SPECIFIC EMITTER IDENTIFICATION FOR GSM CELLULAR TELEPHONES

by

Jeevan Ninan Samuel

Submitted in partial fulfilment of the requirements for the degree
Master of Engineering (Computer Engineering)

in the

Department of Electrical, Electronic and Computer Engineering
Faculty of Engineering, Built Environment and Information Technology

UNIVERSITY OF PRETORIA

January 2018

SUMMARY

SPECIFIC EMITTER IDENTIFICATION FOR GSM CELLULAR TELEPHONES

by

Jeevan Ninan Samuel

Supervisor:	Prof. W. P. du Plessis
Department:	Electrical, Electronic and Computer Engineering
University:	University of Pretoria
Degree:	Master of Engineering (Computer Engineering)
Keywords:	Specific emitter identification, feature extraction, GSM.

GSM cellular telephones are identified by a 15-digit number that resides in the memory of the cellular telephone. This number, or international mobile equipment identity (IMEI), is also used when granting network access to a cellular telephone. The caveat with the usage of IMEI is that it is easy to access and manipulate. This allows for a malicious user to masquerade as another user on a Global System for Mobile Communications (GSM) network and thereby gain illegitimate access to the network. Therefore, there is a need to identify cellular telephones in a manner that is difficult to manipulate and spoof.

This study investigates specific emitter identification (SEI) as a way of identifying GSM cellular telephones using the analogue radio frequency (RF) transmissions of the cellular telephone. Second to that the research investigates the sensitivity of SEI to changes in the transmission characterisitcs of the cellular telephone, signal degradation and the usage of different receivers. This research found that it is possible to identify GSM cellular telephones with a peak accuracy of 88.26%. Futhermore, it is shown that SEI is sensitive to the transmission power of a GSM cellular telephone. Classification accuracy of cellular telephones drops with an increase in transmission power of the cellular telephone. Furthermore, it is shown that GSM cellular telephones cannot be accurately identified when multiple receivers are used, even if the receivers are nominally identical. However, the receivers used for this experiment were low cost and low quality receivers. Hence, the result may not generalise to higher quality receivers. Lastly, it is shown that the SEI technique renders poor accuracy (below 60%) when the signal-to-noise ratio (SNR) is below 9 dB.

LIST OF ABBREVIATIONS

ADC analogue-to-digital converter

ARFCN absolute radio frequency channel number

AuC authentication center

AWGN additive Gaussian white noise

BCCH broadcast control channel

BPF band-pass filter

BTS base transceiver station

COTS commercial off-the-shelf

EER equal error rate

EIR equipment identity register

ETSI European Telecommunications Standards Institute

FAR false acceptance rate

FDMA frequency-division multiple access

FIR finite impulse response

FRR false rejection rate

GMSC gateway mobile services switching centre

GMSK Gaussian minimum shift keying

GSM Global System for Mobile Communications

HLR home location register

HSN hopping sequence number

IF intermediate frequency

IMEI international mobile equipment identity

IQ in-phase and quadrature

KNN k^{th} nearest neighbour

LDA linear discriminant analysis

LPF low-pass filter

MDA multiple discriminant analysis

ML maximum likelihood

MS mobile station

MSC mobile switching center

NB normal burst

PCA principal component analysis

POI probability of intercept

RF radio frequency

RFF radio frequency fingerprinting

RFID radio frequency identification

RICA Regulation of Interception of Communications and Provision of Communication-related Information Act

ROC receiver operating characteristic

SDR software-defined radio

SEI specific emitter identification

SFH slow frequency hopping

SNR signal-to-noise ratio

SVM support vector machine

TAR true acceptance rate

TDMA time-division multiple access

USRP universal software radio peripheral

VLR visitor location register

TABLE OF CONTENTS

CHAPTER 1 INTRODUCTION

1.1 PROBLEM STATEMENT

1.1.1 Context of the problem

Every GSM cellular telephone has a unique number referred to as the IMEI number that is associated with it. GSM networks inspect this number for validity against a database called the equipment identity register (EIR) prior to granting access to the network [1]. However, it is possible to access and change the IMEI number via specialist software and tools [2]. The means of changing IMEI numbers is easily illustrated online in tutorials [3]. The effect of this is that cellular telephones become more difficult to authenticate on networks.

This inability to validly authenticate users has led to the usage of GSM cellular telephones in criminal activities. This is evident in the usage of cellular telephones in rhino poaching activities [4, 5], kidnapping syndicates [6] and cellular phone subscription fraud [7]. The passing of the Regulation of Interception of Communications and Provision of Communication-related Information Act (RICA) further emphasises that this problem is prevalent in South Africa [8].

SEI provides a means of enhancing the authentication of GSM cellphones. SEI, also known as radio frequency fingerprinting (RFF) or physical-layer identification, provides a means of identifying RF transmitters even if they are of the same make and model. The technique relies on analysing the analogue characteristics of the transmitted RF signal for signal artifacts due to hardware tolerances [9]. In this way, SEI provides a means of combatting changes to the IMEI number of GSM cellular telephones as the analogue characteristics analysed in SEI are inherently difficult to control and alter [10]. SEI has been proven to be unaffacted by spoofing or replay attacks when applied to RF access control remotes [11].

SEI has been proven to work for different wireless technologies including GSM [10–12].

1.1.2 Research gap

While SEI has been applied to GSM cellphones, the overall number of devices considered in these studies has been small [13]. Moreover, the robustness of SEI with respect to device transmission parameter variations and positions relative to the SEI system has not been considered. Lastly, the effects of the multiple receivers on an SEI system's classification performance has not been explored.

1.2 RESEARCH OBJECTIVES AND QUESTIONS

Given the aforementioned research gaps, the following research questions are posed:

1. What classification accuracy is achievable for a set of GSM cellular telephones?
2. What effect does transmission power and frequency have on the signal characteristics of GSM cellular telephone signals?
3. Which kind of classifier yields the highest classification accuracy for the same features?
4. Can GSM SEI be successfully applied across multiple receivers?
5. How does signal degradation affect classification accuracy?

1.3 HYPOTHESIS AND APPROACH

The hypothesis can be formulated as follows: The differences in the radio signals produced by the transmitters of GSM mobile stations (MSs) as a result of manufacturing tolerances are sufficient to uniquely distinguish between nominally identical MSs.

A proof-of-concept SEI system was built and tested to verify the aforementioned hypothesis. The proof-of-concept SEI system was implemented as shown in Figure 2.3. The various components of the system are described below.

1. The base transceiver station (BTS) was implemented using an emulated BTS system and a digital receiver. The rationale for using an emulated BTS was to allow for control of various transmission parameters such as transmission power and frequency so that the effects of these parameters on classification accuracy and signal characteristics may be observed.
2. Signal acquisition was implemented using a commercial off-the-shelf (COTS) software-defined radio (SDR) that is capable of capturing signals in the E-GSM-900 uplink band (880 MHz to 915 MHz) as the research focused on this particular frequency band.

3. Signal post-processing was implemented in software where the stored signal samples captured by the acquisition subsystem are processed. This allowed for noise to be added to the recorded signals so as to measure the effects of signal degradation on the SEI process.

4. Feature extraction was implemented in software and converted post-processed signals into features. This was done to determine which type of features produced the best classification accuracy.

5. The classifier was implemented in software to uniquely associate a set of features with a particular GSM cellular telephone. This ultimately verifies the feasibility of the SEI process and helps determine the comparative performance of different classifiers.

This proof-of-concept system was developed to firstly test the SEI technique of being able to identify cellular telephones. Secondly, by subjecting this system to signal degradation and changes in transmission power and frequency, the effect of these changes can be quantified by observing the classification performance and feature vectors produced by said system. In this way, research questions pertaining to signal degradation, transmission power effects and transmission frequency effects can be answered.

1.4 RESEARCH GOALS

The main goal of this research is to determine whether SEI can uniquely identify cellular telephones as well as investigate the robustness of SEI to varying transmission parameters, use of multiple receivers, low quality receivers and degradations in signal quality.

1.5 RESEARCH CONTRIBUTION

The research will contribute to the current body of knowledge in the following ways listed below.

- The effects of signal degradation on the classification accuracy of an SEI system will be presented. From this it can be determined how robust the SEI technique is to poor SNR typically faced in a real-world scenario.
- The effects of varying transmission power on both signal characteristics and classification performance will be presented. Analysing signal characteristics at varying transmission power will aid in understanding changes in transmission power would have on the classification accuracy of an SEI system. This is particularly important because cellular telephones vary their transmission power when operating with real-world GSM networks.

- The effects of varying transmission frequency on both signal characteristics and classification performance will be presented. This will aid in understanding what changes in transmission frequency have on the classification accuracy of an SEI system. Similar to the point above, this is important to consider because real-world GSM networks use frequency hopping. Thus the frequency of GSM cellular telephones is expected to vary in a real world context.
- The effects of applying the SEI process over multiple receivers is considered. This answers the question of whether features derived from signals recorded from one receiver can be used to effectively identify phones whose signals have been recorded on a different receiver.
- Furthermore, since this research considers a larger set of nominally identical cellular telephones than what is seen in the literature, the scalability of the SEI technique is explored in terms of determining whether more nominally identical cellular telephones degrades performance. This will aid in concluding whether the GSM technique is feasible for usage in a GSM network as there is a large number of cellular telephones that operate on the network.

1.6 RESEARCH OUTPUTS

The output of the research is as follows:

- A software system that demonstrates the capability of SEI that can be utilised for future research.
- A dataset of recorded GSM bursts pertaining to several GSM cellular telephones that can be utilised for future research.

1.7 OVERVIEW OF STUDY

The rest of the study is organised as follows:

- Chapter 2 presents a literature study of SEI.
- Chapter 3 describes the proof-of-concept system used to achieve the various measurements required to formulate the results. The chapter presents the design of the proof-of-concept system together with rationale for various design choices of the system.
- Chapter 4 presents a description of the various experiments used to answer the research questions posed. Furthermore, this chapter presents an analysis of the results attained.
- Chapter 5 summarises results, concludes the study and provides recommendations for future work.

CHAPTER 2 LITERATURE STUDY

2.1 INTRODUCTION

This chapter presents an overview of concepts relevant to this study. An overview of the GSM infrastructure together is presented, followed by a presentation of a typical SEI system architecture and SEI system design considerations.

2.2 GSM OVERVIEW

GSM is a wide area wireless communication system developed by European Telecommunications Standards Institute (ETSI) to provide and co-ordinate voice, data and multimedia communication services [14]. The depiction of the GSM system architecture is shown in Figure 2.1.

The architecture consists of components that facilitate the switching of GSM calls (such as the gateway mobile services switching centre (GMSC) and mobile switching center (MSC)), storage of service subscribers information (as with the home location register (HLR) and visitor location register (VLR)) and security as in the case of the EIR and authentication center (AuC). The air or Um interface between a MS and BTS was focused on for this study. A MS is any device (typically a cellular telephone) that communicates with a BTS using radio signals in order to access the cellular network. The area serviced by a BTS is called a cell. Normally, the MS transmits its IMEI, encrypted, over this interface to identify itself to the BTS.

At the physical layer, there are a number of factors that affect the signal acquisition and classification process. These include time-division multiple access (TDMA), frequency-division multiple access (FDMA), slow frequency hopping (SFH), Gaussian minimum shift keying (GMSK) modulation and power control [15].

FDMA works by assigning a user an available channel from a limited set of channels in the frequency domain [15]. Each channel has a spacing of 200 kHz [14] and has a number associated with it referred to as the absolute radio frequency channel number (ARFCN) [15]. In a pure FDMA system, once a frequency has been assigned to a user, it is used exclusively by the user [15].

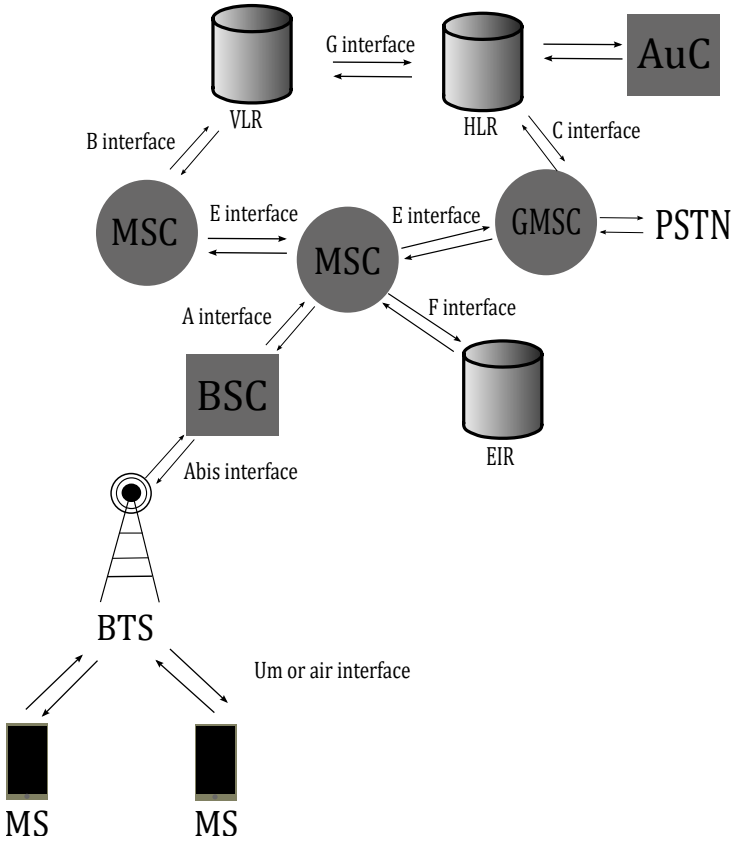


Figure 2.1. GSM architecture [14].

TDMA in GSM allows multiple users to share a single frequency channel. To achieve this, the time usage of a channel is divided into 8 time slots and multiple users are allowed to transmit for a fixed period of time on a particular time slot [15]. According to the GSM standard, the length of a time slot is 577 μs [16]. During a single time slot, the MS's transmitter performs a power ramp-up, transmits data for a period of 542 μs and then performs a power-ramp down. This produces a pulsed transmission within a time slot that is referred to as a GSM burst. Multiple types of GSM bursts exist, but this study utilises the structure of the GSM normal burst (NB) as this is the most common type of burst in the GSM system [15]. The NB is depicted in Figure 2.2. The tail and training bits are the same for multiple bursts from MSs operating within the same cell [15]. Thus these sections of the GSM burst are used to distinguish between MSs as they provide the true signal difference between MSs without any data-dependent bias.

The implementation of SFH in GSM allows the frequency allocations of a number of established calls to change from one frequency channel to another over the period of a TDMA frame. This is done to reduce frequency-selective fading as the MS moves around within a cell [15].

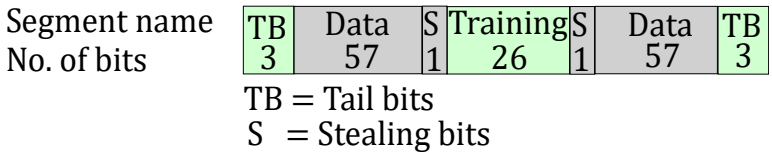


Figure 2.2. GSM Normal Burst [15].

The implications of TDMA are that a signal acquisition system will have to de-interleave the GSM bursts in different time slots as they pertain to different MSs. The implications of FDMA and SFH are that a system used for acquiring the GSM signal will have to be able to monitor a wide range of channels (i.e. have a large bandwidth). Alternatively the hopping sequence number (HSN) can be obtained from the broadcast control channel (BCCH), and the signal acquisition system can be dynamically tuned to follow the transmission frequency of the MS [15].

GSM also implements RF power control to compensate for the signal attenuation of MSs transmitting at different distances away from the BTS so that power arriving at the BTS's receiver is approximately the same for each time slot [15]. The BTS performs power control in steps of 2 dB, and this may vary during a single voice call [15].

2.3 SPECIFIC EMITTER IDENTIFICATION SYSTEM ARCHITECTURE

Historically, SEI has been applied in military contexts, typically for tracking radars [9]. Recently, the technology has been applied to identifying wireless devices for the purpose of enhancing device authentication [17]. This has been applied to a wide variety of wireless devices. Of concern to this study is the application of SEI to GSM cellular telephones.

A SEI system typically works by sampling a radio signal from a device and thus acquiring it. This signal may be processed to remove noise and other variances in the signal. Thereafter, metrics used to uniquely identify the signal (referred to as features) are derived from the radio signal. These features are then presented to a classifier which uniquely associates the radio signal with a specific device [17]. This is depicted in Figure 2.3. From Figure 2.3 it is seen that the system consists of an acquisition subsystem, signal post-processing, a feature extraction subsystem and classifier subsystem.

