted components for all bits in the training sequence. We defined as $\epsilon_{\phi,TS(i)}$ the phase error (resp. $\epsilon_{f,TS(i)}$ the frequency error) of bit i of the considered training sequence code $(3 \leq i \leq 25)$. The Fourier transformation of bit i is defined as follows:

$$E_{\phi_{TS(i)}}[k] = \sum_{n=0}^{L-1} \epsilon_{\phi,TS(i)}[n] \cdot e^{-2\pi jk\frac{n}{L}} \tag{7}$$

$$E_{f_{TS(i)}}[k] = \sum_{n=0}^{L-1} \epsilon_{f,TS(i)}[n] \cdot e^{-2\pi jk\frac{n}{L}} \tag{8}$$

where L is the length of the considered signal portion. Finally, the considered spectral-based features in our evaluation are defined as follows:

$$E_{\phi_{TS}} = \left[E^*_{\phi_{TS(a)}}, ..., E^*_{\phi_{TS(b)}}\right] \tag{9}$$

$$E_{f_{TS}} = \left[E^*_{f_{TS(a)}}, ..., E^*_{f_{TS(b)}}\right] \tag{10}$$

Indexes a and b are, respectively, the first and the last considered bits of the training sequence, i.e., $a = 3$ and $b = 25$. $E^*_{f_{TS(i)}}$ corresponds to $E_{f_{TS(i)}} \backslash E_{f_{TS(i)}}[0]$, i.e., we remove from the spectrum $E_{f_{TS(i)}}$ (resp. $E_{\phi_{TS(i)}}$) the DC component.

The third feature we consider is based on 7 different statistical metrics computed over the phase (frequency) error of each bit in the training sequence. The actual extracted feature is the concatenation of the computed statistical metrics for all bits in the training sequence. The considered metrics include mean μ, root mean square (RMS) r, peak p, standard deviation σ, variance σ^2, skewness γ and kurtosis k. The collection of the statistical metrics of bit i is defined as follows:

$$S_{\phi_{TS}(i)} = \left[\mu(x), r(x), p(x), \sigma(x), \sigma^2(x), \gamma(x), k(x)\right],\ x = \epsilon_{\phi,TS(i)} \tag{11}$$

$$S_{f_{TS}(i)} = \left[\mu(x), r(x), p(x), \sigma(x), \sigma^2(x), \gamma(x), k(x)\right],\ x = \epsilon_{f,TS(i)} \tag{12}$$

Finally, the considered statistical-based features in our evaluation are defined as follows:

$$S_{\phi_{TS}} = \left[S_{\phi_{TS(a)}}, ..., S_{\phi_{TS(b)}}\right] \tag{13}$$

$$S_{f_{TS}} = \left[S_{f_{TS(a)}}, ..., S_{f_{TS(b)}}\right] \tag{14}$$

As for the spectral-based features, indexes a and b are equal to 3 and 25 respectively.

4.2.1 Feature Combination and Matching

We build (and evaluate) fingerprints by considering each defined feature individually. For evaluation, reference and testing, device fingerprints are built from a number N of acquired Normal Bursts. Each device fingerprint is the value of a selected feature averaged over N (as defined in Section 4.1.1, Equation 4). For matching two fingerprints, i.e., computing the similarity score between reference and testing fingerprints, we used Euclidean distance.

5 Performance Results

In this section, we present the evaluation on the identification accuracy obtained by using each one of the proposed features according to the detailed experiments. First, we review the metrics that we use to evaluate the identification accuracy. Then, we elaborate on the achieved results and summarize the main outcomes of our experimental analysis.

5.1 Evaluation Metrics

We evaluate our feature accuracy in terms of the threshold-based identity verification. We adopt the Equal Error Rate (EER) as a single metric since it is a widely agreed metric for evaluating feature-based identification systems (such as biometric identication systems [7]). We estimate the EER as follows. We compute the similarity score between a set of testing fingerprints and a set of reference fingerprints from all devices. We then separate these scores in two categories: genuine and imposter. The genuine category includes all scores from matching two fingerprints from the same device. The imposter category contains all scores from comparing two fingerprints from different devices. Given that each score represents the similarity between two fingerprints (identities), we compute the rate of falsely rejected and falsely accepted devices using a threshold score value. The scores from the genuine category that are above this threshold indicate the number of false rejects or the False Reject Rate (FRR), while the scores from the imposter category that are below the threshold indicate the number of the false accepts or the False Accept Rate (FAR). The EER is the error rate where both FAR and FRR are equal. The value of the

threshold at the EER is our threshold T for an accept/reject decision. We use a 5-fold cross validation [6] in order to validate the error rates. For each device, its set of fingerprints is split in 5 independent folds; one fold is used as reference fingerprints, while the remaining four folds as testing fingerprints. The reference and testing data are thus separated.

5.2 Transient-based Features

We evaluate the device identification accuracy with respect to the transient-based features as detailed in Section 4.1. First, we consider a device population composed of 4 different model and manufacturer devices (M1-M4, Table 2). Then, we consider a device population composed of same model and manufacturer devices. For this latter, we deploy three different sets of devices: a set composed of 5 Wondex ST100 devices (M4-M8, Table 2), a set composed of 5 HTC Desire devices (M11, M13-M16), and a set composed of 10 HTC Desire devices (M9-M18). Within those explorations, we also evaluate the impact of a different device transmission power P_d, as well as a different device position with respect to the acquisition setup antenna (Figure 4). For these evaluations, we deploy the controlled, ad-hoc GSM network based on OpenBTS. This allows, in the one hand, to collect consistent signals, while, on the other hand, to diversify our exploration (i.e., to change P_d) in a controlled setup.

5.2.1 Different Model and Manufacturer Devices

Figures 6, 7 and 8 show the EER evaluation for 4 different model and manufacturer devices (M1-M4, Table 2) considering, respectively, the signal power envelope e, the instantaneous phase ϕ and the instantaneous frequency f. For each feature, the EER evaluation of each considered power (9, 17 and 25 dBm) and transient part (turn-on, turn-off and the combination of them) is shown. The device position with respect to the acquisition setup antenna is fixed at $L0$ (Figure 4). Those results are obtained by using Dataset 1 (Table 4). The instantaneous phase ϕ shows the worst performance among the three transient-based features: the EER is (approx.) equal to 0.5 for $N = 1$ (for any P_d and transient), while the best result with an EER equal to 0.27 is obtained for $N = 50$, $P_d = 9$ dBm and the combination (ϕ_{ON}, ϕ_{OFF}). Differently, both signal power envelope e and instantaneous frequency f provide an accurate identication even for small N. For $N = 1$, the EER is equal to 0.014 and 0.001 for e and f respectively (both for $P_d = 9$ dBm and the turn-on and turn-off combination). The EER is further reduced to 0 when $N \geq 2$ for both e and f ($P_d = 9$ dBm). We note that the device power P_d does not seem to have a consistent effect on the identification accuracy for the considered transients. However, consistent performance improvements are visible when reducing P_d for the signal power envelope feature. In addition, the smallest explored P_d, i.e., 9 dBm provides the best performance for both e and f.

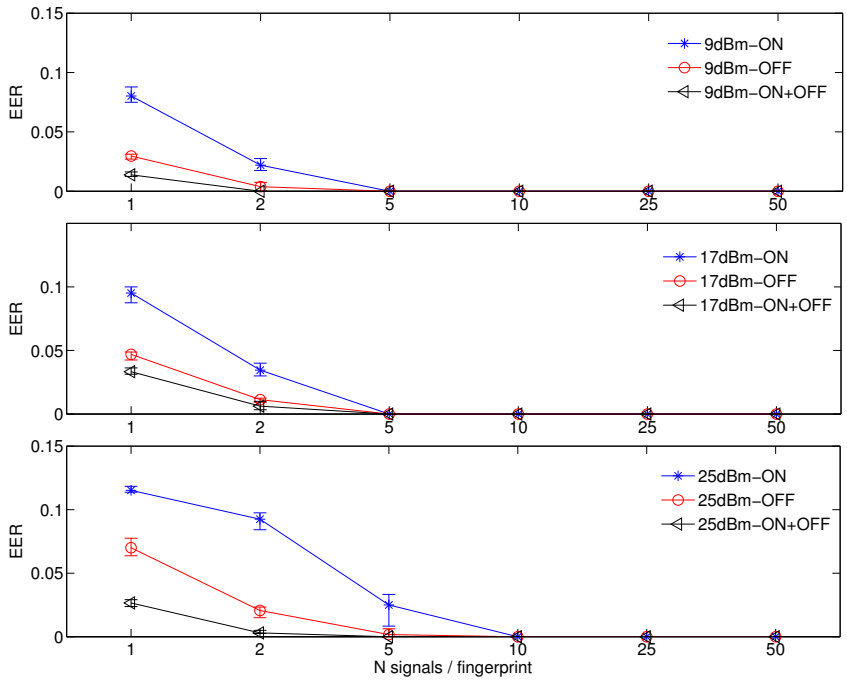


Figure 6: Identification accuracy for 4 different model and manufacturer devices (M1-M4). Transient-based feature - signal power envelope feature e extracted from the signal turn-on (ON) and turn-off (OFF) transients for different device transmission powers P_d (9, 17 and 25 dBm). Device position fixed at $L0$.