2.3.1 Acquisition subsystem

The acquisition subsystem serves to acquire and digitise (without significant degradation) a radio signal from the concerned wireless device [17]. In order to reduce signal degradation due to noise, acquisition subsystems typically use high-quality signal measurement equipment [13, 18].

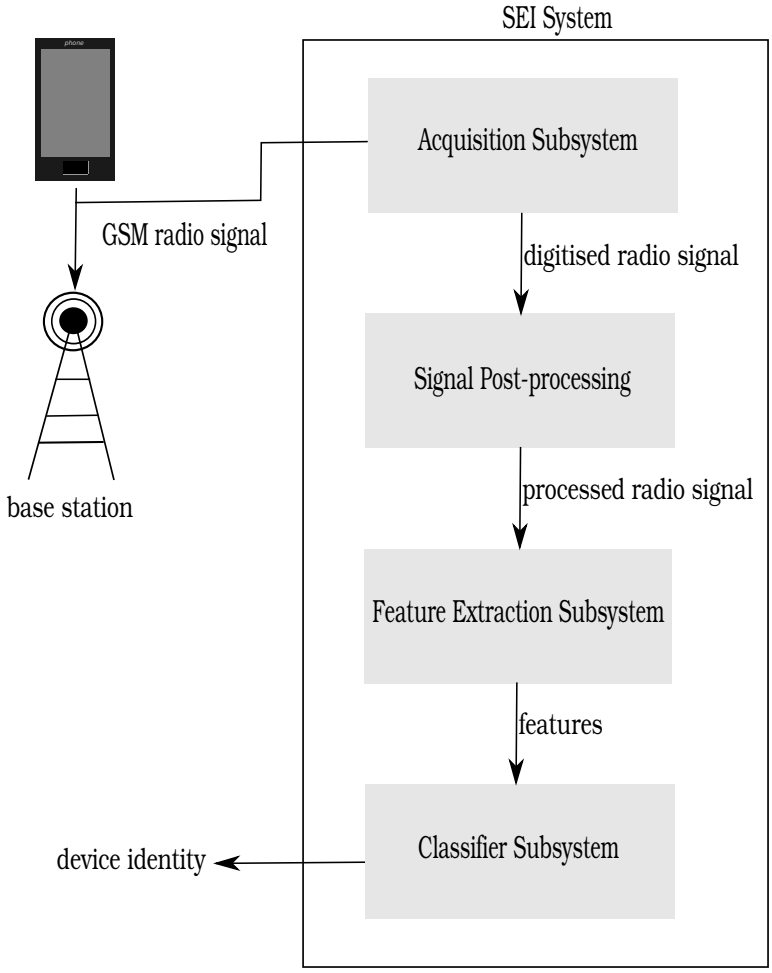


Figure 2.3. SEI System Architecture [17].

Signal acquisition may take place in either an active or passive fashion. In active acquisition, the wireless device to be identified is requested to transmit the radio signal and thereafter the acquisition subsystem samples it [17]. This form of acquisition has only been applied to radio frequency identification (RFID) tags [17]. In passive signal acquisition, the radio signal is obtained from the device to be identified while it is communicating with other devices [17]. Passive signal acquisition has been applied to the identification of GSM cellular telephones during communication with real or emulated base stations [10, 13, 18–20].

As mentioned in Sect. 2.2, GSM devices send data via pulsed transmissions referred to as bursts. In order to identify GSM cellular telephones, the acquisition subsystem must be able to capture and digitise GSM bursts. This is typically done by applying a threshold to signal samples and capturing signal samples that exceed this threshold [10, 13, 20]. It is also possible to acquire GSM bursts by interpreting GSM samples between both the cellular telephone and base station and cross-referencing

it against the GSM protocol applied during a voice call in order to identify samples pertaining to a GSM burst [18]. The former method has the advantage of only sampling the cellular telephone's signal and is thus less computationally intensive than the latter method. However, the threshold acquisition method may suffer in a practical context where multiple bursts from multiple phones may be perceived as belonging to a single cellular telephone [18]. This is because multiple phones can transmit on the same frequency using TDMA, as mentioned in Sect. 2.2.

Regardless of the method used to acquire GSM bursts, a challenge typically faced by acquisition subsystems used for GSM SEI is frequency hopping. In order to deal with frequency hopping, acquisition subsystems sample the frequency range the device is expected to transmit over, which in the case of GSM is wide [10, 13, 20]. This implicates the need for signal acquisition equipment that can observe a wide frequency band. Alternatively, dynamically retuning the acquisition subsystem's receiver frequency to hop with the cellular telephone could be performed [18]. Real-time retuning would require an *a priori* knowledge of the frequency hop sequence which would need to be derived from the base station in turn requiring demodulation of base station signals.

The GSM bursts may be acquired either by interactions with real cellular network base stations [13, 18–20] or emulated ones [10]. The argument for using real GSM network base stations is that it presents a scenario that is more representative of real world application of SEI [13, 18–20]. However, the primary goal of this research is to determine whether SEI is at all possible and whether the technique is sensitive to changes in the transmission power and frequency of MSs. In this way, the need for being able to control various transmission parameters using an emulated BTS is motivated.

2.3.2 Signal post-processing

Following acquisition of the radio signal via the acquisition subsystem, the signal is post-processed prior to feature extraction. This post-processing is done to remove arbitrary variances between signals due to noise, linear phase offsets and amplitude differences that would occlude the true differences in signal traits [13,18–20]. Noise and frequency offsets in the case of GSM SEI are typically removed by down-converting the signal to 0 Hz and thereafter filtering it with a 135 kHz low-pass filter [13,19,20]. Linear phase offsets and amplitude variances are removed by linear phase component removal and normalisation respectively [13, 19, 20].

2.3.3 Feature extraction

The feature extraction subsystem serves to extract numerical metrics from post-processed radio signals from a particular device that can be used to uniquely distinguish it from radio signals from other devices [17]. These numerical metrics, or features, are later passed on to a classifier for the purpose of identification. As such, these features should exhibit several properties in order to ensure that they can be successfully used for classification. These properties are presented below [17]:

- Universality - The set of considered devices should be able to produce the features.
- Uniqueness - No two devices should possess the same feature values.
- Permanence - Features should be invariant over time.
- Collectability - The features should be extractable from signals using available signal sampling and digitisation equipment.
- Robustness - Features should be invariant to external environmental conditions (such as interference from other devices), position relative to the acquisition subsystem and device related aspects such as transmission power.

Features can be predefined or inferred [17]. Predefined features are derived from signal transmission error specifications or known signal regions pertaining to a particular kind of transmitter [17]. Inferred features are derived from signal characteristics that are not known prior to extraction and are produced by some means of spectral transformation [17]. For the application of SEI to GSM cellular telephones, predefined features are used [10, 13, 18–20]. These predefined features are further classified into signal-region-based features [13,19,20], transient-based features [10], and modulation-based features [18].

Signal-region-based features target specific regions of a GSM burst. These signal regions correspond to the training and tail bits of the GSM burst, and in the literature are referred to as near-transient and midamble signal regions respectively [13, 19]. These signal regions, as mentioned in Sect. 2.2, relate to data or bits that remain constant across along all cellular telephones operating within the same cell region. This cancels any data specific differences in the generated features between devices. From the signal regions, phase and amplitude is computed from the signal samples. In some cases the raw phase and amplitude is used in the classifier [10], and in other cases statistical measures (skewness (γ), standard deviation (σ) and kurtosis (k)) derived from the phase and amplitude are used in the classifier [13, 19, 20].

Transient based features target the turn-on and turn-off transient of a radio signal for feature extraction [17]. The transient may also include a portion corresponding to the tail-bits of a GSM burst [20].

Similar to signal-region-based features, phase and amplitude are calculated from the samples corresponding to the transient region. An additional domain considered by the transient based approach is signal power envelopes [10].

Modulation-based feature extraction focuses on extracting unique features from the part of the signal that has been modulated [17], particularly looking at the errors created during modulation. Specifically, in the case of GSM, extracted GSM bursts are demodulated to extract bit information. Thereafter, the bit information is passed to a simulated modulator to create an ideal modulated signal, from which amplitude, phase and frequency errors are computed [10, 18]. This differs from modulation-based approaches used in the identification of devices based on the IEEE 802.11 standard which, in addition to the aforementioned errors, also consider SYNC correlation and I/Q origin offset [21].

In all three feature extraction methods, it is found that phase features render more discriminatory information than amplitude and frequency features. This was determined by comparing the classification accuracy produced using phase, frequency and amplitude features in isolation [10, 13, 18–20]. Signal-region-based features derived from the near-transient region of the signal produce higher classification accuracy as compared to features derived from the midamble region [13, 19]. This is due to the fact that the near-transient region of the signal derives from turn-on and turn-off transient of the GSM burst which has less strict signal restrictions [19].

2.3.4 Dimensionality reduction

Features produced using the aforementioned feature extraction techniques may produce a number of overlapping or irrelevant features (i.e. features that do not add any discriminatory information). Also processing patterns with a large number of features increases the computational complexity of the underlying classification system. This is referred to as the curse of dimensionality [22]. Dimensionality reduction entails removing features that are irrelevant, thereby reducing the number of features under consideration. The benefit of this is two-fold. It reduces the amount of computation during classification and enhances the classification accuracy. The two prominent techniques for dimensionality reduction are principal component analysis (PCA) and multiple discriminant analysis (MDA).

MDA is a multi-class extension of the Fisher linear discriminant analysis (LDA) method. It involves the projection of features from a d-dimensional space to a $c-1$ dimensional space, where d corresponds to the number of features and c is the number of classes [22]. PCA reduces the dimensionality of features by maintaing only those features that have the greatest variance among classes [23]. MDA has been successfully applied to reduce the dimensionality of features considered prior to classification by a maximum likelihood (ML) classifier [13, 19, 20].

2.3.5 Classifier

The classifier subsystem serves to uniquely associate a radio signal with a particular transmitter [22]. These classifiers in the context of GSM SEI are implemented as a nearest neighbour classifier using some distance metric or more sophisticated classifiers such as ML classifiers and support vector machines (SVMs) [17].

Nearest neighbour classifiers calculate a distance of a set of features to an existing database of features sets and associates that set of features with the class corresponding to the feature set that has the smallest distance to it [24]. In the case of GSM SEI applications, a k^{th} nearest neighbour (KNN) classifier using Euclidean distance is typically used [10]. Since these classifiers maintain all sets of features for all classes considered, it presents a large storage requirement on the classifier system [24]. Since it is a non-parametric, instance-based learning algorithm, it is more accommodating to a large number of classes [24].

Sophisticated classifiers such as SVMs and ML classifiers, do not maintain a dataset of all features pertaining to all classes. Rather, the classifiers are trained via a series of examples, where a particular signature is presented to the classifier with its corresponding class label. In this way, it estimates parameters for learning and only maintains the parameters, or a smaller set of training data in comparison to the nearest neighbour classifier [24]. From this it can be seen that there is no large storage requirement imposed by such classifiers. However, if a new class is to be introduced, the classifier may need to be retrained to estimate the new class's parameters [24], making dynamic or online learning more difficult for such classifiers [25]. GSM SEI has utilised SVMs [18] and MDA ML classifiers [13, 19, 20].

Ensemble learning serves to combine or leverage the power of multiple classifiers in order to attain a higher classification accuracy [26]. The principal idea behind ensemble learning is that of a committee of individuals that complement each other is better at making decisions than a single individual on his/her own [26]. This principle may be described as the Mixture of Experts [27,28] in which a gating function establishes weights for the constituent or base classifiers. A higher weight indicates more confidence in the result of the classifier. An underpinning assumption of this approach is that the base classifiers are specialised to identify particular classes. Other techniques for ensemble learning such as bagging and boosting exist [29].

In order to measure the performance of the classifiers, various metrics can be applied. Literature concerning fingerprinting GSM devices utilise confusion matrices [13,19,20], equal error rate (EER) [10] and true acceptance rate (TAR) [18] to quantify the performance of classifiers used. Confusion

matrices are matrices in which diagonal entries show the percentage of correct classifications and off-diagonal entries show the percentage a class was confused with another class [13, 19, 20]. Confusion matrices therefore provide both a measure of classification accuracy and the rate at which an imposter class can be accepted by the classifier. EER is derived from receiver operating characteristic (ROC). A ROC plots the false rejection rate (FRR), the probability of rejecting a genuine device, against different false acceptance rate (FAR), the probability of accepting a false device [17]. EER is the error rate where both FAR and FRR are equal [10]. TAR is the probability of classifying a device correctly [18]. The caveat of TAR is that it does not capture the acceptance of false instances nor the rejection of genuine instances [17].

In the literature concerning GSM SEI, the comparative performance of different classifiers is not presented. However, in the application of SEI to IEEE 802.11 devices, it was found that a SVM provided a TAR of 99.66% whereas a KNN classifier provided a TAR of 97% [21]. Both classifiers utilised signal-region-based features. This therefore suggests that in the case of GSM using the same type of features, SVMs should out-perform KNN classifiers.

2.4 SEI SYSTEM DESIGN CONSIDERATIONS

The performance of a SEI system is underpinned by identification accuracy, computational speed, cost and security [17]. In addition to this, the scalability of the system, that is the number of devices the SEI system can identify, is important to consider. Lastly, as mentioned in Sect.2.3.3, SEI systems must be robust in terms of the features used. These design considerations are presented with respect to what has been achieved in the relevant literature.

2.4.1 Identification accuracy

The identification accuracy (in terms of TAR) of GSM SEI systems in the literature can be structured in three categories: identification accuracy when different make and model devices are considered (inter-manufacturer classification) [13, 19, 20], identification accuracy of devices when devices of the same make and model are considered (intra-manufacturer classification) [13, 19, 20] and identification accuracy when both different and same model devices are considered [18].

Inter-manufacturer identification accuracy is around 90% at a SNR of 6 dB using near-transient phase features [13, 19]. An intra-manufacturer identification accuracy of 90% or more can be achieved at a SNR of 20 dB or greater using transient phase features [20]. The identification accuracy when both different and same make and model devices are considered is 97.62% at a SNR of 5.4 dB using phase-error features [18]. However, only a quarter of the devices considered in the last scenario were

of the same make and model.

From this it becomes evident that intra-manufacturer identification is more challenging, as compared to the inter-manufacturer case, at lower SNR levels.

2.4.2 Computational speed and cost

The cost of an SEI system is coupled to the speed and quality of equipment used during signal acquisition and processing [17]. Higher quality acquisition systems, which are typically used in the state of the art [10, 13, 18–20], are necessary as low-quality receivers typically create two problems. The first is lower-quality receivers degrade the classification accuracy of an SEI system [30]. The second problem is that low-quality receivers suffer from their own manufacturing imperfections which appear in the features generated during feature extraction. Consequently, the features generated through one low-cost receiver will differ from another for the same transmitter [30].

The issue of computational speed may not be tied to the computation equipment itself but rather the number of GSM bursts required in order to produce a robust set of features [18]. It was determined that for phase-error modulation-based features, 4500 training GSM bursts render the best classification accuracy. However, this requires recording a GSM voice call for 21 seconds [18]. Given that GSM authentication takes place before the setup of a call [15], it may be desired to reduce this recording time so as to speed up the call setup process.

2.4.3 Security

The premise behind using SEI for GSM device identification is that the device signatures produced by SEI are difficult to impersonate and thus enhance device authentication [13, 20]. However, the actual resilience of SEI systems to impersonation attacks has not been extensively considered [17]. This highlights the vulnerability of such systems to impersonation attacks.

It was determined in an investigation using SDRs that by replaying transmitted signals, modulation-based features are vulnerable to impersonation, while transient-based features are vulnerable to attack at specific locations [31]. However, using low-cost receivers in the acquisition subsystem makes it more difficult to perform an impersonation attack [30]. The vulnerability of signal-region-based features has not been explored, but holds promise for resilience against replay attacks [17].

2.4.4 Scalability

It is important that a SEI system is capable of distinguishing a large number of devices, even devices of the same make and model, or nominally identical devices. In the current body of research pertinent to GSM SEI, relatively few (between 4 and 10) nominally identical devices are considered for identification [10, 13, 18–20]. However, in the case of IEEE 802.11 device identification, a much larger number of 130 nominally identical devices were considered [21]. Given that IEEE 802.11 device identification utilises features similar to those utilised for GSM device identification [19], it is possible that GSM SEI could scale to identify a large number of nominally identical devices.

2.4.5 Robustness

It is also important that the SEI system be robust in the sense that it is invariant to the location of the device relative to the acquisition subsystem and varying transmission power of the device [17].

In the case of GSM SEI it was determined that transient-based features were partially sensitive to device location relative to the acquisition subsystem [10]. Modulation-based features were found to be invariant to distance by testing identification at two separate distances away from the acquisition subsystem [18]. Noting that only distance was varied and not the orientation of the device relative to the acquisition antennae, the effect of varying location on modulation-based features is still uncertain. The same holds true for signal-region-based features [13, 19, 20].

The effects of varying transmission power are more profound. It was determined that matching features extracted at different transmission power levels lead to inaccurate device identification [10]. Furthermore, it appears that at lower transmission power, more discriminatory information exists in the transmitted radio signal [10].

2.5 SUMMARY OF LITERATURE STUDY

The application of SEI to GSM has proven to be successful with a small set of GSM devices. High accuracy is possible at low SNR when the majority of the dataset consists of different make and model devices. When the devices under consideration consist of nominally identical devices, a higher SNR is required in order to achieve the same accuracy. Furthermore, the majority of the research focuses on a single type of classifier at a time. Thus the comparative performance of classifers for GSM SEI is unknown.

The focus of the current body of knowledge concerning GSM SEI is on feature development and feature extraction, as well as their sensitivity to location and power transmission. Only predefined

features have been explored. These predefined features are further broken down into 3 groups, namely signal-region-based, modulation-based and transient-based features. The sensitivity of transient and modulation-based features was explored and these features were found to be only partially sensitive to location relative to the acquisition receiver, and completely sensitive to device transmission power. Features derived from the phase representation of the signal was shown to yield more discriminatory information relative to features derived from amplitude and frequency.

Only MDA has been considered for the purposes of dimensionality reduction in the context of GSM SEI.

The resilience of the aforementioned features to impersonation attacks has been explored through the use of SDRs. It was shown that modulation-based features are vulnerable to impersonation, while transient-based features are vulnerable to attack at specific locations. The resilience of signal-region-based features has not been explored.

The method for acquiring and recording signals typically employ high-quality and costly signal sampling equipment. This incurs a large cost for the acquisition portion of a SEI system. When low-quality receivers are used, it is seen that features will vary among the different receivers for the same transmitter to be identified. However the effect of low-quality equipment on classification accuracy in comparison to high-quality quality equipment is not explored.

CHAPTER 3 PROOF-OF-CONCEPT SYSTEM DESCRIPTION

3.1 OVERVIEW

This chapter presents the design of a proof-of-concept SEI system that was utilised for all the experiments. The design of this proof-of-concept system is adapted from a SEI system developed as part of a 2013 final year project at the University of Pretoria [12]. The specific algorithms and signal processing techniques utilised are detailed together with rationale for how these aspects of the system aided in answering the research questions.

3.1.1 Conceptual design

The functional blocks of the proof-of-concept system are depicted in Figure 3.1.

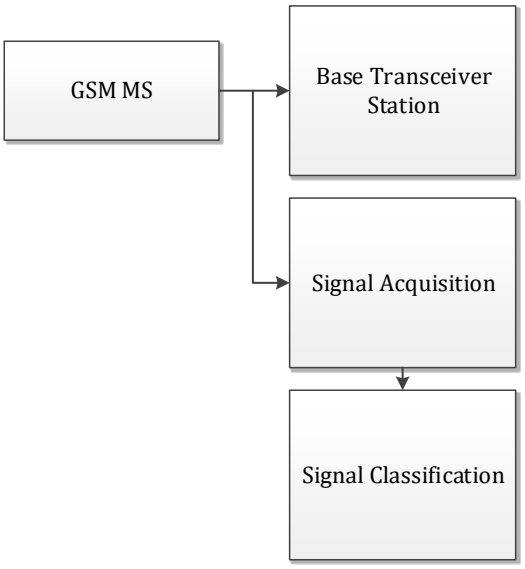


Figure 3.1. Functional block diagram for SEI system.

3.1.1.1 Base Transceiver Station

A BTS, as described in the literature review, communicates with a MS using radio signals and provides the MS with access to the cellular network. It communicates through the Um interface on a downlink frequency with the MS, and the MS in return communicates with the BTS on an uplink frequency. The signals transferred across this interface must be obtained and processed by signal classification block for the unique identification of a MS.

3.1.1.2 Signal Acquisition

Signal acquisition block serves to intercept and obtain signals transmitted on the Um interface on an uplink frequency for later processing by signal classification block. This functional unit does not consider signals transmitted on the downlink frequency as they pertain to the BTS and hence would characterise the transmissions of the BTS and not the MS. As a final step in the signal acquisition phase, burst extraction is performed. Burst extraction serves to extract only the samples corresponding to a GSM burst and ignores the remainder of the samples. In addition to extracting only the relevant information from the recording, burst extraction serves to reduce memory storage requirements. This is seen in the way the average size of sample data, containing about between 400 to 900 GSM bursts, is 320 MB in size while burst extracted data for 1000 bursts is about 20 MB in size. These values were ascertained by observing the file sizes.

3.1.1.3 Signal Classification

Signal classification block serves to process the signals acquired by signal acquisition block and uniquely map the signal to an originating MS. This functional unit is sub-divided as seen in Figure 3.2.

3.1.1.3.1 Post-processor

The signals obtained by signal acquisition block have arbitrary variances within them that distort the true representation of a MS's GSM bursts. These variances are due to noise, phase offsets and amplitude variations. These variances must therefore be accounted for and removed prior to classification of the signal. The post-processor serves this purpose.

3.1.1.3.2 Feature Extractor

The feature extractor takes in the post-processed signal and derives a series of numerical values that serve as features for the signal. The resultant series of values is referred to as a feature vector.

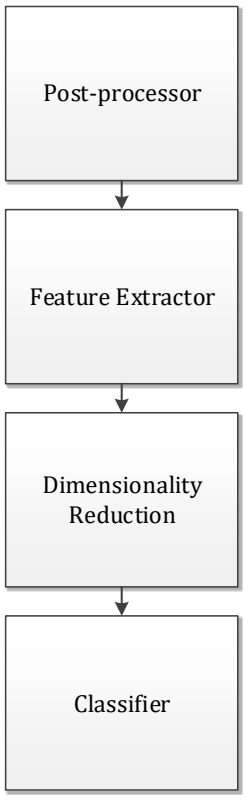


Figure 3.2. Functional unit 3 sub-units for SEI system.

3.1.1.3.3 Dimensionality Reduction

As was specified in the literature review, as the number of feature dimensions considered increase beyond a certain point, classification performance degrades due to redundancy or overlap in various feature dimensions. Dimensionality reduction serves to reduce the number of features under consideration.

3.1.1.3.4 Classifier

The classifier takes in a dimensionally reduced feature vector and associates with it a particular class, which in this context is the identity of a MS.

3.2 PROOF-OF-CONCEPT SYSTEM RESEARCH ALTERNATIVES

For each of the previously mentioned functional units, a number of research alternatives were considered. The paragraphs that follow detail these alternatives and rationale for choosing between the alternatives.

3.2.1 Base transceiver station research alternatives

For the BTS, two alternatives were considered. The BTS could either operate as part of a real cellular telephone network or be part of a self-contained cellular network (i.e. a cellular network that was privately maintained by the author). In the former case, the merit is that one would not need to actively set up the BTS. Calls would simply need to be established between an MS and BTS belonging to a cellphone network, and signals would need to be acquired. The problem with using a real BTS would be that the signals transmitted to and from the BTS would be subject to variations in transmission power and frequency as dictated by the BTS. These variations have an effect on the signals acquired and therefore would cause a loss in the repeatability of results if they vary constantly. Furthermore, there is no guarantee that a MS will connect to the same BTS repeatedly, which adds another dimension of variation. In the case of using a self-contained network, the BTS is controllable and consequently, so are the aforementioned parameters (i.e. transmission power and frequency). This allows for consistent data to be obtained and processed by the system. It further enables the exploration of system performance under varying conditions which is a key goal of this research. Provided one BTS is maintained by the self-contained cellphone network, the MS will consistently connect to it, eliminating the variation seen in the use of a real cellphone network. In this way, sensitivity of the SEI process can be researched using this controlled ad-hoc cellular network.

3.2.2 Signal acquisition research alternatives

Several off-the-shelf components exist for the purposes of signal acquisition. A number of these devices were considered and compared in terms of bandwidth, sampling rate, frequency tuning range, ADC bits and cost. Bandwidth and sampling rate provides an indication of how much of a particular frequency range is observable simultaneously by the device and has an effect on probability of intercept (POI) of the signals. Sampling rate also provides an indication of how accurately a signal can be represented. The higher the sampling rate, the more accurate the representation. The frequency tuning range refers to the range of frequencies the device can tune to. The ADC bits provide an indication of the range of values that the device can represent.

Given that this research focuses on the acquisition of GSM bursts in the GSM-900 band, it was paramount that the chosen component is able to tune to between 900 MHz and 915 MHz. Second to this, the sampling rate and analogue-to-digital converter (ADC) resolution of the component were the other important specifications to consider. This is due to the fact that, as mentioned earlier, SEI process relies on picking up minor signal characteristics due to hardware tolerance. When trying to distinguish between signals produced by nominally identical cellular telephones, these signal characteristics are more difficult to pick up, necessitating high sampling rates and ADC resolution. Instantaneous bandwidth is less important because a controlled cellular network is utilised thus eliminating the need to simultaneously observe a wide bandwidth. Based on this aspect, the Nuand bladeRF was chosen for the majority of the experiments as it was capable of high sampling rates (higher than 10 MHz), had a high 12-bit ADC resolution for the cost and could tune to the relevant GSM frequency band. A DVB-T based tuner was used in an experiment, which will be elaborated on later, to determine the effect of using multiple receivers in an SEI setup. This receiver was chosen because of its low cost allowing for three receivers to be used in the experiment.

3.2.3 Post-processing research alternatives

The first step to post-processing is to filter the signal and down-convert it to baseband. Two alternatives exist for this process, namely, to first band-pass filter the signal and then down-convert, or first down-convert the signal then low-pass filter it. The first of the two approaches requires that the band-pass filter (BPF) be adaptive in the sense that it should be able to filter the signal at its intermediate frequency (IF), which in this case may vary due to SFH and FDMA. The second approach is preferred as the low-pass filter (LPF) need not be adaptive. It only needs to filter the down-converted representation of the received signal.

3.2.4 Dimensionality reduction research alternatives

A number of different techniques exist to reduce the dimensionality of feature vectors. Those methods considered include PCA, MDA and forward feature selection.

PCA is a mathematical technique that considers a data set of multiple feature vectors, each feature vector containing many features, and determines those features that account for most variability in the entire data set [23]. However, PCA does not consider the grouping of observations into classes [32]. Consequently, PCA cannot distinguish between the variations within classes and between classes, and produces features that are a mixture of these variations [23]. As a result, PCA may fail in yielding features that provide discriminatory information.

MDA, on the other hand, takes into account class information. It aims to find a projection on which to project a large number features to produce a reduced number of features. The projection is found such that it best separates the classes under consideration, while minimising separation within a particular class [22, 33]. For this reason, MDA is more applicable to the classification problem at hand.

Another possible means of reducing the features under consideration is to employ forward feature selection. Feature selection entails selecting a subset of features from a larger feature set in order to reduce dimensionality and improve classification accuracy [34]. However, forward selection usually entails some search of the feature space, which may be exhaustive or greedy. An exhaustive search is computationally expensive [35]. While a greedy (or hill-climbing) search is less computationally intensive, it will only yield a local optimum [24]. Furthermore, over-fitting of the data may result from forward feature selection [36]. For these reasons forward feature selection was not considered in this research.

3.2.5 Classifier research alternatives

Three classifiers have been used for the purposes of SEI. Non-parametric distance based classifiers [10], ML classifiers [13, 19, 20, 37] and a SVM [18].

The merit of using a non-parametric distance based classifiers is that it makes no assumptions of the underlying distribution of the features [22]. Furthermore, such classifiers generalise well provided various parameters in the classifier are adjusted [24]. A non-parametric distance-based classifier which is considered for this research is the KNN classifier. KNN computes a distance of a test feature vector to an existing set of feature vectors and associates with it the most occurring class among its nearest neighbours. The advantage of KNN is that it requires no training stage [24]. A set of feature vectors is maintained by the classifier and serve to classify new test feature vectors presented to the classifier. This lack of training implies that a new class can be added to the classifier by simply adding the relevant feature vectors and corresponding class labels. The disadvantage of KNN is that it performs a sequential evaluation of many distances, which is computationally intensive. This may be alleviated through the use of binary trees or hashing to perform distance evaluation [24]. KNN can also be improved through parallelisation [38].

Another non-parametric classifier is the SVM. It works by maintaining a maximum margin separator between classes using training feature vectors transformed to higher feature dimensions pertaining to the various classes [22]. SVMs are promising as they generalise well, and by adjusting the kernel function of the underlying decision boundary, non-linear decision boundaries can be achieved [24]. The disadvantage of SVMs is that, to add a new class to the classifier, the SVM must be retrained

to accommodate the new class. This is undesirable as each MS to be classified forms a separate class. Also SVMs are only directly applicable to binary classification tasks and must be modified or cascaded for multi-class operation [22, 24].

Probabilistic classifiers, such as the ML classifier, are regarded as parametric as they use parameters derived from training feature vectors (such as the mean and covariance) to discriminate between classes [39]. The benefit of using such classifiers is that the relative likelihood of a feature vector belonging to a particular class is provided [39]. This likelihood gives a confidence value of a feature vector belonging to a particular class. If this confidence falls below a certain value for all possible classes, it maybe used to classify the feature vector as belonging to an unknown class. The disadvantage of such classifiers are that they are computationally expensive for higher dimensional feature spaces, and make the assumption that the distribution of feature vectors in a particular class are normally distributed [40], which may not be the true distribution of the features.

This research focuses on distance based classifiers and the SVM classifier.

3.2.6 Program structure

Based on the overall design of the SEI system, the data presented to the program would be processed in the following discrete stages:

- Signal acquisition.
- Signal post-processing.
- Feature extraction.
- Dimensionality reduction.
- Classification.

3.2.6.1 Signal acquisition stage

In this stage, a script is called to sample data from a cellular telephone using a SDR. Following this a separate program reads the sampled data and extracts GSM bursts from it, as described in Algorithm 1.

3.2.6.2 Signal post-processing stage

In this stage, the individual extracted GSM bursts are down converted to base band and filtered using an N order finite impulse response (FIR) filter. Random linear offsets in the phase offsets in the GSM burst are corrected and the burst is scaled between 0 and 1.

Data: Complex I and Q sample data (**IQ**)

Result: Array of GSM bursts (GSM_**IQ**)

Compute threshold; burst_time $\leftarrow$ 542 μs;

transient_time $\leftarrow$ 28 μs;

sample_rate $\leftarrow$ 8 MHz;

burst_samples $\leftarrow$ burst_time $\times$ sample_rate;

transient_samples $\leftarrow$ transient_time $\times$ sample_rate;

threshold $\leftarrow$ 0.5$\times$ μ ;

above_threshold $\leftarrow$ find **IQ** > threshold;

difference_components $\leftarrow$ compute difference of above_threshold samples twice;

break_points $\leftarrow$ find difference_components not equal to 0;

break_points $\leftarrow$ break_points + 1;

start $\leftarrow$ 1; count $\leftarrow$ 1; k $\leftarrow$ 1;

data_length $\leftarrow$ length of **IQ**;

while *k less than number of breaks_points-1* **do**

    end_ $\leftarrow$ break_points(k);

    if *length of start to end_ is between burst_samples and transient_samples* **then**

        if *start - 150* $\geq$ *0 and end_ + 150* $\leq$ *data_length* **then**

            burst_array(count) $\leftarrow$ Complex I and Q sample data from start to end_ ;

            increment count by 1;

        end

    end

    start $\leftarrow$ break_points(k+1);

    increment k by 2;

end

GSM_**IQ** $\leftarrow$ burst_array;

return GSM_**IQ**;

Algorithm 1: Algorithm for burst extraction.

3.2.6.3 Feature extraction stage

The feature extraction process (described in Algorithm 2) is used to produce a feature vector of statistical features (skewness (γ), standard deviation (σ) and kurtosis (k)) from a post-processed GSM

burst.

Data: Array of GSM bursts

Result: Feature vector of statistical features

Representations of GSM burst ← GSM bursts;

NR ← 5;

for *all representations of GSM burst* **do**

    N ← number of samples in representation;

    s ← ⌊ N/NR ⌋;

    for $m = 1$ *to NR* **do**

        g ← m × s;

        d ← (g-s)+1;

        segment ← representation from samples d to g;

        feature_vector(m) ← standardise([σ γ k of segment]);

    end

    feature_vector(m+1) ← standardise([σ γ k of entire representation]);

end

final_feature_vector ← concatenate feature_vector 1 to NR+1;

return final_feature_vector;

Algorithm 2: Algorithm for feature extraction.