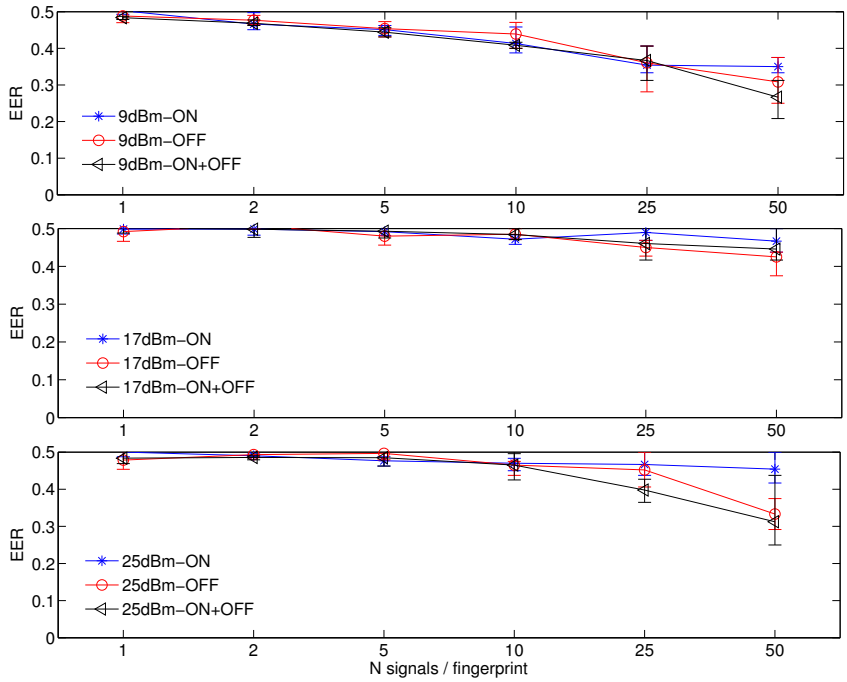


Figure 7: Identification accuracy for 4 different model and manufacturer devices (M1-M4). Transient-based feature - signal instantaneous phase feature ϕ extracted from the signal turn-on (ON) and turn-off (OFF) transients for different device transmission powers P_d (9, 17 and 25 dBm). Device position fixed at $L0$.

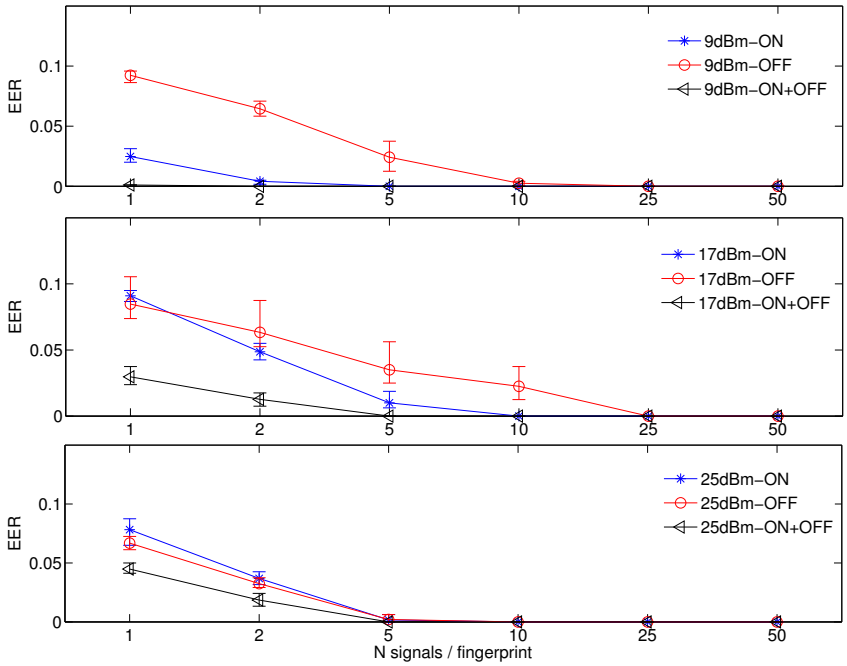


Figure 8: Identification accuracy for 4 different model and manufacturer devices (M1-M4). Transient-based feature - signal instantaneous frequency feature f extracted from the signal turn-on (ON) and turn-off (OFF) transients for different device transmission powers P_d (9, 17 and 25 dBm). Device position fixed at $L0$.

Figures 9 and 10 show the identication accuracy for, respectively, the signal power envelope e and the instantaneous frequency f when the device fingerprints extracted at different device transmission powers P_d are considered in a single evaluation set (the device position with respect to the acquisition setup antenna is fixed at $L0$; those results are obtained by using Dataset 1, Table 4). To compute the shown EERs, we use the fingerprints extracted at a specific device power $P_{d,i}$ as reference fingerprints, while the fingerprints extracted at a different device power $P_{d,j}$ as testing fingerprints (marked as $P_{d,i}/P_{d,j}$ in Figures 9 and 10). The figures show the evaluation results for the turn-on and turn-off transients, as well as the transient combination. We note that for both the signal power envelope e and the instantaneous frequency f, the fingerprints extracted at different transmission powers present differences leading to relatively high EERs. Different fingerprints means different transients; Figure 11 shows the signal power envelope extracted from the turn-off transient acquired at different device transmission powers (9, 17 and 25 dBm) for the 4 considered devices. It is clearly visible how, for the same device, the transient changes as the power changes.

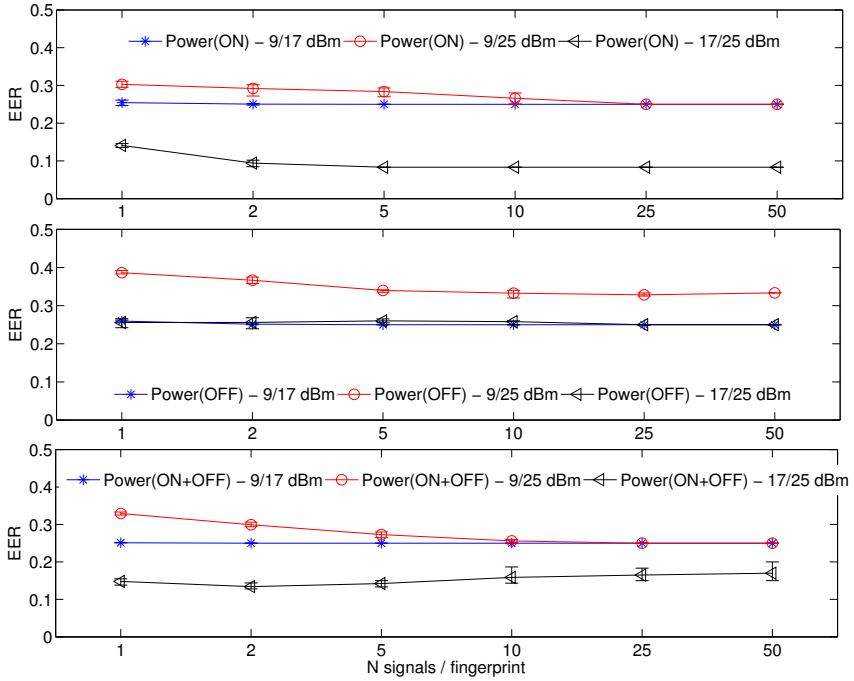


Figure 9: Identification accuracy for 4 different model and manufacturer devices (M1-M4) for signals acquired at different transmission powers (9, 17 and 25 dBm) and at a fixed position ($L0$). Transient-based feature - signal power envelope e feature extracted from the signal turn-on (ON) and turn-off (OFF) transients. *9/17 dBm* indicates that signals acquired when $P_d = 9$ dBm are used as reference, while signals acquired when $P_d = 17$ dBm as testing.

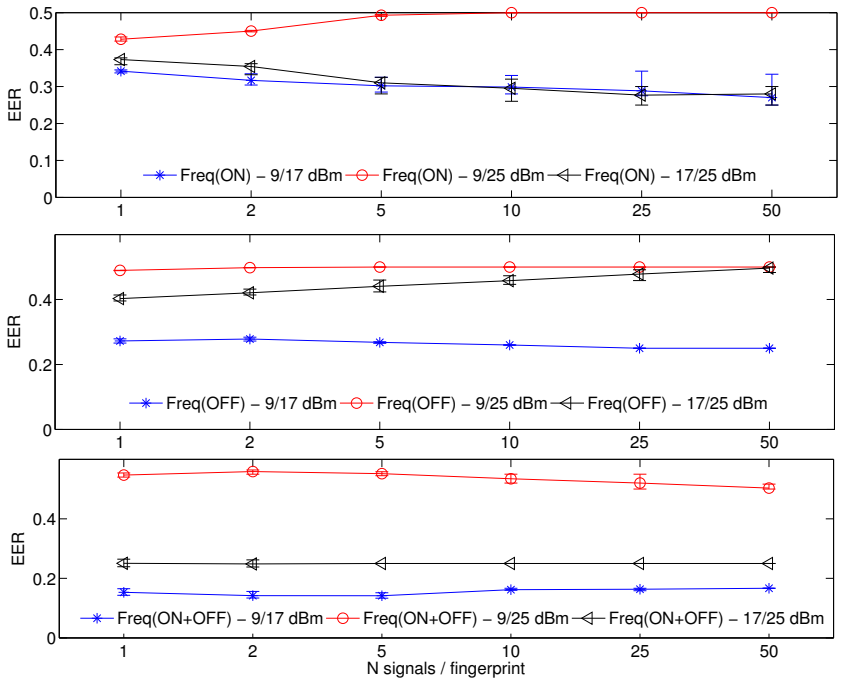


Figure 10: Identification accuracy for 4 different model and manufacturer devices (M1-M4) for signals acquired at different transmission powers (9, 17 and 25 dBm) and at a fixed position ($L0$). Transient-based feature - signal instantaneous frequency feature f extracted from the signal turn-on (ON) and turn-off (OFF) transients. *9/17 dBm* indicates that signals acquired when $P_d = 9$ dBm are used as reference, while signals acquired when $P_d = 17$ dBm as testing.