3.2.6.4 Dimensionality reduction stage

MDA was utlised to perform dimensionality reduction on the produced feature vectors. MDA aims to reduce the dimensionality of data while maintaining discriminatory information between classes. It achieves this by optimising a measure of separation between classes. The best-known separation measure is the Fisher discriminant [22]. For a two-class problem, the Fisher discriminant is defined in Equation 3.1.

$$J(\mathbf{w}) = \frac{|\mu_1' - \mu_2'|^2}{\mathbf{s_1'^2} + \mathbf{s_2'^2}} \tag{3.1}$$

where:

- μ_i' is the class mean for class i projected on the vector $\mathbf{w}$.
- $\mathbf{s_i'}$ is the within class scatter for class i projected on the vector $\mathbf{w}$.

The goal of MDA in this two class problem is to find a vector $\mathbf{w}$ that maximises Equation 3.1. For this, Equation 3.1 must be expressed in terms of $\mathbf{w}$. Thus, the definitions for within-class scatter (as shown in Equation 3.2) and between-class scatter (as shown in Equation 3.3) [22].

$$\mathbf{S_W} = \mathbf{s_1} + \mathbf{s_2} \tag{3.2}$$

$$\mathbf{S_B} = (\mu_1 - \mu_2)(\mu_1 - \mu_2)^{\mathbf{T}} \tag{3.3}$$

where:

- $\mathbf{s_i} = \sum_{\mathbf{x} \in \mathbf{C_i}} (\mathbf{x} - \mu_\mathbf{i})(\mathbf{x} - \mu_\mathbf{i})^{\mathbf{T}}$
- $\mu_\mathbf{i}$ is the mean for class i.
- $\mathbf{x}$ is a feature vector.

If $\mathbf{s_i}'$ is $\mathbf{s_i}$ projected on the vector $\mathbf{w}$, then it can be seen that:

$$\mathbf{s_i'^2} = \sum_{\mathbf{x} \in \mathbf{C_i}} \mathbf{w}(\mathbf{x} - \mu_\mathbf{i})^\mathbf{2} = \sum_{\mathbf{x} \in \mathbf{C_i}} \mathbf{w^T}(\mathbf{x} - \mu_\mathbf{i})(\mathbf{x} - \mu_\mathbf{i})^\mathbf{T}\mathbf{w} = \mathbf{w^T s_i w} \tag{3.4}$$

From this, it can be seen that denominator of Equation 3.1 may be expressed as shown in Equation 3.5.

$$\mathbf{s_1'^2} + \mathbf{s_2'^2} = \mathbf{w^T}(\mathbf{s_1} + \mathbf{s_2})\mathbf{w} = \mathbf{w^T}(\mathbf{S_W})\mathbf{w} \tag{3.5}$$

Similarly, the numerator of Equation 3.1 may be expressed in terms of $\mathbf{w}$ and $\mathbf{S_B}$ as shown in Equation 3.6.

$$|\mu_\mathbf{1}' + \mu_\mathbf{2}'|^\mathbf{2} = \mathbf{w^T}(\mu_1 + \mu_2)(\mu_1 + \mu_2)^\mathbf{T}\mathbf{w} = \mathbf{w^T}(\mathbf{S_B})\mathbf{w} \tag{3.6}$$

Thus, the Fisher discriminant, expressed in terms of $\mathbf{w}$ is presented in Equation 3.7 below.

$$J(\mathbf{w}) = \frac{\mathbf{w^T}(\mathbf{S_B})\mathbf{w}}{\mathbf{w^T}(\mathbf{S_W})\mathbf{w}} \tag{3.7}$$

In order to maximise Equation 3.7, the first derivative of the equation is taken with respect to $\mathbf{w}$, set to 0 and $\mathbf{w}$ is solved for. Using this approach, a generalised eigenvalue problem as shown in Equation 3.8, is arrived at.

$$\mathbf{S_B w} = \lambda \mathbf{S_W w} \tag{3.8}$$

The optimum projection vector, **w**, is found as the eigenvector solving the generalised eigenvalue problem in Equation 3.8.

MDA expands the two-class problem presented above to a multi-class problem involving C classes by redefining the within-class scatter and between-class scatter as shown in equations 3.9 and 3.10 respectively [22].

$$\mathbf{S_W} = \sum_{\mathbf{i=1}}^{\mathbf{C}} \mathbf{s_i} \tag{3.9}$$

$$\mathbf{S_B} = \mathbf{N_i}(\mu_\mathbf{i} - \mu)(\mu_\mathbf{i} - \mu)^\mathbf{T} \tag{3.10}$$

where:

- $\mathbf{s_i} = \sum_{\mathbf{x} \in \mathbf{C_i}} (\mathbf{x} - \mu_\mathbf{i})(\mathbf{x} - \mu_\mathbf{i})^\mathbf{T}$
- $\mu_\mathbf{i}$ is the mean for class i.
- μ is the total mean for all the feature vectors in all the classes.
- C_i is a set of feature vectors belonging to class i.
- N_i is the number of feature vectors in class i.
- **x** is a feature vector.

In the multi-class case, a projection matrix **W** is found as opposed to a vector. The projection matrix, according to [22], is derived from the first C-1 eigenvectors corresponding to the largest eigenvalues of the generalised eigenvalue problem shown in Equation 3.11.

$$\mathbf{S_B W} = \lambda \mathbf{S_W W} \tag{3.11}$$

The solution of the above generalised eigenvalue problem is only possible when the within-class and between-class scatter matrices are invertible. Regularisation serves to avoid the aforementioned singularity (non-invertible matrices) problem and attain a more accurate estimate of the sample scatter matrices [41] by adding a diagonal component to the scatter matrices [33]. The form of regularisation applied to this project combines that seen in [42] and [43] as it adds the diagonal of the scatter matrix instead of an identity matrix scaled by an arbitrary constant, and is presented in Equation 3.12.

$$\mathbf{S'} = \mathbf{S} + \mathbf{D} \tag{3.12}$$

where:

- $\mathbf{S}'$ is the regularised scatter matrix.
- $\mathbf{S}$ is the original scatter matrix ($\mathbf{S_B}$ or $\mathbf{S_W}$).
- $\mathbf{D} = \mathbf{diag}((\mathbf{x} - \mu_\mathbf{i})(\mathbf{x} - \mu_\mathbf{i})^\mathbf{T})$ in the case of regularising $\mathbf{S_W}$.
- $\mathbf{D} = \mathbf{diag}((\mu_\mathbf{i} - \mu)(\mu_\mathbf{i} - \mu)^\mathbf{T})$ in the case of regularising $\mathbf{S_B}$.

In addition to regularisation, a whitening transformation is applied to the regularised between-class scatter matrix $\mathbf{S}'_\mathbf{B}$. Whitening, according to [44, 45], serves to transform a covariance matrix of possibly correlated variables to one where all variables are uncorrelated and have unity variance. The interpretation of this transformation when applied to the regularised version of $\mathbf{S_B}$ is that it finds the direction maximal variance between the class centers (i.e. performs PCA on the class centers of the training feature vectors) and thus finds a dominant direction that further enhances the separation between the class centers of the classes under consideration [46]. The whitening transform applied in this research is a variant of the eigenvalue decomposition method and is similar to the whitening technique shown in [46], and is presented in Equation 3.13.

$$\mathbf{S_B}'' = \mathbf{S_B}'\mathbf{V}\mathbf{D}\mathbf{V}^\mathbf{T}. \tag{3.13}$$

where:

- $\mathbf{S_B}''$ is the whitened between-class scatter matrix.
- $\mathbf{S_B}'$ is the regularised between-class scatter matrix.
- $\mathbf{V}$ are the eigenvectors of $\mathbf{S}'_\mathbf{B}$.
- $\mathbf{D}$ is a diagonal matrix with diagonal elements corresponding to the eigenvalues of $\mathbf{S}'_\mathbf{B}$.

Thus, in summary, this approach to MDA consists of the above mentioned regularisation to avoid singular matrices and whitening to enhance class separation and solves the generalised eigenvalue problem in Equation 3.14 to obtain the optimum projection matrix $\mathbf{W}$.

$$\mathbf{S}''_\mathbf{B}\mathbf{W} = \lambda\mathbf{S}'_\mathbf{W}\mathbf{W} \tag{3.14}$$

3.2.6.5 Classification stage

Feature vectors are then presented to the relevant classifiers. Four separate classifiers were considered, namely a KNN classifier, Mahalanobis distance-based classifier, SVM classifier and an ensemble classifier. The KNN classifier was implemented according to Algorithm 3. The SVM was implemented using LIBSVM [47]. The LIBSVM classifier was set to use a radial-basis kernel function to establish the decision boundary due the fact that radial-basis functions are better suited for features that cluster.

The ensemble classifier employs ensemble learning.

Ensemble learning combines the power of a number of classifiers to improve classification accuracy. For this sub-routine, the Mixture of Experts model was applied using KNN classifer and Mahalanobis distance classifier as the base classifiers. Instead of utilising a gating function that assigns weights to the base classifiers, the gating function used compares the distances produced by KNN classifier and Mahalanobis distance classifier in order to make a classification decision. The classification decision corresponds to the resultant class label that has the lowest distance between the two base classifiers. In order to effectively compare the distances produced by the base classifiers, they need to be scaled with respect to one another. This scaling is achieved by taking the ratio of mean Mahalanobis distances ($\mu_{Mahalanobis}$) to the mean KNN distances (μ_{KNN}) and scaling the Mahalanobis distances by this ratio, as shown in Equation 3.16. The distances are thereafter concatenated and standardised using Equation 3.17.

The portion of feature vectors utilised to train the classifiers are referred to as the training set, and the portion of the feature vectors used to test the classifiers' performance are referred to as the test set. The performance of each classifier was recorded under various conditions to quantify how performance is affected under those conditions. For classification experiments, 100 test feature vectors and 100 training feature vectors are used.

In the sections that follow, the algorithms for each of the classifiers is presented and explained.

3.2.6.5.1 KNN algorithm description

The KNN algorithm classifies an input feature vector by calculating the distance of the input feature vector to a database of feature vectors which are correspondingly labelled with cellular telephone identities. The classification label for the input vector is chosen according to the most occurring class label among the n^{th} nearest neighbours with the lowest distance to the input feature vector.

Data: Feature vector (**x**), training feature vectors (**tr**), class labels l and value for k

Result: Class labels and mean distance from nearest neighbours for each **x**

P ← number of feature vectors **x**;

Q ← number of training feature vectors **tr**;

for $p = 1$ *to* P **do**

  for $q = 1$ *to* Q **do**

    $\mathbf{x}' \leftarrow \mathbf{x}(\mathbf{p})$;

    $\mathbf{tr}' \leftarrow \mathbf{tr}(\mathbf{q})$;

    $d(q) \leftarrow \sum_{i=1}^{m} |\mathbf{x}'(\mathbf{i}) - \mathbf{tr}'(\mathbf{i})|$;

  end

  Sort d in ascending order;

  Sort l based on sorted indices of d;

  if $k > 1$ **then**

    nearest_neighbours ← l from 1 to k;

    class_result(p) ← most_occurring_class(nearest_neighbours);

    distance_result(p) ← $\frac{1}{k}\sum_{i=1}^{k} d(i)$;

  else

    class_result(p) ← $l(1)$;

    distance_result(p) ← $d(1)$;

  end

end

return class_result and distance_result;

Algorithm 3: Algorithm for KNN implemented in the function knn.

3.2.6.5.2 Mahalanobis distance-classifier algorithm description

The Mahalanobis classifier is constituted of two parts, namely an initialisation stage followed by a classification stage.

The initialisation stage serves to create a data structure that stores data containing the covariances of the feature vectors belonging to a particular class as well as the class mean values for feature vectors belonging to a particular class. The algorithm takes in an array of feature vectors, the class labels for the feature vectors and the number of classes considered in order to compute the mean and covariance for each class. The covariance ($\sum$), class means ($\mu_\mathbf{i}$) and total mean (μ) are stored in

the data structure (mahalanobis_struct) together with the class labels. Furthermore, regularisation is applied to the covariance matrix ($\sum$) of each class using Equation 3.12.

The algorithm takes in a number of training feature vectors (**tr**), corresponding class labels (l) and the number of classes (C) considered, and returns a data structure containing the class covariances ($\sum$), class means ($\mu_\mathbf{i}$) and class labels. The processing detail for the algorithm is presented in Algorithm 4.

Data: Training feature vectors (**tr**), class labels (l) and the number of classes (C)

Result: mahalanobis_struct

patterns_per_class $\leftarrow$ (number of training feature vectors)/(C);

for $p = 1$ *to* C **do**

  patterns_for_class_indices $\leftarrow$ (1+(p-1)patterns_per_class) to

   (patterns_per_class+(p-1)patterns_per_class);

  $\mathbf{C_i} \leftarrow$ **tr**(patterns_per_class_indices);

  $\sum$(p) $\leftarrow$ covariance of $\mathbf{C_i}$;

  $\mu_\mathbf{i}$(p) $\leftarrow$ mean of $\mathbf{C_i}$;

  class_label(p) $\leftarrow$ l(1 + (p-1)patterns_per_class);

end

mahalanobis_struct.c $\leftarrow \sum$;

mahalanobis_struct.class_mean $\leftarrow \mu_\mathbf{i}$;

mahalanobis_struct.label $\leftarrow$ class_label;

return mahalanobis_struct;

Algorithm 4: Algorithm for Mahalanobis initialisation.

The Mahalanobis distance of a feature vector **x**, as defined in Equation 3.15, measures the distance of **x** to a particular class mean ($\mu_\mathbf{i}$) by taking into account the covariance ($\sum$) of the corresponding class [24].

$$d_m = (\mathbf{x} - \mu_\mathbf{i}) \left(\sum\right)^{-\mathbf{1}} (\mathbf{x} - \mu_\mathbf{i}) \tag{3.15}$$

The mahalanobis classification algorithm assigns a class label to an input feature vector (**x**) using Mahalanobis distance as described in Equation 3.15. The algorithm returns the class label that corresponds to the class which has the lowest Mahalanobis distance from the feature vector (**x**) presented.

The algorithm takes in a number of feature vectors **x** and the mahalanobis_struct (containing covariances and class means), and returns a class label and Mahalanobis distance (d_m) for the feature vector

having the lowest Mahalanobis distance. The algorithm is presented in Algorithm 5.

Data: Feature vector (**x**) and mahalanobis_struct

Result: Class labels and Mahalanobis distance (d_m)

$\sum \leftarrow$ mahalanobis_struct.c;

$\mu_{\mathbf{i}} \leftarrow$ mahalanobis_struct.class_mean;

$l \leftarrow$ mahalanobis_struct.label;

number of classes $\leftarrow$ number of elements in l;

P $\leftarrow$ number of feature vectors in **x**;

Q $\leftarrow$ number of classes;

lowest_distance $\leftarrow$ inf;

for $p = 1$ *to* P **do**

  for $q = 1$ *to* Q **do**

    $d_m \leftarrow$ mahalanobis_dist(**x**(p), $\mu_{\mathbf{i}}$(q), $\sum$(q));

    if $d_m <$ *lowest_distance* **then**

      lowest_distance(p) $\leftarrow d_m$;

      class_label(p) $\leftarrow$ l(q);

    end

  end

end

return lowest_distance and class_label;

Algorithm 5: Algorithm for Mahalanobis distance classification.

3.2.6.5.3 Ensemble Classifier Algorithm Description

Ensemble learning combines the power of a number of classifiers to improve classification accuracy. For this algorithm, the Mixture of Experts model was applied using the KNN classifier and Mahalanobis distance classifer as the base classifiers. Instead of utilising a gating function that assigns weights to the base classifiers, the gating function used compares the distances produced by the base classifiers in order to make a classification decision. The classification decision corresponds to the resultant class label that has the lowest distance between the two base classifiers. In order to effectively compare the distances produced by the base classifiers, they need to be scaled with respect to one another. This scaling is achieved by taking the ratio of mean Mahalanobis classifier distances to

the mean KNN classifier distances and scaling the Mahalanobis classifier distances by this ratio, as shown in Equation 3.16. Thereafter the concatenated distances are scaled with Equation 3.17.

$$\mathbf{d_s} = \mathbf{d_{Mahalanobis}} \frac{\mu_{\mathbf{Mahalanobis}}}{\mu_{\mathbf{KNN}}} \tag{3.16}$$

where:

- $\mu_{Mahalanobis}$ is the mean of the Mahalanobis distances.
- μ_{KNN} is the mean of the KNN distances.
- $\mathbf{d_{Mahalanobis}}$ is the array of Mahalanobis distances prior to scaling.
- $\mathbf{d_s}$ is the array of scaled Mahalanobis distances.

$$\mathbf{d_m} = \frac{\mathbf{d} - \mu}{\sigma} \tag{3.17}$$

where:

- $\mathbf{d_m}$ is the modified array of concatenated distances.
- $\mathbf{d}$ is the concatenated array of distances.
- μ is the mean of the concatenated array of distances produced by each base classifier.
- σ is the standard deviation of the concatenated array of distances produced by each base classifier.

This approach assumes that the base classifiers are specialised to classify particular classes (i.e. behave in a complementary manner). Initial testing of KNN classifier and Mahalanobis classifier showed that they classified feature vectors in a complementary manner, making the aforementioned assumption valid and thus advocating the use of Mixture of Experts to form an ensemble classifier.

The ensemble classifier algorithm takes in the resultant distances ($\mathbf{d_m}$) and partitions them into corresponding class labels (l_m) and distances ($\mathbf{d'_{Mahalanobis}}$) for the Mahalanobis classifier. Similarly the same data is extracted for the KNN classifier ($\mathbf{d'_{KNN}}$ and l_k). It then returns a number of class labels corresponding to the lowest distances between the two classifiers. The algorithm processing details are presented in Algorithm 6.

Data: Mahalanobis distances ($\mathbf{d_m}$) and class labels l_m; knn distances $\mathbf{d}$ and class labels l_k

Result: Class labels

Scale $\mathbf{d_m}$ using Equation 3.16;

dist_vector $\leftarrow$ Concatenate $\mathbf{d}$ and $\mathbf{d_m}$;

dist_vector $\leftarrow$ standardise(dist_vector) (using Equation 3.17);

$\mathbf{d'_{knn}} \leftarrow$ first half of dist_vector;

$\mathbf{d'_{Mahalanobis}} \leftarrow$ second half of dist_vector;

$n \leftarrow$ number of distances;

for $p = 1$ *to* n **do**

  if $\mathbf{d'_{knn}}(p) \leq \mathbf{d'_{Mahalanobis}}(p)$ **then**

    class_label(p) $\leftarrow l_k$;

  else

    class_label(p) $\leftarrow l_m$;

  end

end

return class_label;

Algorithm 6: Algorithm for ensemble classifier

CHAPTER 4 EXPERIMENTS

4.1 OVERVIEW OF EXPERIMENTS

Several experiments were devised to address research objectives. The experiments and the research objective they address are listed in Tables 4.1 and 4.2:

Table 4.1. Description of experiments.

Experiment	**Description**	**Research Objective Addressed**
General SEI experiment	In this experiment, GSM bursts were sampled from multiple cellular telephones and classified.	Which features yield the highest classification accuracy? What classification accuracy is achievable for multiple cellular telephones?
Multiple low-cost receiver experiment	In this experiment, classifiers were trained using signals recorded from one receiver and tested using signals recorded from a separate receiver.	Can GSM SEI be successfully applied across multiple receivers?
Positional dependence experiment	In this experiment, the position of a single cellular telephone was varied and the signal characteristics were analysed.	What effect does device position relative to the acquisition antenna have on signal characteristics?

Table 4.2. Description of experiments continued.

Experiment	Description	Research Objective Addressed
Transmission frequency dependence experiment	In this experiment, the transmission frequency of a cellular telephone was varied over multiple recordings and the signal characteristics for each frequency were observed.	What effect does variations in the transmission frequency of the cellular telephone have on its signal characteristics?
Transmission power dependence experiment	In this experiment, the transmission power of a cellular telephone was varied over multiple recordings and the signal characteristics for each transmission power were observed.	Are GSM signal characteristics sensitive to variations in the transmission power relative of the cellular telephone being identified?
Effect of SNR on classification accuracy	In this experiment, noise was artificially added to cellular telephone recordings and the effects on classification accuracy were observed.	How does signal degradation affect classification accuracy?

4.2 CELLULAR TELEPHONE DATASET

The majority of the experiments utilise a signal and feature database derived from 15 cellular telephone as part of a 2013 final year project [12]. The data processing in the experiments has been updated from the final year project. Table 4.3 describes the make and model of the cellular telephones as well as the abbreviated labels for the cellular telephones used in the text. These cellular telephones were loaned from various students. It must be noted that SS33 was initially included in the dataset. However, the phone was no longer available for the end phases of testing and it was thus removed from the dataset.

Table 4.3. Description of cellular telephones utilised for experiments.

Make and model	Labels
Samsung S3	SS30-SS32, SS34-SS35
Samsung S2	SS20-SS24
Blackberry 8520	BB0-BB4

4.3 GENERAL GSM CELLULAR TELEPHONE CLASSIFICATION EXPERIMENT

In this experiment, the dataset of GSM bursts produced by the cellular telephones presented in Table 4.3 were processed by the proof-of-concept SEI system. The aim of the experiment was to compare the performance of various types of features in terms of the classification accuracy they render. Furthermore, the experiment aimed to investigate how the classification accuracy of the proof-of-concept SEI system varied with changes in the transmission power of the cellular telephones considers.

4.3.1 Experiment setup

This experiment utilises the general SEI system architecture as shown in Figure 3.1. The experiment was conducted by training the classifiers with data derived from one call and tested with data pertaining to a separate call to ensure the classification accuracy was consistent between different calls. For each cellular telephone, 100 training feature vectors were used to setup or train the classifiers while 100 test feature vectors were used to evaluate the performance of the classifiers.

4.3.2 Results and discussion

The classification accuracy results obtained at different MS transmission powers when all MSs are considered simultaneously are presented in Figures 4.1 to 4.3.

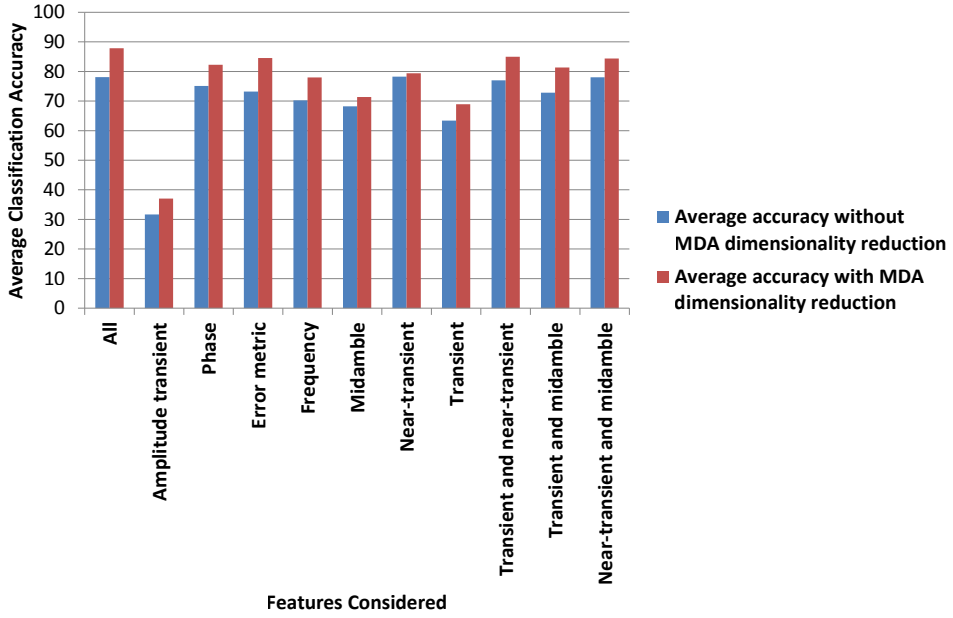


Figure 4.1. Classification accuracies for different features considered for GSM bursts obtained at a transmission power of 9 dBm.

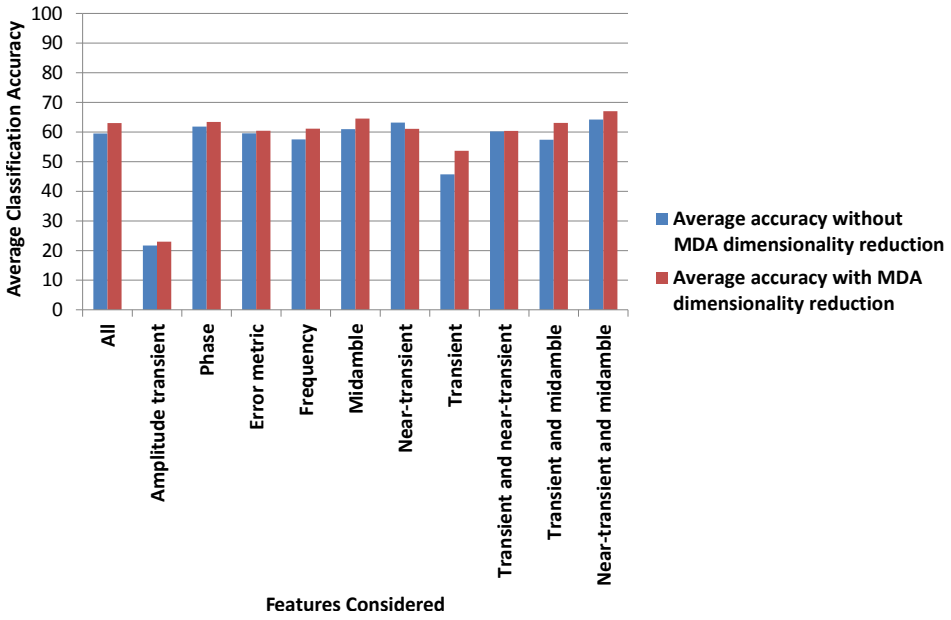


Figure 4.2. Classification accuracies for different features considered for GSM bursts obtained at a transmission power of 19 dBm.

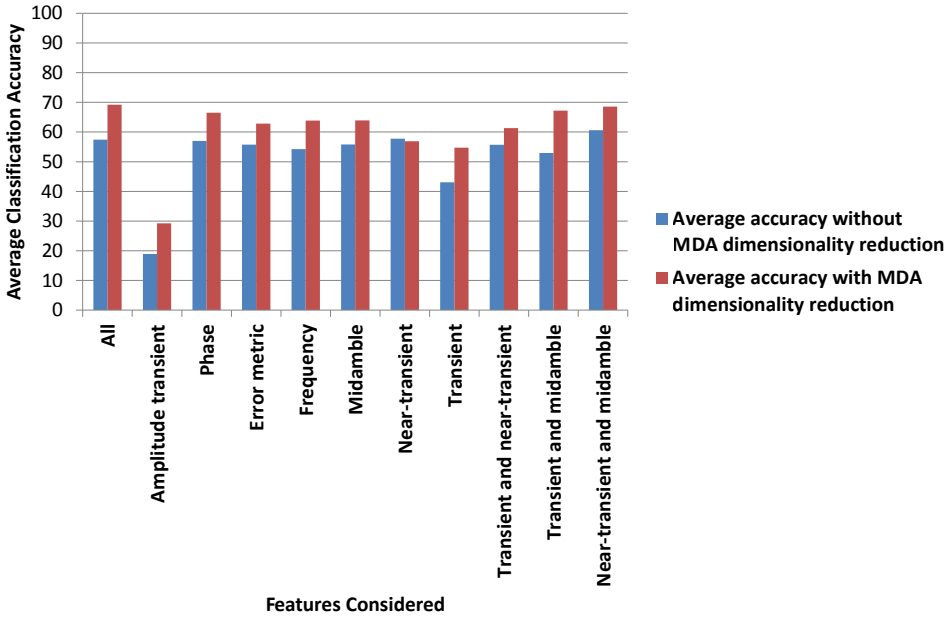


Figure 4.3. Classification accuracies for different features considered for GSM bursts obtained at a transmission power of 29 dBm.

Figure 4.1 shows a bar graph of average classification accuracies for different features considered when signal acquisition was performed at a MS transmission power of 9 dBm. The average classi-

fication accuracy is calculated as the mean of all the classifier accuracies. The features considered include all feature types concatenated, amplitude features, phase features and frequency features of the GSM burst. Furthermore, features corresponding to the transient, near-transient and midamble regions of the signal as well as combinations thereof were considered. When features for a particular region of interest were considered, it consisted of the phase and frequency features belonging to that region of interest. Figures 4.2 and 4.3 show the same data, but for signals acquired at transmission powers of 19 dBm and 29 dBm respectively.

Based on the above figures, the best classification results are achieved at a MS transmission power of 9 dBm when MDA dimensionality reduction is applied. The peak classification accuracy achieved in this case is 88.26%. Poorer classification accuracies (when no dimensionality reduction is applied) are achieved when the transmission power of a MS is increased. However, with dimensionality reduction applied, the classification accuracies in the 29 dBm transmission power case surpass those in the 19 dBm case.

Furthermore, it is observed that MDA dimensionality reduction enhances classification accuracy. When all features are considered together, the best classification accuracy is achieved, while the poorest classification accuracy is achieved with the amplitude transient features. Phase features render the most discriminatory information when compared to amplitude and frequency features (when MDA is not applied). Furthermore, the transient and near-transient regions of the GSM burst appear to render more discriminatory information than the midamble region of GSM burst.

Tables 6.1 to 6.9 in Appendix 6.1 present the confusion matrices for all MSs considered simultaneously, using all features with dimensionality reduction applied.

Table 6.1 to Table 6.3 show the confusion matrices derived from the results of the KNN classifier for different MS transmission powers. Once again, the prevailing trend is a degradation in classification accuracy as the transmission power of a MS is increased. While the best classification results are achieved at a power setting of 9 dBm, it must be noted that some classes of MSs are still poorly identified (as in the case of the bb0 and ss24 MSs). Tables 6.4 to 6.6, as well as Tables 6.7 to 6.9 show the same information, but for the Mahalanobis classifier and the ensemble classifier respectively. In Tables 6.10 to 6.12, the same information is presented for a SVM classifier. The SVM classifier was derived from LIBSVM [47] and developed by Chih-Chung Chang and Chih-Jen Lin. The SVM classifier was tested using a radial basis kernel. All classifiers considered exhibited the same trend of poorer classification accuracy with an increase MS transmission power. This is due to the increased randomness and noise in the signal as transmission power is increased.

The comparative performance of the different classifiers is presented in Table 4.4. As in the case of the confusion matrices, the results are computed for the scenario where all MSs are considered simultaneously, for all features considered and with MDA dimensionality reduction applied. The values in Table 4.4 are the percentage of correct classifications for the relevant classifier.

Table 4.4. Comparison of classifier performance.

	9 dBm	**19 dBm**	**29 dBm**
KNN classifier	87.60%	62.47%	69.13%
Mahalanobis classifier	87.67%	63.53%	69.00%
Ensemble classifier	88.26%	63.07%	69.53%
SVM classifier	85.40%	62.00%	68.27%

As seen in Table 4.4, the distance-based classifiers out-perform the SVM classifier under all conditions. Furthermore, it is observed that the ensemble classifier has slightly superior performance when compared to its base classifiers, except for the 19 dBm case.

Thus in summary, it is observed that a peak classification accuracy of 88.26% is achievable provided the MS consistently transmits GSM bursts with low power and signals are obtained at a high SNR (30 dB or more). Furthermore, a degradation in classification accuracy (without dimensionality reduction applied) is observed when MS transmission power is increased. Finally, it is seen that the distance-based classifiers out-perform the SVM classifier under all conditions.

4.4 POSITIONAL DEPENDENCE EXPERIMENT

4.4.1 Experiment setup

To determine whether there existed a positional dependence in the signal characteristics of the GSM bursts, a number of signal recordings were taken at three different positions relative to the bladeRF's receiver, as seen in Figure 4.4. The MS used for these tests was bb1 from the BlackBerry 8520 dataset. The OpenBTS network parameters were held constant at an ARFCN of 75 and GSM.MS.Power of 9 dBm.

In Figure 4.4, the positions p0 to p1 are where the MS was positioned during the experiment. The distance from the receiver (L) varied between 0.1 to 0.5 cm. In order to obtain GSM bursts with high SNR, the MS had to be placed extremely close to the receiver (without any antenna attached). However, in some cases putting the MS too close (i.e. 0.1 cm) to the receiver caused the obtained

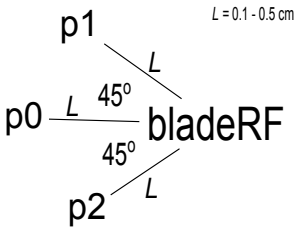


Figure 4.4. Positional dependence experiment set up.

signal to be saturated, thus necessitating the further distance of 0.5 cm.