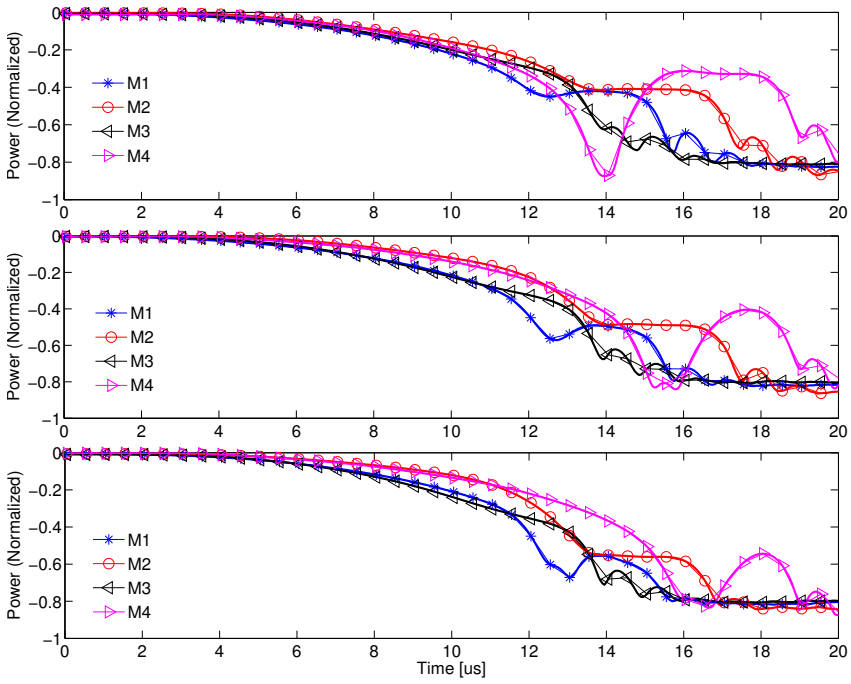


Figure 11: Different model and manufacturer devices (M1-M4): signal power envelope extracted from the turn-off transient acquired at a transmission power P_d equal to 9 (upper plot), 17 (middle plot) and 25 dBm (lower plot). The device position is fixed to $L0$.

Figure 12 shows the identication accuracy considering the signal power envelope e and the instantaneous frequency f for signals acquired at two different device positions (L0 and L1, Figure 4 - the device transmission power P_d is fixed at 17 dB. Those results are obtained by using both Datasets 1 and 2, Table 4). To compute the shown EERs, we use the fingerprints extracted from signals acquired when the devices are at position $L0$ as reference fingerprints, while the fingerprints extracted at position $L1$ as testing fingerprints. The plots in Figure 12 show the evaluation results for the turn-on and turn-off transients, as well as the transient combination. When considering the signal power envelope feature, although a general performance degradation can be observed, it is also possible to notice that the device position does not dramatically affects the identication accuracy, especially for higher N. In fact, for $N \geq 10$, the EER is still equal to 0 for both the turn-off transient and the combination (e_{ON}, e_{OFF}). Figure 13 shows the signal power envelope extracted from the turn-off transient acquired at the two considered device positions $L0$ and $L1$ for the 4 considered devices. The transients at the different positions are quite similar. Mainly, differences can be observed in the low-power part of the signal: for a fixed transmission power, a larger distance ($L1$ with respect to $L0$) means a smaller signal-to-noise ratio, which affects the low-power part of the signal. When considering the instantaneous frequency feature we observe a similar performance degradation, but differently from what noticed for the signal power envelope feature, the device position largely affects the identication accuracy: an EER equal to 0 is obtained only for the combination (f_{ON}, f_{OFF}) and for $N = 25$.

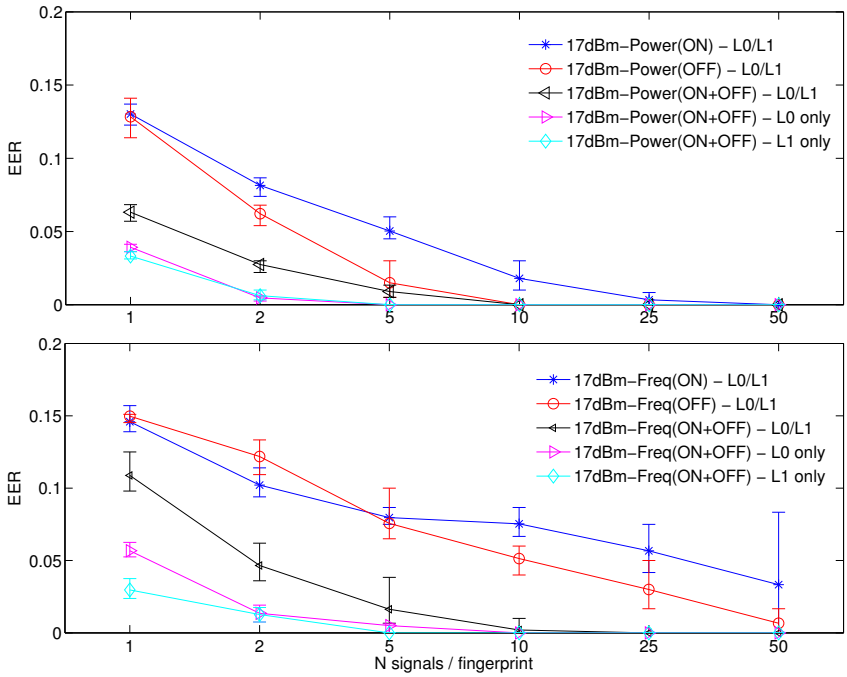


Figure 12: Identification accuracy for 4 different model and manufacturer devices (M1-M4) for signals acquired in 2 different positions (L0 and L1). Transient-based feature - signal power envelope e (upper plot) and instantaneous frequency f (lower plot) features extracted from the signal turn-on (ON) and turn-off (OFF) transients for $P_d = 17$ dBm. *L0/L1* indicates that signals acquired at position L0 are used as reference, while signals acquired at position L1 as testing. *Lx only* means that both reference and testing signals are acquired at position Lx.

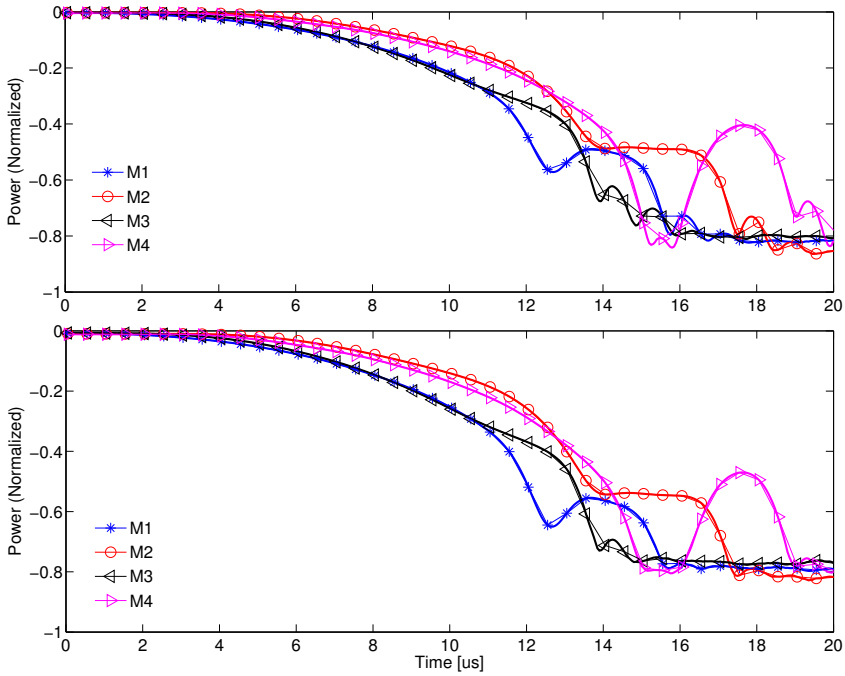


Figure 13: Different model and manufacturer devices (M1-M4): signal power envelope extracted from the turn-off transient acquired at position $L0$ (upper plot) and $L1$ (lower plot). P_d equal to 17 dBm.

5.2.2 Same Model and Manufacturer Devices

Figure 14 shows the identification accuracy for 5 Wondex ST100 device (M4-M8, Table 2) considering the signal power envelope feature e (upper plot), the instantaneous phase feature ϕ (middle plot) and the instantaneous frequency feature f (lower plot) for $P_d = 9$ dBm and position $L0$ (Dataset 3). Similarly to the previous results, the instantaneous phase feature does not provide reliable identification and the signal power envelope feature leads to an accurate identification. Although the identication accuracy has generally degraded, the signal power envelope feature extracted from the turn-off transient still presents an $EER = 0$ for $N \geq 10$ (but, for $N = 1$, the EER has increased to 0.13). Differently from previous results, the instantaneous frequency feature does not provide an accurate identification (unless a large N is considered: for $N = 50$, the EER is equal to 0.04).

Figure 15 shows the identification accuracy for 5 HTC Desire devices (M11, M13-M16) considering the signal power envelope feature e (upper plot), the instantaneous phase feature ϕ (middle plot) and the instantaneous frequency feature f (lower plot) for $P_d = 9$ dBm and position $L0$ (Dataset 4). Both the instantaneous phase and frequency features present similar results as for the set of 5 Wondex ST100 devices; the best case is obtained by considering the instantaneous frequency feature extracted from the turn-off transient and $N = 50$, which gives an EER equal to 0.06. Differently from the previous results, the signal power envelope feature leads to an inaccurate identification, in which the best case gives an $EER = 0.23$ for $N = 50$.