4.4.2 Results and discussion

The results of the experiment are presented in Figures 4.5 to 4.7.

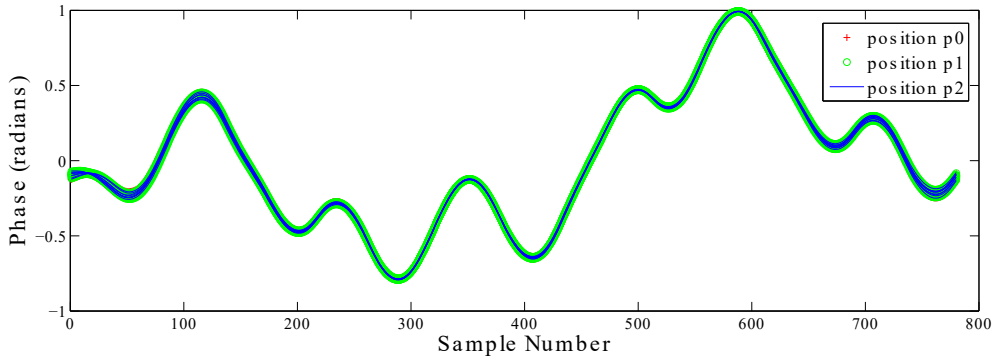


Figure 4.5. Phase midamble at varying positions for BlackBerry 8520.

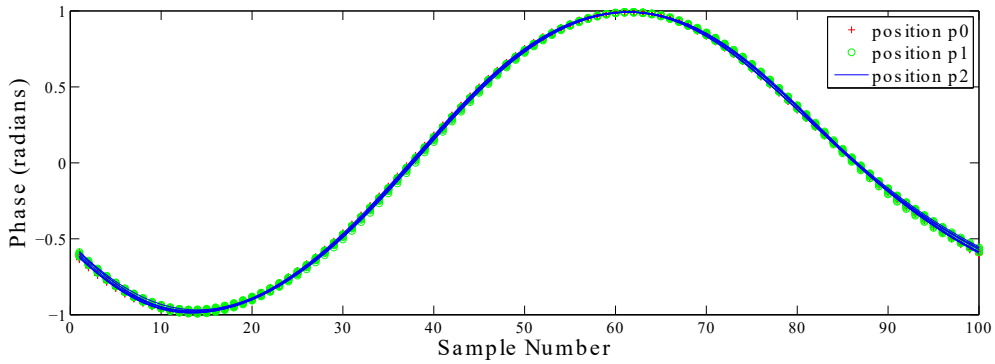


Figure 4.6. Phase near-transient at varying positions for BlackBerry 8520.

Based on Figures 4.5 and 4.6, it is apparent that there is no positional dependence in the phase midamble and phase near-transient as the position of the MS varies with respect to the bladeRF's

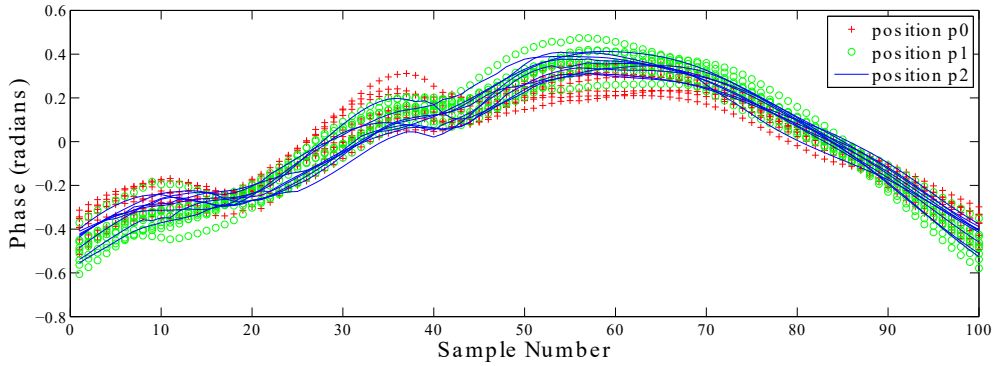


Figure 4.7. Phase transient at varying positions for BlackBerry 8520.

receiver. There are slight differences in the phase transient as the position of the MS varies with respect to the receiver as seen in Figure 4.7.

4.5 TRANSMISSION FREQUENCY DEPENDENCE EXPERIMENT

4.5.1 Experiment setup

To determine whether there existed any fluctuations in the signal characteristics of a GSM burst due to transmission frequency of the MS, a number of recordings were taken under varying transmission frequency conditions for bb1 of the Blackberry 8520 dataset. The OpenBTS and bladeRF parameters used for this experiment are described in Table 4.5.

Table 4.5. Parameters for frequency dependence experiment.

OpenBTS GSM.MS.Power	**OpenBTS ARFCN**	**MS Up-link frequency**	**bladeRF center frequency**
9 dBm	0	890 MHz	890 MHz
9 dBm	65	903 MHz	903 MHz
9 dBm	124	915 MHz	915 MHz

4.5.2 Results and discussion

The results of this experiment are presented in Figures 4.8 to 4.10.

As can be seen in Figure 4.8 and 4.9, the varying frequency apparently has no effect on the phase midamble and near-transient as the plots at varying frequencies overlap one another. In Figure 4.10, the phase transient is affected by varying frequency as the plots at varying frequencies do not correlate

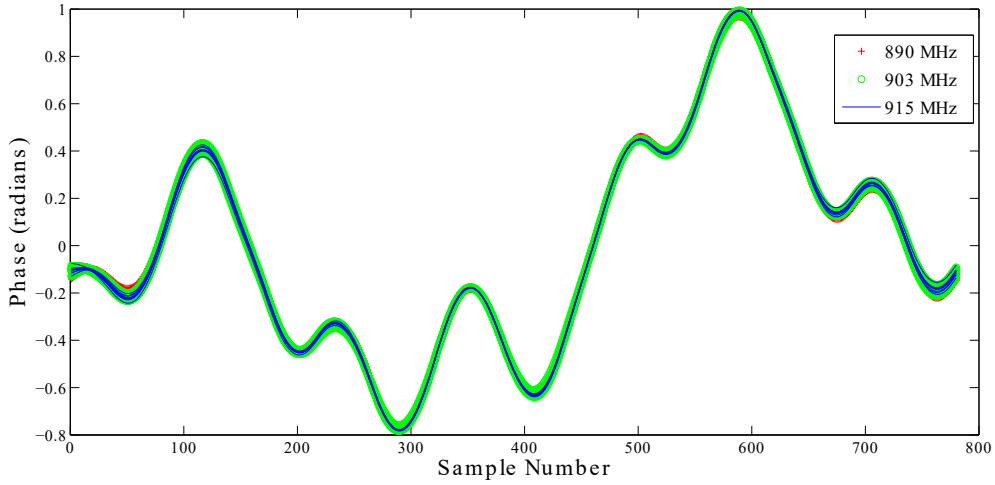


Figure 4.8. Phase midamble at varying frequencies for BlackBerry 8520.

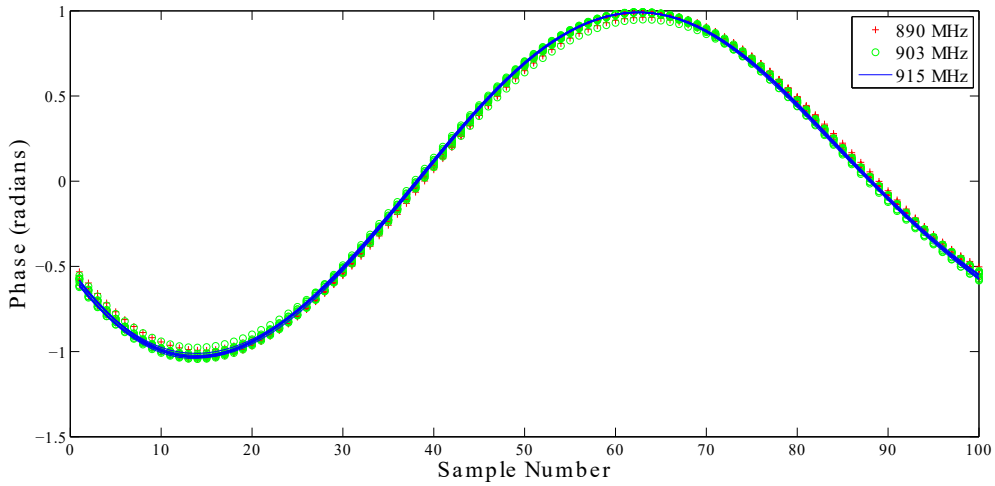


Figure 4.9. Phase near-transient at varying frequencies for BlackBerry 8520.

with one another.

4.6 TRANSMISSION POWER DEPENDENCE EXPERIMENT

4.6.1 Experiment setup

To determine whether there existed any fluctuations in the signal characteristics of a GSM burst due to transmission power of the MS, a number of recordings were taken under varying MS transmission power conditions, by varying the OpenBTS network parameters as described in Table 4.6.

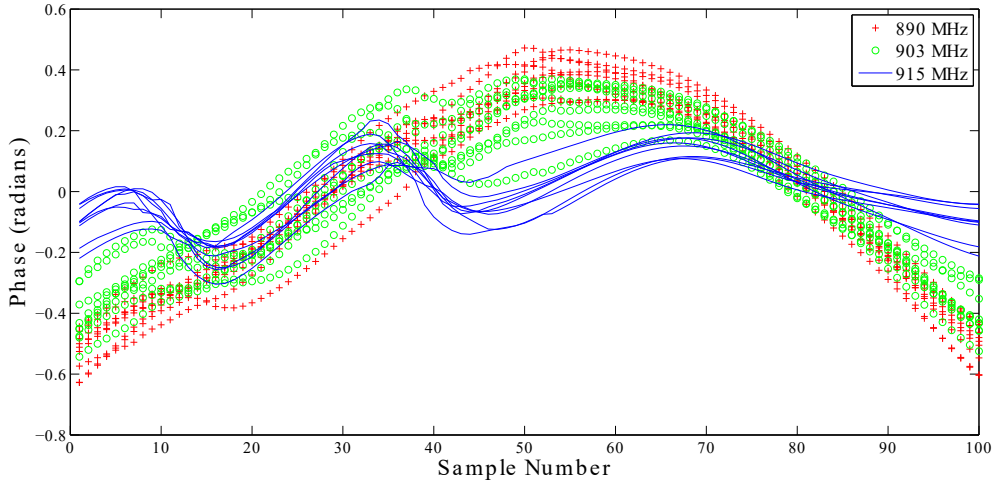


Figure 4.10. Phase transient at varying frequencies for BlackBerry 8520.

Table 4.6. Parameters for power dependence experiment.

OpenBTS GSM.MS.Power	**OpenBTS ARFCN**	**MS Up-link frequency**	**bladeRF center frequency**
9 dBm	75	905 MHz	905 MHz
19 dBm	75	905 MHz	905 MHz
29 dBm	75	905 MHz	905 MHz

4.6.2 Results and discussion

The results of the experiment are presented in Figure 4.11.

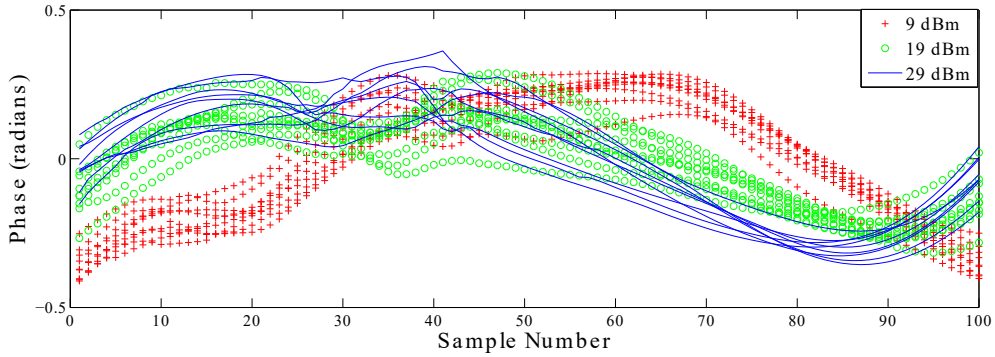


Figure 4.11. Phase transient at varying transmission power for BlackBerry 8520.

In Figure 4.11, the differences in the signal characteristics at varying transmission power are severe. Futhermore, the signal characteristics at 19 dBm and 29 dBm are more distorted and less repeatable from one burst to another. This lack of repeatablity is the reason for reduced classification accuracy at higher transmission power.

4.7 EFFECT OF SNR ON CLASSIFICATION ACCURACY EXPERIMENT

4.7.1 Experiment setup

In order to determine whether there was degradation in the classification accuracy of the SEI system due to a degradation of signal quality, noise was artificially added to the dataset of recordings. This is depicted in the experimental setup shown in Figure 4.12.

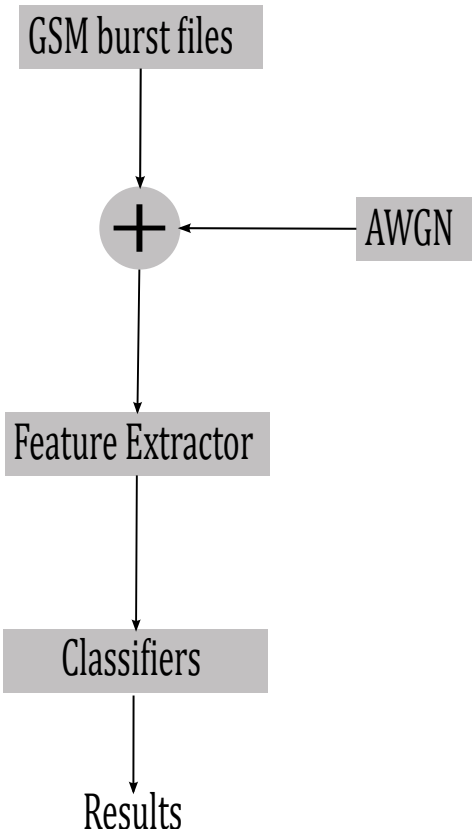


Figure 4.12. Experimental setup for determining the effect of SNR on classification accuracy.

4.7.2 Results and discussion

As seen in Figure 4.12, for each GSM burst file, additive Gaussian white noise (AWGN) was added to the in-phase and quadrature (IQ) samples retained within the burst file. Different levels of noise were added per file, resulting in several new GSM burst files with different SNR levels. The SNR levels

generated for each file range from 9 dB to 30 dB in steps of 3 dB. Using the newly generated burst files, classification tests were performed for a particular SNR level. The classification tests were performed without performing dimensionality reduction. Furthermore, classification tests were performed tested for amplitude and phase features in order to determine which features were most robust against the degradations in signal quality. Figures 4.13 to 4.14 visualises the effect on classification accuracy for increasing levels of SNR for recordings taken at 9 dBm and 29 dBm respectively.

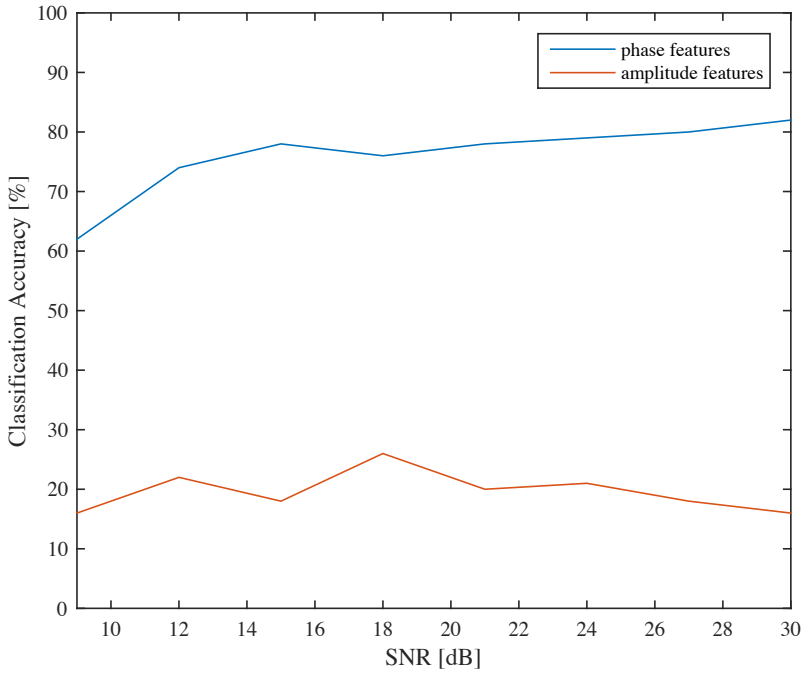


Figure 4.13. Classification accuracy against SNR for recordings taken at a MS transmission power of 9 dBm.