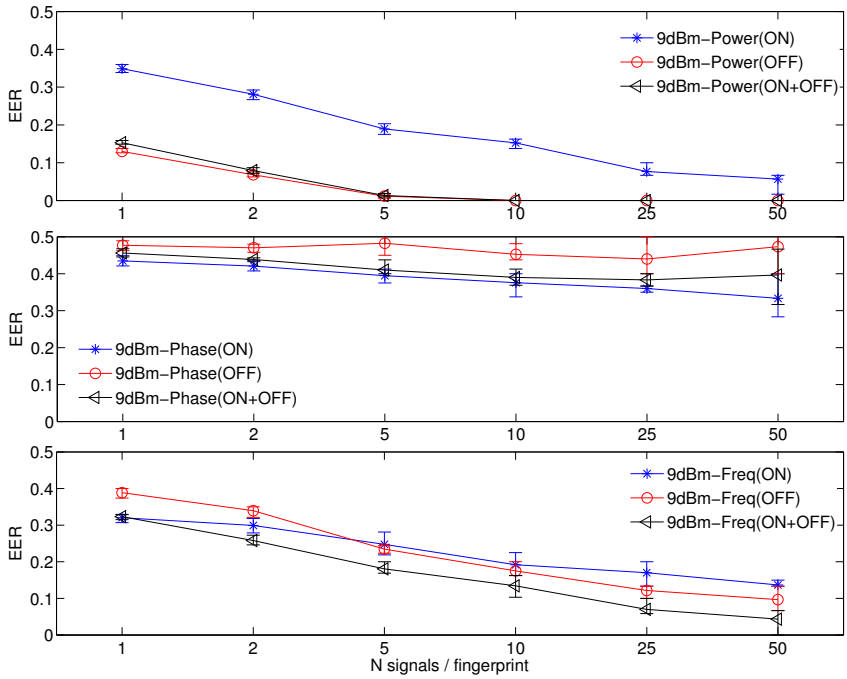


Figure 14: Identification accuracy for 5 Wondex ST100 devices (M4-M8). Transient-based features extracted from the signal turn-on (ON) and turn-off (OFF) transients for $P_d = 9$ dBm and position $L0$. Signal power envelope feature e (upper plot), instantaneous phase feature ϕ (middle plot) and instantaneous frequency feature f (lower plot).

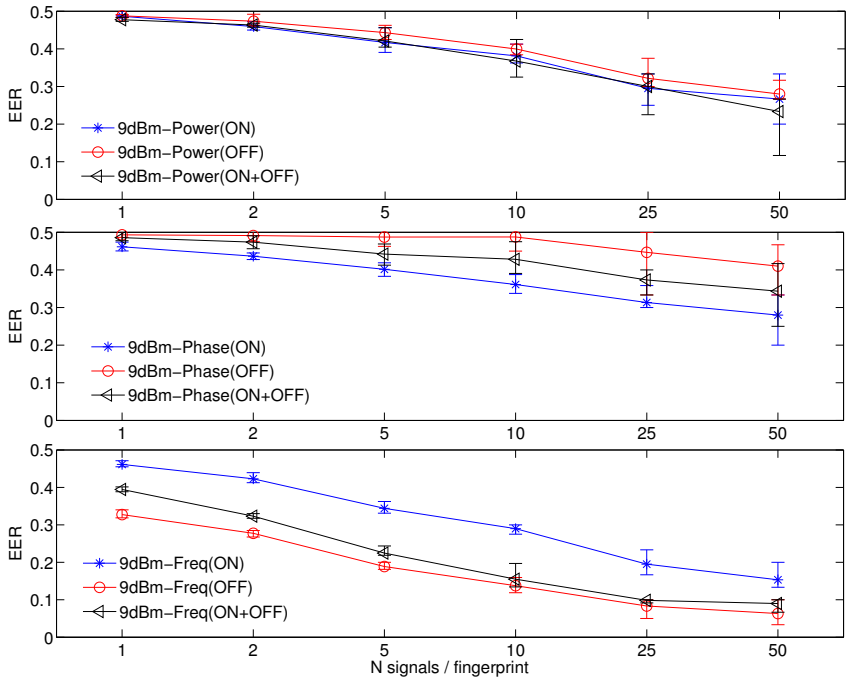


Figure 15: Identification accuracy for 5 HTC Desire devices (M11, M13-M16). Transient-based features extracted from the signal turn-on (ON) and turn-off (OFF) transients for $P_d = 9$ dBm and position $L0$. Signal power envelope feature e (upper plot), instantaneous phase feature ϕ (middle plot) and instantaneous frequency feature f (lower plot).

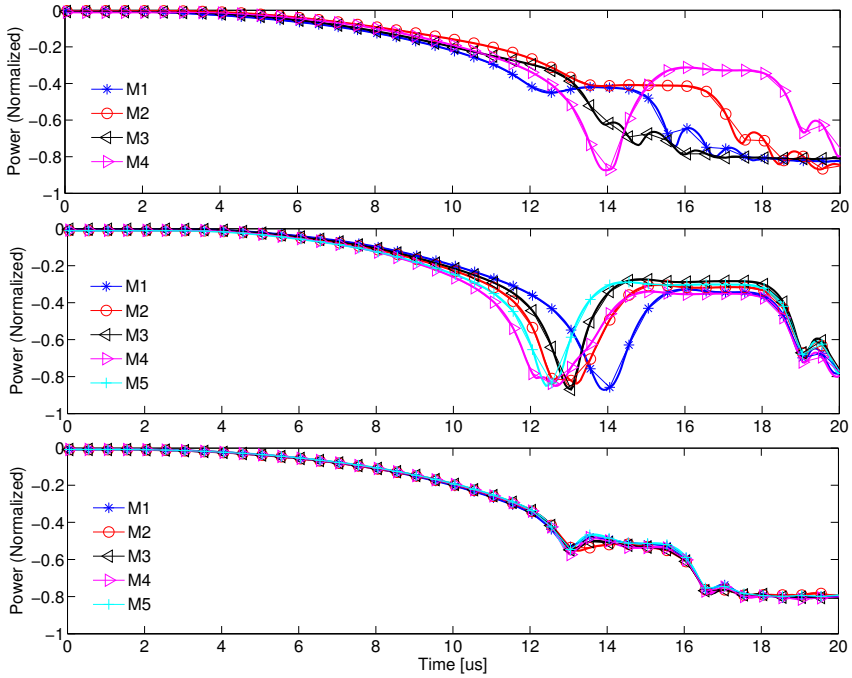


Figure 16: Signal power envelopes extracted from the turn-off transient for three different sets of devices: 4 different model and manufacturer devices (M1-M4, upper plot), 5 Wondex ST100 devices (M4-M8, middle plot) and 5 HTC Desire devices (M11, M13-M16, lower plot). $P_d = 9$ dBm and device position $L0$.

The differences in the identification performance of the three considered sets of devices can be visually inferred in Figure 16, which shows the signal power envelope extracted from the turn-off transient for the different model and manufacturer devices (M1-M4, upper plot), the 5 Wondex ST100 devices (M4-M8, middle plot) and the 5 HTC Desire devices (M11, M13-M16, lower plot). Signals are acquired at a fixed $P_d = 9$ dBm and position $L0$ (Datasets 1, 3, and 4). The different model and manufacturer devices present significant differences when comparing their turn-off power envelopes. These differences are reduced within the set of Wondex ST100 devices, while the 5 HTC Desire devices have similar envelopes.

Figures 17 and 18 show the EER evaluation for 10 HTC Desire devices (M9-M18) considering the signal power envelope e and the instantaneous frequency f respectively. For each feature, a plot displaying the evaluation results for each considered power (5, 25 and 33 dBm) and transient part (turn-on, turn-off and the combination of them) is provided (device position $L2$, Dataset 5). The considered features provide similar identification accuracy, leading to the best results at $N = 50$, where the EER is equal to 0.086 and 0.08 for the instantaneous frequency feature (turn-on transient, $P_d = 5$ dBm) and the signal power envelope (turn-on transient, $P_d = 5$ dBm) respectively. The combination (f_{ON}, e_{ON}) leads to a relatively small improvement: for $N = 50$, the EER is equal to 0.072 ($P_d = 5$ dBm). Given the shown results, as well as the results in Figure 15, smaller device transmission powers seem to provide a better identification accuracy. This may be inferred from Figure 19, which shows the signal power envelope extracted from the turn-on transient of 10 HTC Desire devices (M9-M18) for two different device transmission powers. Comparing the extracted features within that set of devices, those extracted when $P_d = 5$ dBm (upper plot) present a larger number of discriminant points with respect to those extracted when $P_d = 33$ dBm (lower plot).

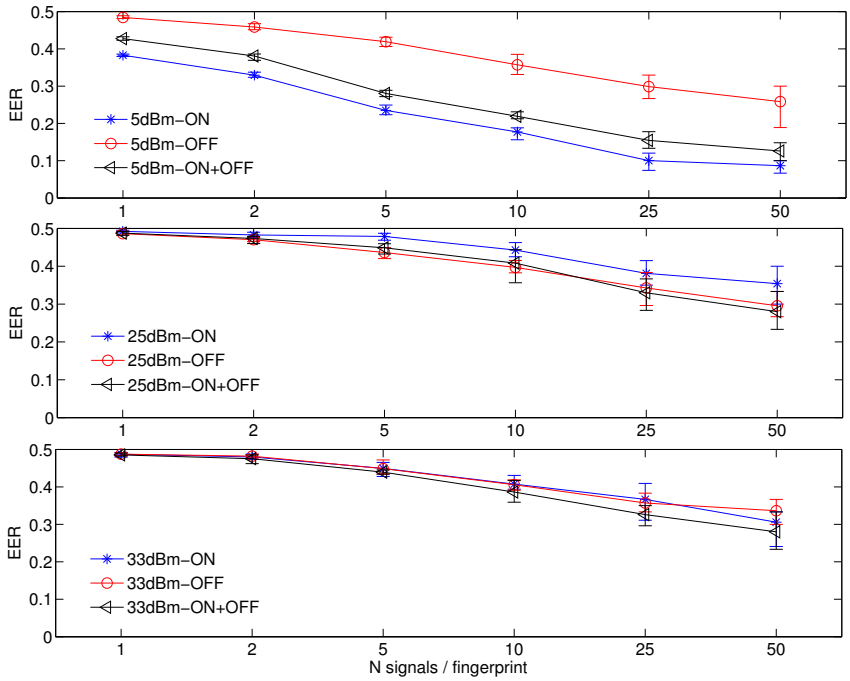


Figure 17: Identification accuracy for 10 HTC Desire devices (M9-M18). Transient-based feature - signal power envelope feature e extracted from the signal turn-on (ON) and turn-off (OFF) transients for different device transmission powers (5, 25 and 33 dBm) and at a fixed device position ($L2$).