In Figures 4.13 to 4.14, the general trend (regardless of transmission power) is that classification accuracy is poor for 9 dB to 12 dB. When the SNR is greater than 15 dB, the classification accuracy is improved and remains relatively consistent for SNR values greater than 15 dB.

It is also seen that amplitude features produce the lowest classification accuracy of all the feature considered. In contrast, phase derived features appear to be the most robust of all the features considered as a classification accuracy of above 60% is achieved at a low SNR level of 9 dB for recordings taken at 9 dBm and 29 dBm.

From this it can be inferred that phase derived features would perform best in a real-world system given that SNR is not consistently high in the real-world.

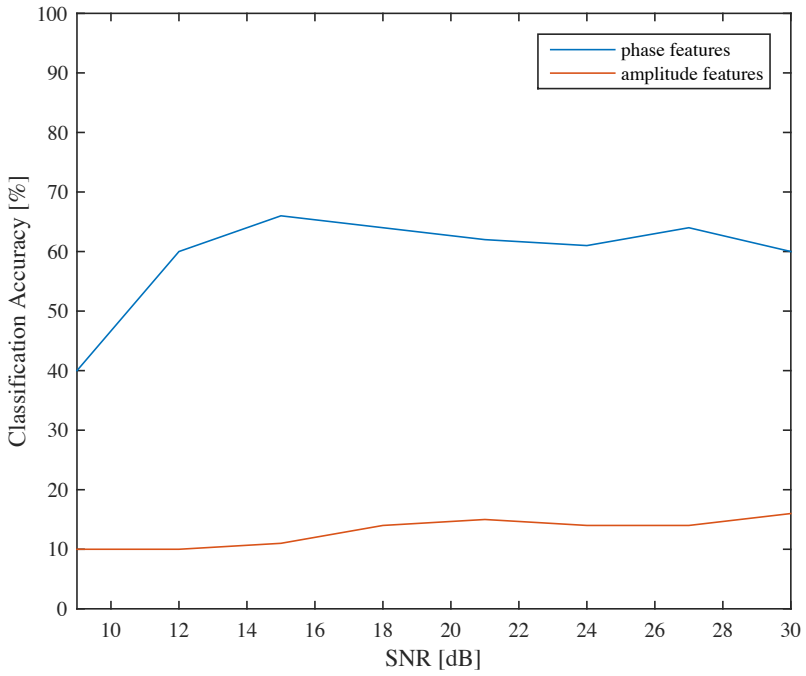


Figure 4.14. Classification accuracy against SNR for recordings taken at a MS transmission power of 29 dBm.

4.8 MULTIPLE LOW-COST RECEIVER EXPERIMENT

As mentioned earlier, the current state of the art regarding SEI typically utilise a single high-quality receiver for the purposes of identification [10, 13, 18–20]. Consequently, it is not known whether identification can consistently and accurately be performed across multiple receivers. A receiver may introduce signal artifacts from its own minor hardware defects, causing the signal to be identified differently from receiver to receiver. This has been observed for low-cost receivers [30]. A secondary issue is that low-cost receivers have been known to degrade the classification accuracy of SEI systems [30].

Thus, an experiment was performed to assess the performance of classification when multiple low-cost receivers were utilised.

4.8.1 Experiment setup

The experiment setup depicted in Figure 4.15 consists of several components. The purpose of each of these components is described below:

1. GSM cellular telephone represents the device to be classified. For this experiment three cell-

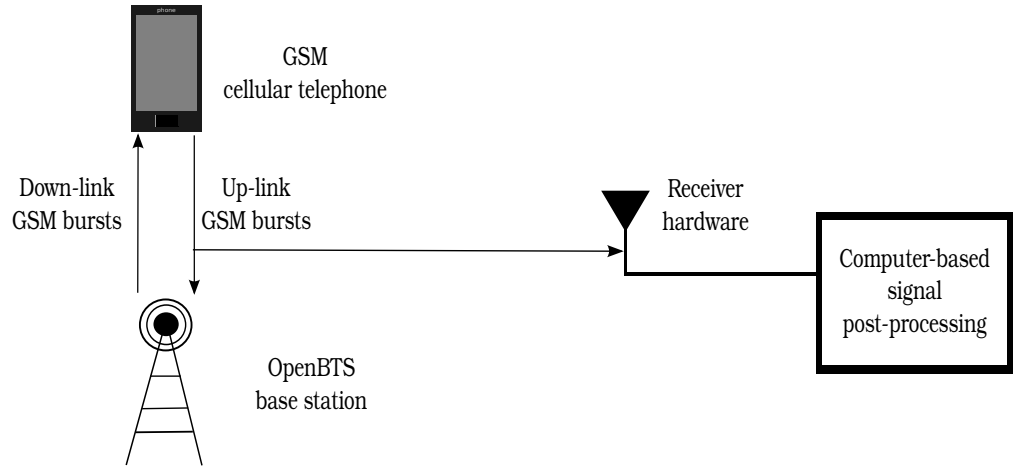


Figure 4.15. Experiment setup to determine the effect of using multiple receivers.

phones were utilised and are described in Table 4.9.

2. OpenBTS base station: OpenBTS software was used to emulate a BTS on a Ettus B210 universal software radio peripheral (USRP). This was done to ensure that the GSM bursts are transmitted at a fixed frequency of 902.5 MHz and transmission power of 9 dBm. The configuration of OpenBTS utilised for this experiment is detailed in Table 4.7. The listed configuration parameters can be set using the command line interface for OpenBTS (OpenBTSCLI). To configure via the OpenBTSCLI, simply enter the command as follows:
   <configuration parameter> <value>

3. Receiver hardware: The receiver hardware was used for the purposes of passively sampling up-link GSM bursts and coverting it to a digital format for the purposes of storage. For the purposes of this experiment the RTL2832U SDR was utilised and will be discussed in detail shortly. The receiver hardware was utilised in conjuction with GNURadio to store the acquired signals in a digital format.

4. Computer-based signal post-processing: Shall perform the aforementioned signal processing on the captured up-link GSM bursts as well as classification of the GSM bursts.

The RTL2832U SDR receiver was chosen for the experiment. It is a relatively inexpensive SDR [48] and can thus be considered as a low-cost receiver. It consists of three types of models based on the tuning chip it utilises. The three variants are the Raphael R820T, Elonics E4000 and the Fitipower FC series of RTL2823. The R820T SDR can tune from 24 MHz to 1766 MHz [49], allowing it to capture signals in the GSM band (880 MHz to 915 MHz). The Elonics E4000 can tune between 52 MHz to

Table 4.7. OpentBTS configuration.

Configuration Parameter	Value	Purpose
Control.LUR. OpenRegistration	.*	Allows any phone to register on the network.
Control.Radio.C0	51	Sets the ARFCN to 51 causing the phone to transmit at 902.5 MHz.
Control.Channels.NumC1s	3	Sets the number of traffic channels to 3.
Control.MS.Power.Min	9	Sets the minimum transmission power to 9 dBm causing the cellphone to transmit bursts at a power of 9 dBm.
Control.MS.Power.Max	9	Sets the maximum transmission power to 9 dBm causing the cellphone to transmit bursts at a power of 9 dBm.

Table 4.8. Receivers used for experiment.

Receiver Label	Type	Tuner Chip.
Receiver A	RTL2832U	Raphael R820T.
Receiver B	RTL2832U	Raphael R820T.
Receiver C	RTL2832U	Elonics E4000.

2200 MHz. Regardless of the type of tuner used, the RTL2832U can sample data at up to 3.2 Msps and has an 8-bit ADC resolution. However, it has been found that the RTL2832U can only sample data reliably (i.e. without dropping samples) at sampling rates lower than 2.56 Msps [50]. For the experiment, three RTL2832U receivers were utilised as described in Table 4.8. The cellphones chosen for classification in this experiment are described in Table 4.9.

The experiment was performed as follows:

1. GSM bursts from each cellular telephone were passively sampled from the receivers described in Table 4.8.

2. Feature vectors from each cellphone were established using GSM bursts generated by the cellphone. This was done for all three receivers.

Table 4.9. Cellphones used for experiment.

Phone Make	Model	Phone Label
LG	KS360	BLG
LG	KS360	WLG
Sony	Xperia V	SXP

3. Classification on the derived feature vectors was then performed using training feature vectors produced on receiver A, and test feature vectors produced on receiver A.

4. Classification on the derived feature vectors was then performed using training feature vectors produced on receiver A, and test feature vectors produced on receiver B.

5. Classification on the derived feature vectors was then performed using training feature vectors produced on receiver A, and test feature vectors produced on receiver C.

6. The differences in the recorded GSM bursts corresponding to a single cellular telephone were then analysed across all three receivers (i.e. receiver A, B and C).

7. The differences in the feature vectors corresponding to a single cellular telephone were then analysed across all three receivers (i.e. receiver A, B and C).

4.8.2 Results

4.8.2.1 Classification Accuracy Results

As mentioned earlier, the aim of the experiment was to:

1. Determine whether GSM SEI can be performed on a low-cost receiver.

2. Determine whether GSM SEI classification accuracy is affected when feature vectors are generated by different receivers. That is to say, can features generated on one receiver be accurately classified with feature vectors generated from a different receiver.

In order to demonstrate these two aspects, three separate classification scenarios were defined as listed below.

1. Classification scenario A - test and training feature vectors were derived on the same receiver (i.e. receiver A).

2. Classification scenario B - training feature vectors were derived from receiver A, while test feature vectors were derived from receiver B. This demonstrates classification performance when nominally identical receivers are used.

3. Classification scenario C - training feature vectors were derived from receiver A, while test feature vectors were derived from receiver C. This demonstrates classification performance when receivers with different tuners are used.

The classification accuracy of the above mentioned scenarios is shown in Table 4.10.

Note that while the average classification accuracy for scenario C is higher than that of B, it is not due to overall better identification but rather due to the classifiers having a very high bias for one of the identified classes. For instance, the Mahalanobis classifier in scenario C identifies BLG 90.91% of the time and does not identify WLG at all (i.e. 0%). This misidentification is worse than that in scenario B because some classes cannot be identified at all. Based on this, classification in scenario C is worse than that in B.

4.8.2.2 Signal and Feature Vector Analysis

4.8.2.2.1 Average Signal Representations

In order to visualise the differences in the signals produced by the three receivers (A, B and C), the average normalised amplitude representation and average phase representation of the bursts captured by each receiver were plotted. Average normalised amplitude was calculated by taking the absolute of the IQ samples of a single down-converted and filtered GSM burst. The absolute values were scaled between 0 and 1. Thereafter the mean of the absolute samples across 1000 bursts was taken to produce the average normalised amplitude representation. Similarly the average phase representation was derived by taking the phase of down-converted and filtered bursts. However, in the case of phase no scaling was performed.

The average amplitude and phase representations of BLG captured on the same receiver (i.e. receiver A) are shown in Figure 4.16 and Figure 4.17 respectively. The average amplitude and phase representations of WLG captured on the same receiver (i.e. receiver A) is shown in Figure 4.18 and Figure 4.19 respectively. The average amplitude and phase representations of BLG captured on receiver A and B are shown in Figure 4.20 and Figure 4.21 respectively.The average amplitude and phase representations of BLG captured on Raphael R820T receiver (receiver A) and Elonics E4000 receiver (receiver C) are shown in Figure 4.22 and Figure 4.23 respectively. The average amplitude

Table 4.10. Classification results showing the accuracy of identifying nominally identical phones (LG Accuracy) and the accuracy when two nominally identical phones and one phone of a different make and model is considered (overall accuracy) for the three different classification scenarios.

Kth Nearest Neighbour Classifier											
Classification Scenario A Confusion Matrix				**Classification Scenario B Confusion Matrix**				**Classification Scenario C Confusion Matrix**			
	BLG	WLG	SXP		BLG	WLG	SXP		BLG	WLG	SXP
BLG	57.58	42.42	0	BLG	42.42	57.58	0	BLG	33.33	66.67	0
WLG	37.37	62.63	0	WLG	73.74	26.26	0	WLG	37.37	62.63	0
SXP	0	0	100.0	SXP	0	0	100.0	SXP	0	1.01	98.99
Overall Accuracy = 73.40% **LG Accuracy = 60.10%**				**OverallAccuracy = 55.21%** **LG Accuracy = 32.83%**				**OverallAccuracy = 64.98%** **LG Accuracy = 47.48%**			
Mahalanobis Classifier											
Classification Scenario A Confusion Matrix				**Classification Scenario B Confusion Matrix**				**Classification Scenario C Confusion Matrix**			
	BLG	WLG	SXP		BLG	WLG	SXP		BLG	WLG	SXP
BLG	77.78	22.22	0	BLG	38.38	61.62	0	BLG	90.91	9.09	0
WLG	42.42	57.58	0	WLG	76.77	23.23	0	WLG	100	0	0
SXP	0	0	100.0	SXP	0	0	100.0	SXP	39	0	60.61
Overall Accuracy = 73.67% **LG Accuracy = 67.68%**				**OverallAccuracy = 53.54%** **LG Accuracy = 30.30%**				**OverallAccuracy = 61.67%** **LG Accuracy = 42.50%**			
Ensemble Classifier											
Classification Scenario A Confusion Matrix				**Classification Scenario B Confusion Matrix**				**Classification Scenario C Confusion Matrix**			
	BLG	WLG	SXP		BLG	WLG	SXP		BLG	WLG	SXP
BLG	60.61	39.39	0	BLG	42.42	57.58	0	BLG	26.26	73.74	0
WLG	41.41	58.59	0	WLG	76.77	23.23	0	WLG	41.44	58.59	0
SXP	0	0	100.0	SXP	0	0	100.0	SXP	0	0	100.0
Overall Accuracy = 73.07% **LG Accuracy = 59.60%**				**OverallAccuracy = 55.21%** **LG Accuracy = 32.83%**				**OverallAccuracy = 56.90%** **LG Accuracy = 40.40%**			

and phase representations of WLG captured on Raphael R820T receiver (receiver A) and Elonics E4000 receiver (receiver C) are shown in Figure 4.24 and Figure 4.25 respectively.

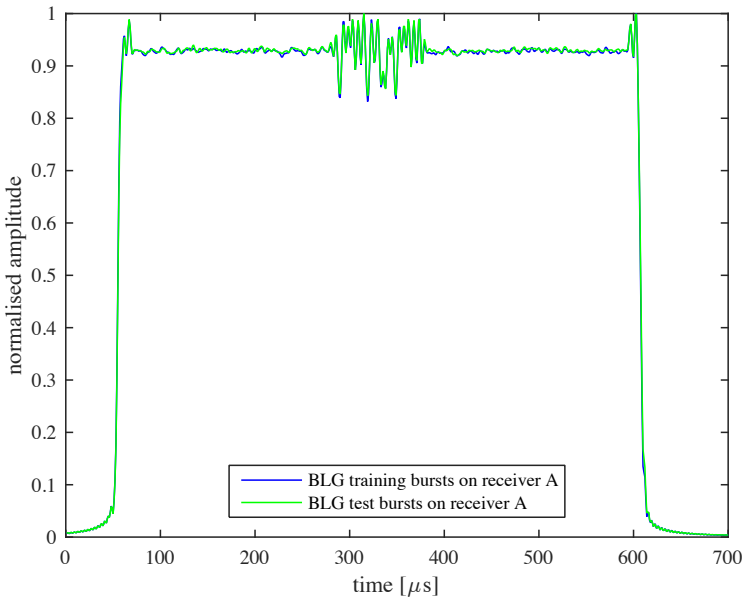


Figure 4.16. Average normalised amplitude representations for bursts captured from BLG on receiver A.

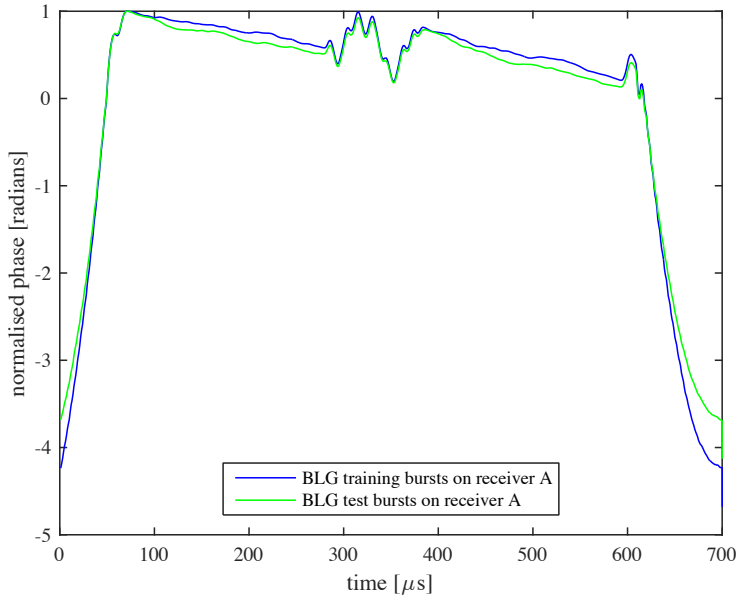


Figure 4.17. Average phase representations for bursts captured from BLG on receiver A.