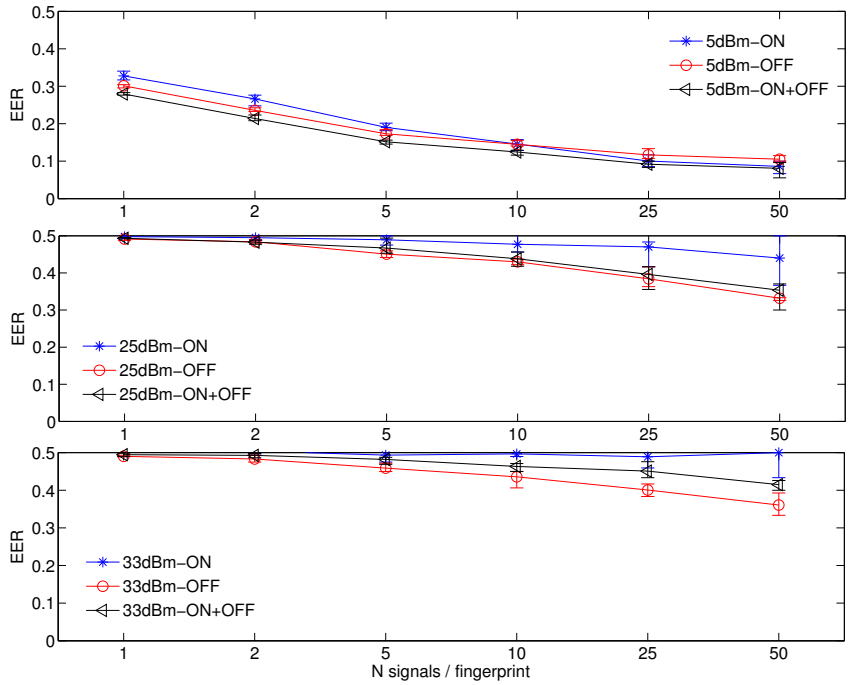


Figure 18: Identification accuracy for 10 HTC Desire devices (M9-M18). Transient-based feature - signal instantaneous frequency feature f extracted from the signal turn-on (ON) and turn-off (OFF) transients for different device transmission powers (5, 25 and 33 dBm) and at a fixed device position ($L2$).

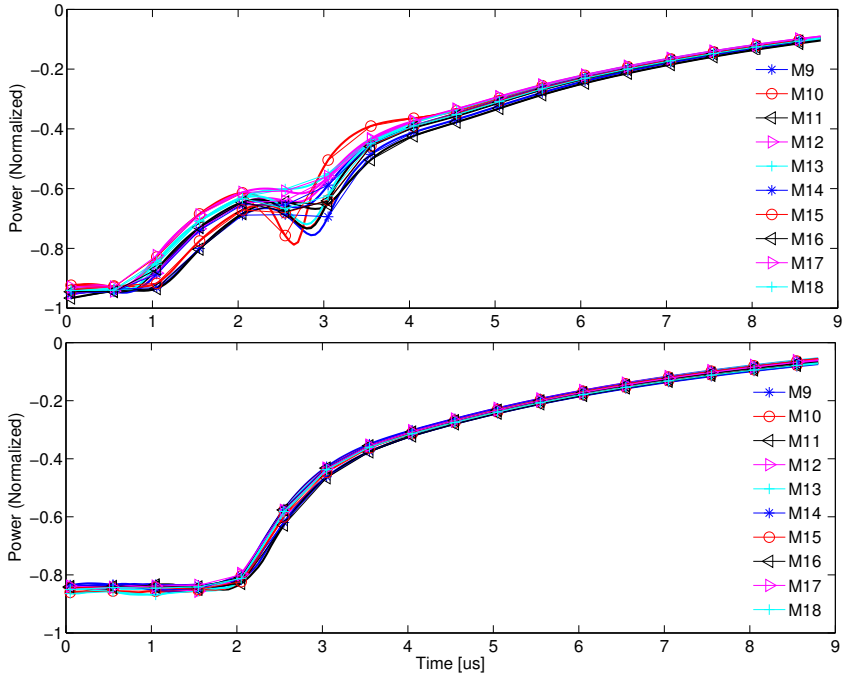


Figure 19: Signal power envelopes extracted from the turn-on transient of 10 HTC Desire devices (M9-M18). The upper plot shows the feature extracted for a device transmission power P_d equal to 5 dBm, while the lower plot for $P_d = 33$ dBm (device position $L2$).

5.3 Data-based Features

We evaluate the device identification accuracy with respect to the data-based features as detailed in Section 4.2 for a device population composed of two sets of 4 same model and manufacturer devices: 4 Wondex ST100 (M4, M6-M8, Table 2) and 4 HTC Desire devices (M13-M16). For these evaluations, only the signals obtained when the devices are attached to the local Swisscom network are used[3]. Therefore, we evaluate the impact of different device positions with respect to the acquisition setup antenna, but not different device transmission powers (since the device power cannot be tuned when exploiting a network which is not under control of the entity performing the device identication).

Figure 20 shows the identification accuracy for the 4 Wondex ST100 devices considering the features related to the phase error (ϵ_ϕ, $E_{\phi_{TS}}$ and $S_{\phi_{TS}}$ - upper plot) and the features related to the frequency error (ϵ_f, $E_{f_{TS}}$ and $S_{f_{TS}}$ - lower plot). The devices are positioned at $L2$ (Dataset 6). None of the features provide accurate identication, even with such a low number of considered devices. The best cases are obtained for the statistical-based, phase error feature $S_{\phi_{TS}}$ and the frequency error feature ϵ_f, where the EER is equal to 0.19 and 0.32 respectively ($N = 50$).

Figure 21 shows the identification accuracy for the 4 HTC Desire devices considering the features related to the phase error (upper plot) and the features related to the frequency error (lower plot). The devices are positioned at $L2$ (Dataset 7). The best cases are obtained for the phase error related features: the EER is equal 0.022, 0.027 and 0.033 ($N = 50$) for ϵ_ϕ, $E_{\phi_{TS}}$ and $S_{\phi_{TS}}$ respectively. None of the frequency error related features provide accurate identication (the best case EER is equal to 0.11 for $N = 50$ and the feature $E_{f_{TS}}$).

Figure 22 shows the identification accuracy for the 4 HTC Desire devices (M13-M16) considering the phase error features ϵ_ϕ (upper plot), $E_{\phi_{TS}}$ (middle plot) and $S_{\phi_{TS}}$ (lower plot) extracted from signals

[3]Details in Section 6.

acquired at 5 different positions ($L2$-$L6$, Dataset 7). To compute the shown EERs, we use the fingerprints extracted from signals acquired when the devices are at position $L2$ as reference fingerprints, while the fingerprints extracted at the other positions ($L3 - L6$) as testing fingerprints (each one in turn). We note that any of the phase error features provide high EER when fingerprints are extracted from signals acquired at different device positions, which indicates that fingerprints obtained at different device positions are also different.

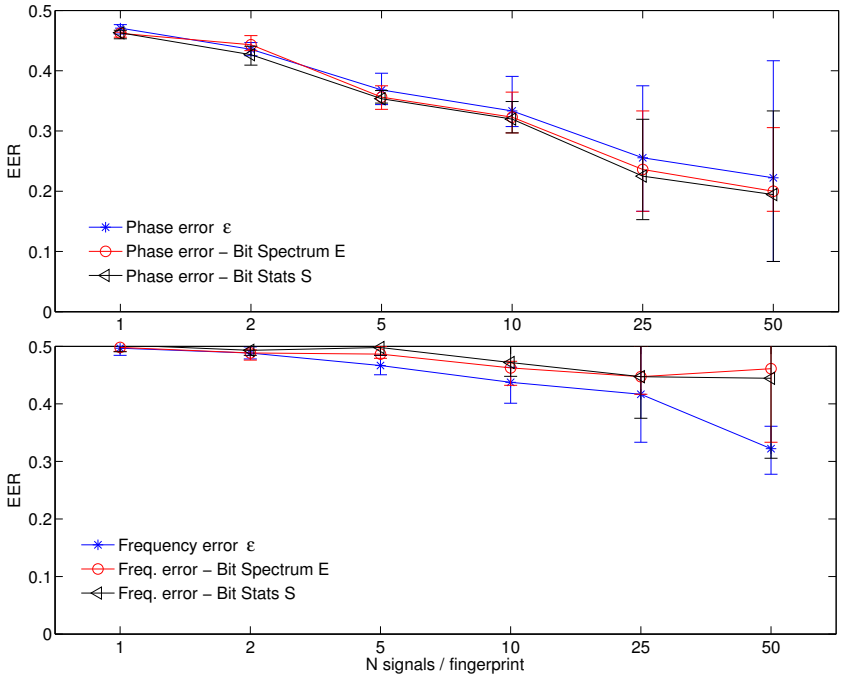


Figure 20: Identification accuracy for 4 Wondex ST100 devices (M4, M6-M8). Data-based, phase error features (ϵ_ϕ, $E_{\phi_{TS}}$, $S_{\phi_{TS}}$, upper plot) and frequency error features (ϵ_f, $E_{f_{TS}}$, $S_{f_{TS}}$, lower plot) extracted from the burst training sequence. Device position $L2$.

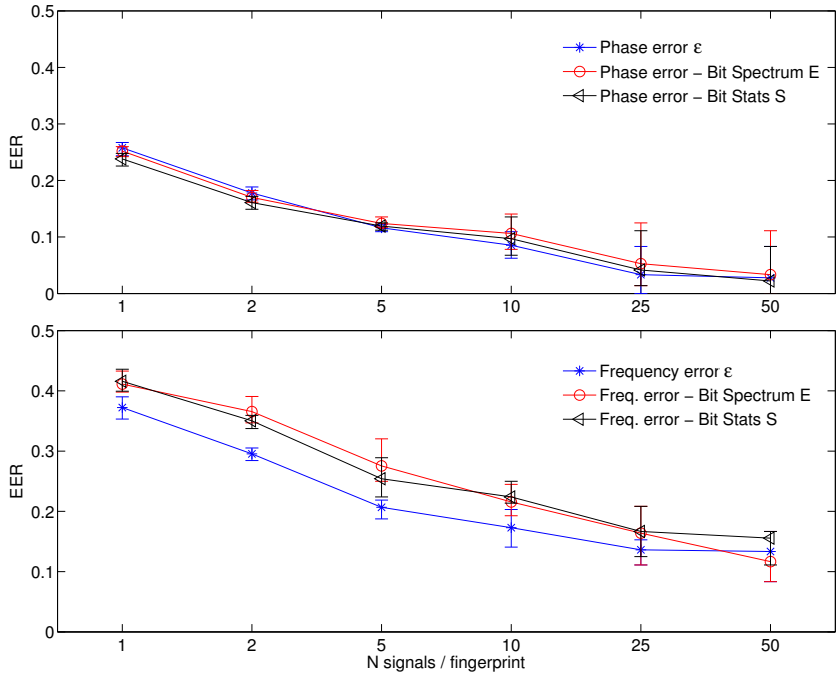


Figure 21: Identification accuracy for 4 HTC Desire devices (M13-M16). Data-based, phase error features (ϵ_ϕ, $E_{\phi_{TS}}$, $S_{\phi_{TS}}$, upper plot) and frequency error features (ϵ_f, $E_{f_{TS}}$, $S_{f_{TS}}$, lower plot) extracted from the burst training sequence. Device position $L2$.

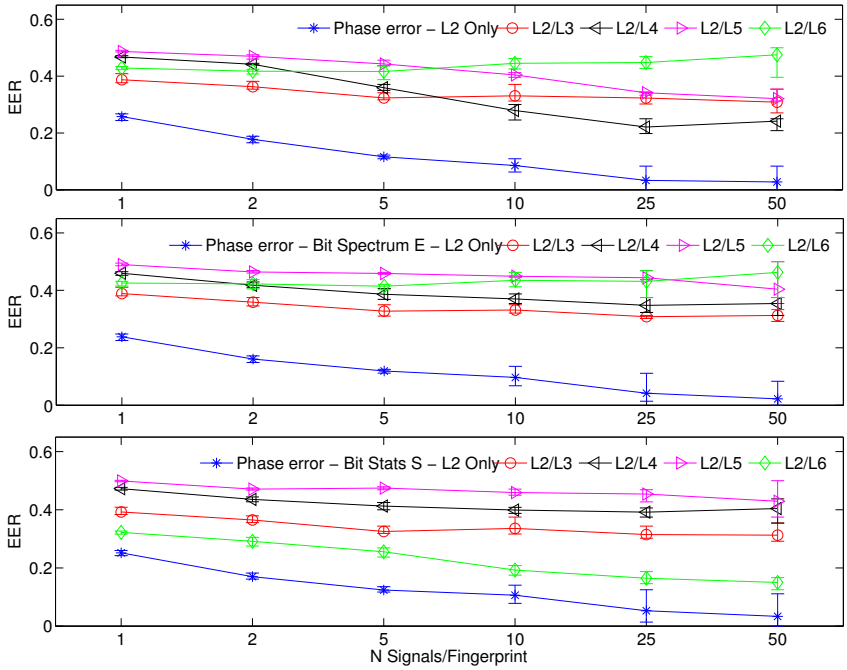


Figure 22: Identification accuracy for 4 HTC Desire devices (M13-M16) when signals are acquired in 5 different positions ($L2$-$L6$). Data-based, phase error features ϵ_ϕ (upper plot), $E_{\phi_{TS}}$ (middle plot) and $S_{\phi_{TS}}$ (lower plot) extracted from the burst training sequence. $L2/L3$ indicates that signals acquired at position $L2$ are used as reference, while signals acquired at position $L3$ as testing. $L2$ *only* means that both reference and testing signals are acquired at position $L2$.

6 Discussion

Different model and manufacturer devices can be uniquely identified with high accuracy by extracting the signal power envelope e and the instantaneous frequency f of the signal turn-off and turn-on transients. This highly accurate identication ($EER = 0$) can be obtained even for small N (equal to 2 for both e and f, $P_d = 9$ dBm), but only when the power transmission of the device is fixed. Matching fingerprints extracted from signals transmitted at different powers leads to inaccurate identication. The device position with respect to the acquisition antenna setup affects the quality of both the fingerprints extracted from the signal power envelope and the instantaneous frequency, but, with an increase of N (from 5 to 10 for e and from 5 to 25 for f, $P_d = 17$ dBm), both features are still providing a reliable identication ($EER = 0$). Although the device power P_d does not seem to have a consistent effect on the identification accuracy for the considered transients and features (for the same device position), we note that (i) consistent performance improvements are visible when reducing P_d for the signal power envelope feature and (ii), the smallest explored P_d, i.e., 9 dBm provides the best performance for both e and f. Exploring the actual extracted features, it seems that at low-power, the signals have more discriminant points. However, the less the transmission power, the higher the signal-to-noise ratio, which impacts the fingerprints quality (especially for larger distances between the device under investigation and the receiving antenna of the acquisition setup). The possibility of extracting reliable fingerprints from different positions enables both defensive (e.g., access control) and offensive (i.e., clandestine tracking) applications. However, the constraint of a fixed device transmission power (only possible when controlling the GSM network or the GSM stack implemented in the devices) may limit the possible deployment to defensive applications[4]. Devices attached to a non-controlled network would be also uniquely identified if the power-dependency of the acquired signals could be removed. For example, by discarding signals with a power level (or a signal-to-noise ratio) that excesses certain predefined thresholds. To validate the obtained results, a large number of different model and manufacturer devices should be explored.

Same model and manufacturer devices could be uniquely identified with high accuracy by extracting the signal power envelope e (signal turn-off transient), but among the explored set for devices, only with the set of 5 Wondex ST100 devices we obtained an highly accurate identication ($EER = 0$) even for small N (equal to 10). For the 10 HTC Desire set, we obtained a higher identification accuracy even when considering a large $N = 50$ (EER of approx. 0.08 for both the instantaneous frequency and the signal power envelope feature). Those results are affected by the device transmission power and position as for the different model and manufacturer devices. We note that the best results for the explored sets of devices are obtained by considering diffent transient parts and features: for the set of 5 Wondex ST100 devices, the signal power envelope of the turn-off transient (the transients combination also performs well), while for the HTC Desire devices, the instantaneous frequency of the combination of both the turn-on and turn-off transients (the single transients also perform well). This indicates that it may be infeasible to define *a priory* the best transient part and feature for any device (model). We additionally note that, as remarked for the different model and manufacturer exploration, the smallest explored P_d, i.e., 5 dBm provides the best performance for both e and f. Similar conclusions as done for different model and manufacturer exploration can be drawn for the possible applications. To validate the obtained results, a large number of Wondex ST100 devices should be explored (as well as different device positions for that set of devices). In addition, other sets of same model and manufacturer devices should be considered.

Same model and manufacturer devices could also be uniquely identified with relatively-high accuracy ($EER = 0.02$) by extracting the phase error features from the Normal Burst training sequence.

[4]Device tracking could be performed by using controlled network in which the attacker forces the devices to connect. However, the overhead and constraints of forcing the devices to switch to the controlled network may limit the actual applicability. In addition, other less sophisticated means of identication could be used instead of physical-layer identification when controlling a GSM network, e.g., the device IMEI or the user IMSI.

However, this requires a large number of acquired signal ($N = 50$) and is valid only for the set of 4 HTC Desire devices. When considering the set of 4 Wondex ST100 devices, even with $N = 50$ the EER has a modest value equal to 0.19. In addition, data-based features seem sensitive to the device position with respect to the antenna setup. The obtained results are based on signals acquired from devices attached to a non-controlled network (the local Swisscom one). For the exploration of the data-based features we could not use the controlled network based on the OpenBTS, since, even though we provided the OpenBTS hardware (i.e., the USRP) with an highly accurate reference clock, the signal phase and frequency were randomly affected by the network operations, leading to inconsistent data. Therefore, without the possibility to set a fixed device transmission power, we cannot exclude that the obtained EERs are affected by the varying transmission power. In fact, the extracted features present large inconsistencies even for the same device, which may indicate a perturbation due to a varying transmission power. To properly evaluate the proposed data-based features, the possible effect of a varying device transmission power needs to be considered (e.g., as proposed for the different model and manufacturer exploration, by discarding signals with a power level, or a signal-to-noise ratio that excesses certain predefined thresholds.) In addition, the obtained results should be validated with a large number of Wondex ST100 and HTC Desire devices.

Feature work may include to exploration of a larger set of different model and manufacturer devices, as well as a larger set of Wondex ST100 devices to confirm the promising results obtained by exploiting the signal power envelope feature on the signal turn-off transient. Additionally, other sets of same model and manufacturer devices could be considered, as well as a proper evaluation of the data-based features without the effect of an uncontrolled device transmission power and with larger sets of devices. Moreover, more sophisticated feature extraction techniques (e.g., PCA or LDA) may be also explored in the purpose of both performance improvement and fingerprint dimensionality reduction (currently, a fingerprint corresponds to the *raw* extracted feature and has dimensionality equal to 400 points). Regarding the applicability of the proposed physical-layer techniques in real-world scenarios, an evaluation of the effect of using different acquisition setups (mainly, by considering different acquisition antennas), as well as an evaluation of the repeatability over time of the performed experiments and results may need to be considered. In order to define the effort in terms of the number of acquired signals needed to build reliable fingerprints in noisy environments, a proper estimation of the signal-to-noise ratio of the acquired signals is necessary.

We note that not all the collected datasets, performed experiments and considered features are detailed in this report. Several additional datasets are listed in Table 4, from dataset 8 to 16. Those datasets vary in the considered device position with respect to the acquisition antenna, acquisition parameters (sampling rate and signal downmixing frequency), deployed GSM network, as well as calling method: one single call per acquisition, multiple calls per acquisition, calls with the microphone on mute and calls with the microphone on and injecting sound. Withing the explored bounds and cases, we did not experienced any remarkable effect on the identification accuracy when varying the mentioned parameters, except for the deployed GSM network (as detailed above, the OpenBTS-based network is not suitable to collect signals for the extraction of data-based features). Regarding additional features, for the transient part we considered the spectral components of both the turn-on and turn-off transients. For the data-part, we considered the phase and frequency errors of the entire data part of the Normal Burst, as well as the IQ constellation of both the training sequence and the entire data part of the Normal Burst. In addition, we also considered the phase and frequency of the training sequence, as well as its spectral components. Those feature do not provide improved results with respect to those detailed in this report.

7 Related Work

Physical-layer identification has been investigated on a number of hardware platforms including GSM devices [22, 23, 29]. Reising et al. [22] deployed the instantaneous phase and frequency information of

both the Normal Burst turn-on transient and training sequence to build device fingerprints. The authors evaluated the proposed physical-layer identification techniques for a population of 3 different model and manufacturer devices. In addition, the authors evaluated the effect of noise (additive white Gaussian noise) on the device fingerprints. The results show that the fingerprints built using the instantaneous phase information of the turn-on transient can be classified with high accuracy even for a low signal-to-noise ratio (SNR): for an SNR of 6, 10, and 20 dBm, the classification success rate is 90, 96, and 99.5% respectively. The results also show that the fingerprints built using the instantaneous phase information of the turn-on transient outperform the fingerprints based on the training sequence (for both the instantaneous phase and frequency information) for SNRs < 20 dBm, while both signal parts provide accurate device classification for higher SNRs (> 40 dBm). Although the presented work is technically sounds, due to the low number of considered devices (3) and their diversity (different model and manufacturer), additional work should be carried out in order to prove the actual feasibility and effectiveness of physical-layer identification for GSM devices. In a follow-up work [23], the authors explored similar features and feature extraction method to perform the physical-layer identication of a different set of 4 devices (different model and manufacturer devices). This new exploration confirm the results and conclusions of the previous one. Additional performance analysis was provided for GSM devices from the same model and manufacturer by Williams et al. [29]. The authors explored 4 sets of 4 same model and manufacturer devices by exploiting the instantaneous phase feature and feature extraction method on the Normal Burst turn-on transient and training sequence as detailed in [22, 23]. The analysis reveals that the training sequence provides more discriminant information than the turn-on transient, as well as that a significant SNR increase (≥ 35 dB) was required in order to achieve high classification accuracy ($\geq 90\%$) within same manufacturer devices (for all the 4 considered sets). As for the previously mentioned works, the work of Williams et al. [29] is technically sound, but due to the low number of considered devices per model (4) additional work should be carried out in order to prove the actual feasibility and effectiveness of physical-layer identification for same model and manufacturer devices. In addition, a stability analysis including different device positions with respect to the acquisition setup and different acquisition setups (antennas) should be performed.

Besides the mentioned works on GSM devices, physical-layer device identification techniques have been explored for several wireless platforms, including VHF [26, 27], Bluetooth [15], IEEE 802.11 [8, 16, 28], 802.15.4 (ZigBee) [10, 21], HF RFID [9, 24, 25], and UHF RFID [18–20, 30]. For a thoughtful survey on physical-layer device identification, see Danev et al. [11].

8 Conclusion

In this work we explored the physical-layer identification of GSM devices. We acquired GSM signals with an ad-hoc setup during voice calls, and built fingerprints by considering both the transient and the data part of the acquired signals. In our investigation we deployed different sets of GSM devices: a set of 4 different model and manufacturer devices, a set of 5 Wondex ST100 devices and a set of 10 HTC Desire devices (therefore, two sets of same model and manufacturer devices). We found that the set of 4 different model and manufacturer devices can be identified with high accuracy (0% identification error) by exploiting transient-based fingerprints, while only one of the set of same model and manufacturer devices, the 5 Wondex ST100 devices, can be identified with the same high accuracy. The 10 HTC Desire devices have been identified with an identification error equal to 8% (transient-based features). We also found that the proposed transient-based features and physical-layer techniques are sensitive to the device transmission power, but only partially to the device position with respect to our acquisition setup (which can be compensated by a higher number of signals used to build the fingerprints), possibly enabling defensive (e.g., access control) applications. Although with less accuracy with respect to transient-based features, data-based features could also be used to identify same model and manufacturer devices: for a set of 4 HTC Desire devices, the identification error is equal to 2%. Future work may include to

exploration of a larger set of different model and manufacturer devices, as well as a larger set of Wondex ST100 devices. Additionally, other sets of same model and manufacturer devices could be considered. Moreover, more sophisticated feature extraction techniques (e.g., PCA or LDA) may be also explored in the purpose of both performance improvement and fingerprint dimensionality reduction.

Acknowledgment

This work was partially funded by armasuisse under the research program *Kommunikation und Cyberspace*, competence field *Sicherheitstechnologien mobiler Informationssysteme*, project *DEVIDENT: Wireless Device Identification* (aramis Nr. R3210/047-10). It represents the views of the authors.

References

[1] http://openbts.sourceforge.net/.

[2] http://www.etsi.org/.

[3] http://www.ettus.com/.

[4] http://www.asterisk.org/.

[5] http://www.mathworks.com/.

[6] C.M. Bishop. *Pattern Recognition and Machine Learning*. Springer, 2006.

[7] R. Bolle, J. Connell, S. Pankanti, N. Ratha, and A. Senior. *Guide to Biometrics*. Springer, 2003.

[8] V. Brik, S. Banerjee, M. Gruteser, and S. Oh. Wireless device identification with radiometric signatures. In *Proc. ACM International Conference on Mobile Computing and Networking*, 2008.

[9] B. Danev, T. S. Heydt-Benjamin, and S. Čapkun. Physical-layer identification of RFID devices. In *Proc. USENIX Security Symposium*, 2009.

[10] B. Danev and S. Čapkun. Transient-based identification of wireless sensor nodes. In *Proc. ACM/IEEE Conference on Information Processing in Sensor Networks*, 2009.

[11] Boris Danev, Davide Zanetti, and Srdjan Čapkun. On physical-layer identification of wireless devices. *ACM Computing Surveys (CSUR)*, 2012.

[12] ETSI. *ETSI TS 100 959 V8.4.0 - 3GPP TS 05.04 version 8.4.0 Release 1999*, 2001.

[13] ETSI. *ETSI TS 100 908 V8.11.0 - 3GPP TS 05.02 version 8.11.0 Release 1999*, 2003.

[14] Siegmund H. Redl, Matthias K. Weber, and Malcolm W. Oliphant. *An introduction to GSM*. Artech House, 1995.

[15] J. Hall, M. Barbeau, and E. Kranakis. Enhancing intrusion detection in wireless networks using radio frequency fingerprinting. In *Proc. Communications, Internet, and Information Technology*, 2004.

[16] Suman Jana and Sneha Kumar Kasera. On fast and accurate detection of unauthorized wireless access points using clock skews. In *Proc. ACM International Conference on Mobile Computing and Networking*, 2008.

[17] Michel Mouly and Marie-Bernadette Pautet. *The GSM system for mobile communications*. Europe Media Duplication, 1993.

[18] Senthilkumar Chinnappa Gounder Periaswamy, Dale R. Thompson, and Jia Di. Ownership transfer of RFID tags based on electronic fingerprint. In *Proc. International Conference on Security and Management*, 2008.

[19] Senthilkumar Chinnappa Gounder Periaswamy, Dale R. Thompson, and Jia Di. Fingerprinting RFID tags. *IEEE Transactions on Dependable and Secure Computing*, PrePrints(99), 2010.

[20] Senthilkumar Chinnappa Gounder Periaswamy, Dale R. Thompson, Henry P. Romero, and Jia Di. Fingerprinting radio frequency identification tags using timing characteristics. In *Proc. Workshop on RFID Security - RFIDsec Asia*, 2010.

[21] K. Rasmussen and S. Čapkun. Implications of radio fingerprinting on the security of sensor networks. In *Proc. International ICST Conference on Security and Privacy in Communication Networks*, 2007.

[22] Donald R. Reising, Michael A. Temple, and Michael J. Mendenhall. Improved wireless security for GMSK-based devices using RF fingerprinting. *Int. J. Electron. Secur. Digit. Forensic*, 3(1):41–59, March 2010.

[23] Donald R. Reising, Michael A. Temple, and Michael J. Mendenhall. Improving intra-cellular security using air monitoring with RF fingerprints. In *Proc. IEEE Wireless Communications and Networking Conference (WCNC)*, Apr 2010.

[24] Henry P. Romero, Kate A. Remley, Dylan F. Williams, and Chih-Ming Wang. Electromagnetic measurements for counterfeit detection of radio frequency identification cards. *IEEE Transactions on Microwave Theory and Techniques*, 57(5):1383–1387, 2009.

[25] Henry P. Romero, Kate A. Remley, Dylan F. Williams, Chih-Ming Wang, and Timothy X. Brown. Identifying RF identification cards from measurements of resonance and carrier harmonics. *IEEE Transactions on Microwave Theory and Techniques*, 58(7):1758–1765, 2010.

[26] D. Shaw and W. Kinsner. Multifractal modeling of radio transmitter transients for classification. In *Proc. IEEE Conference on Communications, Power and Computing*, 1997.

[27] O. Ureten and N. Serinken. Detection of radio transmitter turn-on transients. In *Electronic Letters*, volume 35, pages 1996–1997, 2007.

[28] O. Ureten and N. Serinken. Wireless security through RF fingerprinting. *Canadian Journal of Electrical and Computer Engineering*, 32(1), Winter 2007.

[29] M.D. Williams, M.A. Temple, and D.R. Reising. Augmenting bit-level network security using physical layer RF-DNA fingerprinting. In *IEEE Global Telecommunications Conference (GLOBECOM)*, pages 1–6, Dec 2010.

[30] Davide Zanetti, Boris Danev, and Srdjan Čapkun. Physical-layer identification of UHF RFID tags. In *Proc. ACM Conference on Mobile Computing and Networking*, 2010.

Appendix A: Equipment and Components of our Acquisition Setup

Table 1 lists the equipment and components deployed to build our acquisition setup. The element naming follows the labeling in Figure 2.

Table 1: Equipment and components of our acquisition setup.

Label	Description	Manufacturer	Model
AN1	Directive antenna GSM	Vimcom	171770
AM1	Ultra low-noise amplifier	Mini-Circuits	ZX60-1215LN+
AM2	Wideband voltage amplifier	FEMTO	DHPVA-200
AM3	Wideband voltage amplifier	FEMTO	DHPVA-200
MX1	Frequency Mixer	Mini-Circuits	ZFM-4H+
MX2	Frequency Mixer	Mini-Circuits	ZFM-4H+
PS1	Power Splitter, 2 Way-0°	Mini-Circuits	ZAPD-1+
PS2	Power Splitter, 2 Way-90°	Mini-Circuits	ZX10Q-2-12+
FI1	Bandpass Filter	Mini-Circuits	VBFZ-925+
FI2	Low-pass filter	Mini-Circuits	VLFX-80
FI3	Low-pass filter	Mini-Circuits	VLFX-80
SG1	Analog signal generator	Agilent	N5181A
OS1	High performance oscilloscope	Agilent	DSA90804A
-	Cabling (several lengths)	Huber+Suhner	S04262D
-	Cabling (several lengths)	Huber+Suhner	K02252D

Appendix B: Device Population

Table 2 lists the devices we consider in our experiments.

Table 2: Deployed devices.

Code	Manufacturer	Model	Number[1]
M1	HTC	Touch	-
M2	Apple	Iphone 3G	-
M3	Nokia	6020	-
M4	Wondex	ST100	001
M5	Wondex	ST100	228
M6	Wondex	ST100	224
M7	Wondex	ST100	227
M8	Wondex	ST100	223
M9	HTC	Desire	05
M10	HTC	Desire	07
M11	HTC	Desire	14
M12	HTC	Desire	23
M13	HTC	Desire	24
M14	HTC	Desire	27
M15	HTC	Desire	32
M16	HTC	Desire	35
M17	HTC	Desire	37
M18	HTC	Desire	39

[1] This is an arbitrary identifier we assign to same model and manufacturer devices in order to distinguish them.

Appendix C: Explored Features

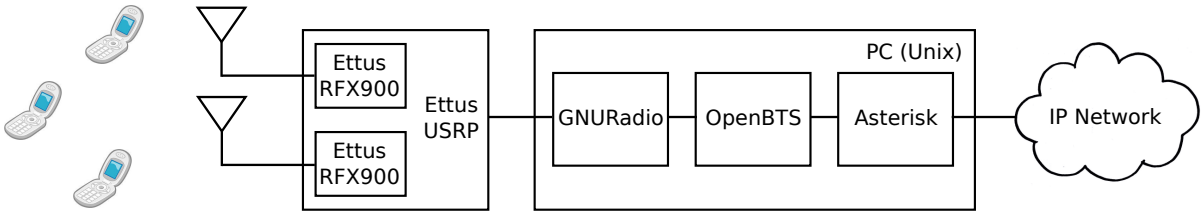
Table 3 lists the signal features we consider in our experiments.

Table 3: Considered Features

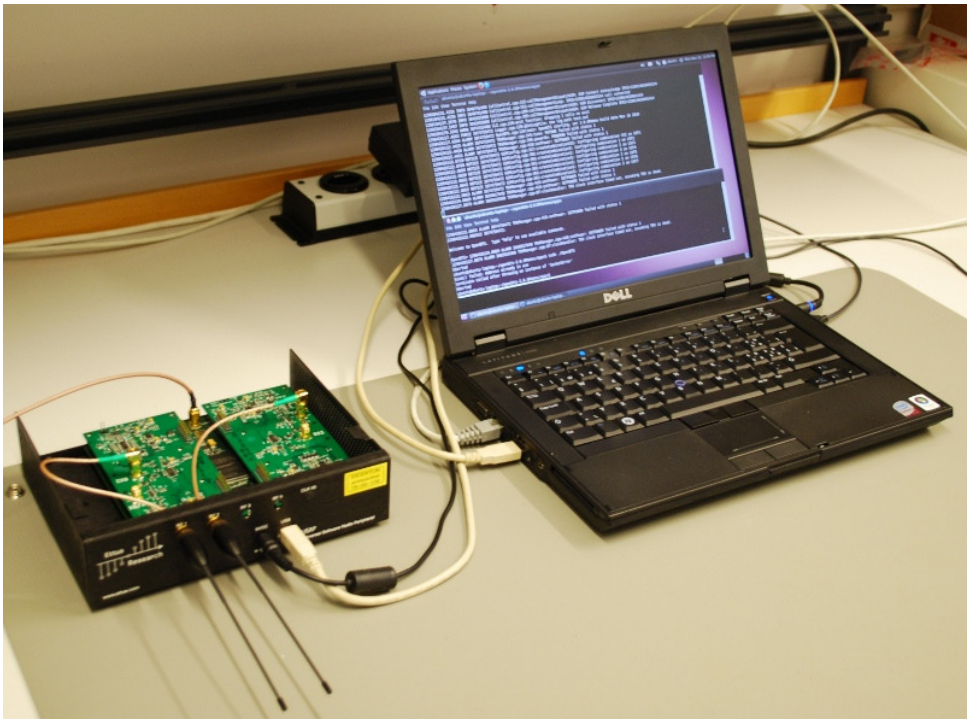
	Signal part	Feature
ϕ_{ON}	Turn-on transient	Instantaneous phase
ϕ_{OFF}	Turn-off trans.	Instantaneous phase
$\phi_{ON,OFF}$	Turn-on and -off trans.	Instantaneous phase
f_{ON}	Turn-on trans.	Instantaneous frequency
f_{OFF}	Turn-off trans.	Instantaneous frequency
$f_{ON,OFF}$	Turn-on and -off trans.	Instantaneous frequency
e_{ON}	Turn-on trans.	Power envelope
e_{OFF}	Turn-off trans.	Power envelope
$e_{ON,OFF}$	Turn-on and -off trans.	Power envelope
ϵ_{ϕ}	Training sequence (data)	Phase error
ϵ_{f}	Training sequence (data)	Frequency error
$E_{\phi_{TS}}$	Training sequence (data)	Phase error - Bit spectral components
$E_{f_{TS}}$	Training sequence (data)	Frequency error - Bit spectral components
$S_{\phi_{TS}}$	Training sequence (data)	Phase error - Bit statistical metrics
$S_{f_{TS}}$	Training sequence (data)	Frequency error - Bit statistical metrics

Appendix D: Our OpenBTS-based GSM network

Figures 23(a) and 23(b) show the blocks that compose our GSM network implementation and the actual implementation.



(a)



(b)

Figure 23: Our GSM network implementation: (a) basic blocks and (b) actual implementation.

Appendix E: Collected Datasets

Table 4 lists the collected datasets for our experiments.

Table 4: Collected data. TS stands for Training Sequence.

Dataset	Device M Table 2	# of Devices	# acquired burst per M, P_d, L, ST	Power P_d	Position L Figure 4	Training Sequence TS	Total # acquired burst per device	Network	Sampling rate [GS/s]	Downmixing frequency [MHz]
1	M1-M4	5	250	9, 17, 25dBm	L0	0	750	OpenBTS	1	850
2	M1-M4	5	250	17dBm	L1	0	250	OpenBTS	1	850
3	M4-M8	5	200	9dBm	L0	0	200	OpenBTS	0.1	888.2
4	M11, M13-M16	5	200	9dBm	L0	0	200	OpenBTS	0.1	888.2
5	M9-M18	10	200	5, 25, 33dBm	L2	0	200	OpenBTS	0.1	888.2
6	M4, M6-M8	4	200	Network	L2	Network (1)	200	Swisscom	0.1	902.4
7	M13-M16	4	200	Network	L2-L6	Network (1)	1000	Swisscom	0.1	902.4
8	M1-M5	5	250	Network	L0	0	250	OpenBTS	1	850
9	M1-M5	5	250	31dBm	L0, L1, L8	0	750	OpenBTS	1	850
10	M9-M18	10	200	5dBm	L0	0	200	OpenBTS	0.1	888.2
11	M9-M18	10	600	25, 29, 33dBm	L2	0	1800	OpenBTS	0.1	888.2
12	M9-M18	10	600	29dBm	L2	0,2,7	1800	OpenBTS	0.1	888.2
13	M9-M18	10	600	29dBm	L3	0,2,7	1800	OpenBTS	0.1	888.2
14	M18	1	200	9dBm	L2-L6	0	4000[1]	OpenBTS	0.1	888.2
15	M18	1	200	9dBm	L2-L6	0	4000[2]	OpenBTS	0.025	889.2
16	M18	1	200	Network	L2	0	200	OpenBTS	0.2	888.2

[1] Explored 4 different calling method: one single call for all the 5 different position, one call at each position, one call at each position with the microphone on mute, one call at each position with the microphone with voice.

[2] As Dataset 15, but signals were collected at the baseband.