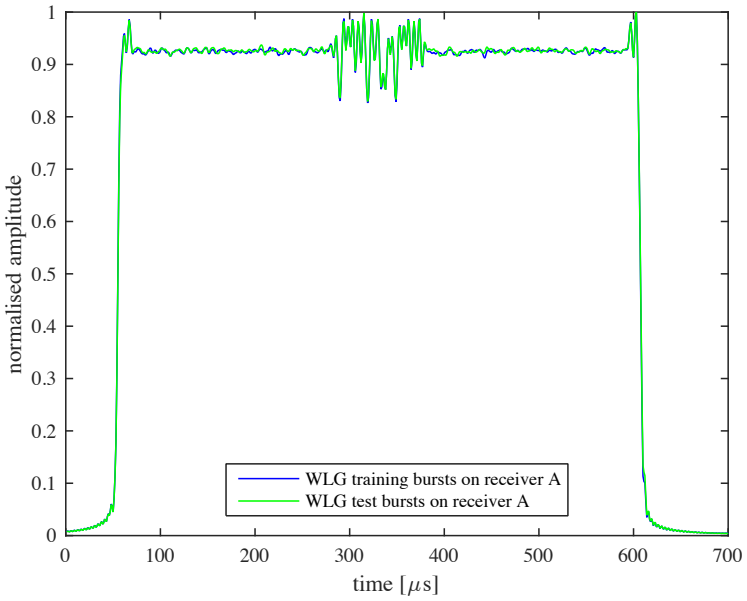


Figure 4.18. Average normalised amplitude representations for bursts captured from WLG on receiver A.

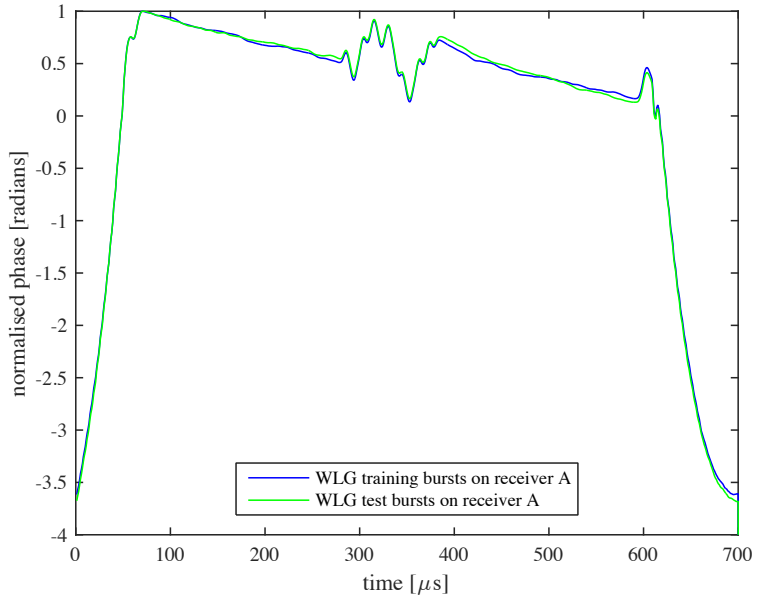


Figure 4.19. Average phase representations for bursts captured from WLG on receiver A.

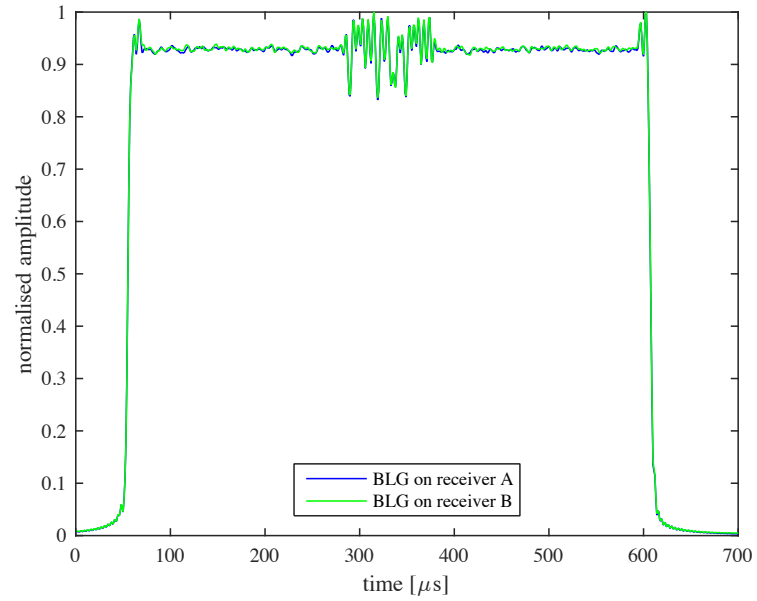


Figure 4.20. Average normalised amplitude representations for bursts captured from BLG on receiver A and receiver B.

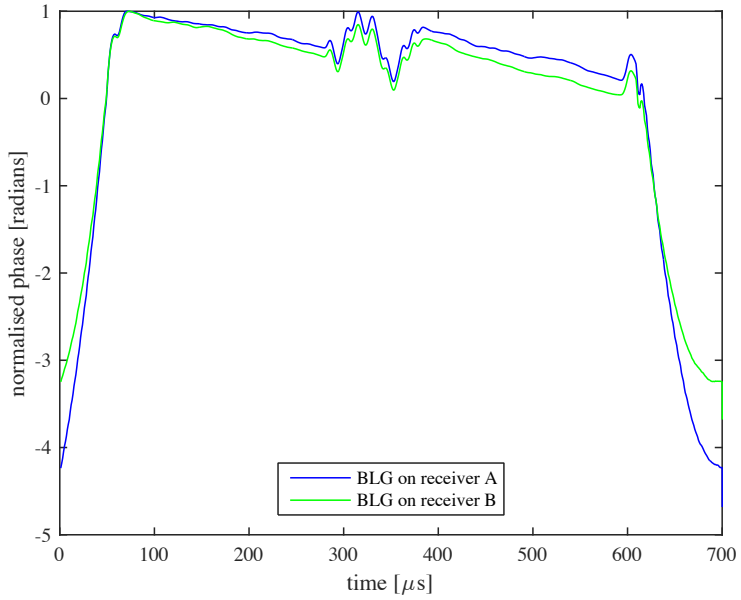


Figure 4.21. Average phase representations for bursts captured from BLG on receiver A and receiver B.

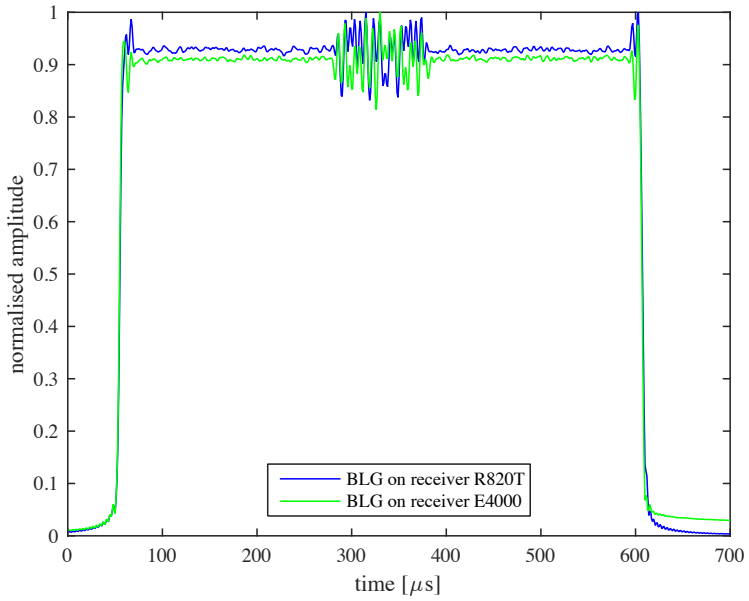


Figure 4.22. Average normalised amplitude representations for bursts captured from BLG on Raphael R820T receiver (receiver A) and Elonics E4000 (receiver C).

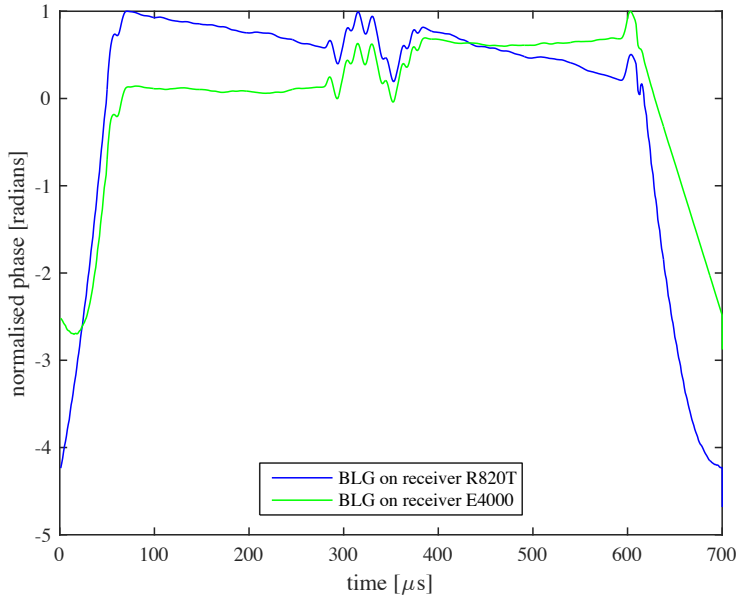


Figure 4.23. Average phase representations for bursts captured from BLG on Raphael R820T receiver (receiver A) and Elonics E4000 (receiver C).

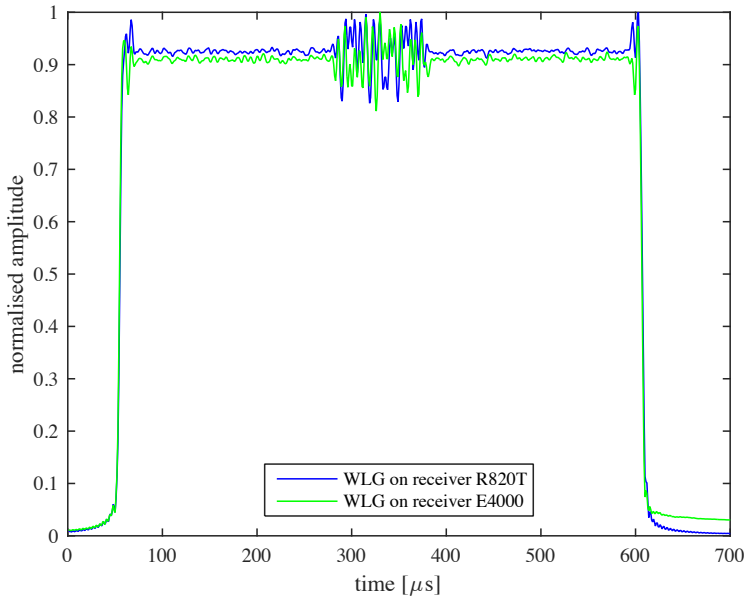


Figure 4.24. Average normalised amplitude representations for bursts captured from WLG on Raphael R820T receiver (receiver A) and Elonics E4000 (receiver C).

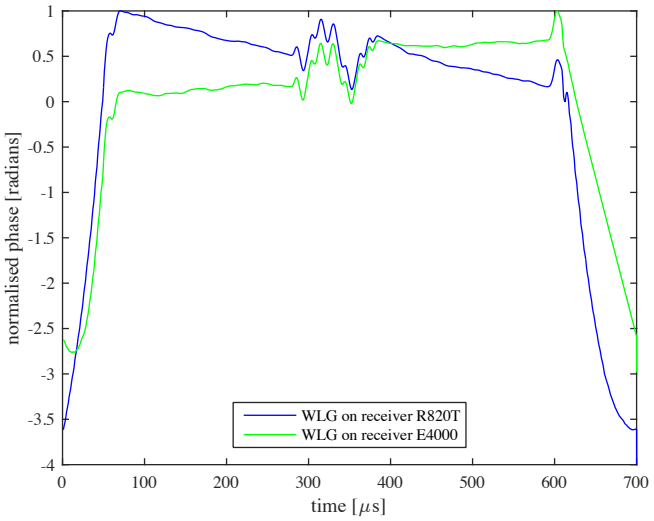


Figure 4.25. Average phase representations for bursts captured from WLG on Raphael R820T receiver (receiver A) and Elonics E4000 (receiver C).

As an additional test, the same signal was simultaneously sampled from BLG using the three receivers mentioned in Table 4.8. This was done to ensure no differences were being falsely introduced in the data (due receiver positioning or signal data differences) between recordings. The average amplitude and phase representations produced by the three receivers is shown in Figure 4.26 and Figure 4.27 respectively.

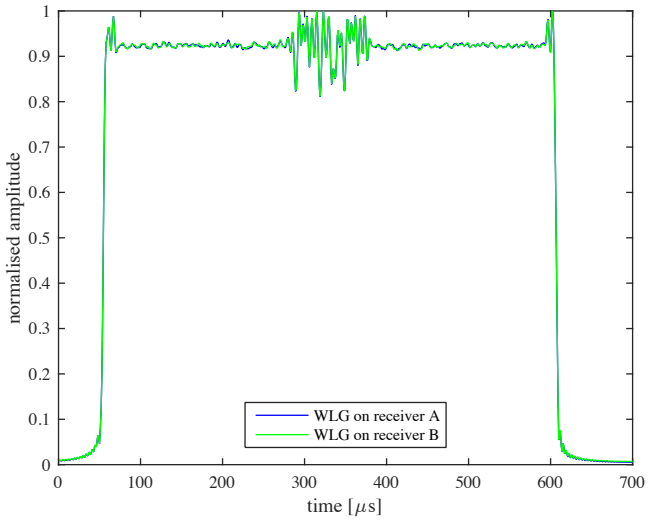


Figure 4.26. Average amplitude representation for BLG GSM bursts generated on two Raphael R820T receivers and the Elonics E4000 receiver.

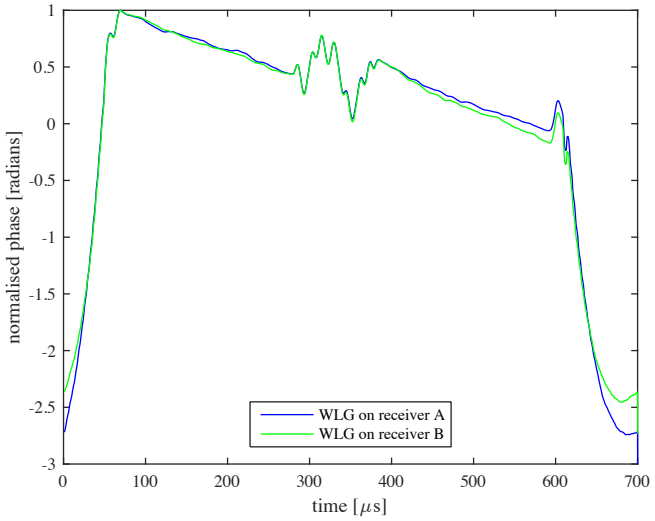


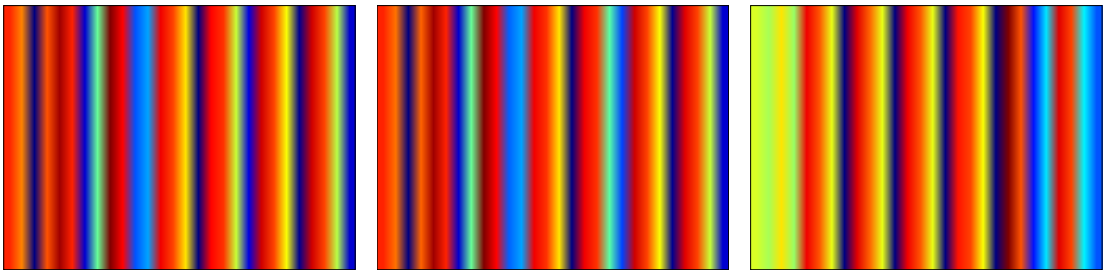
Figure 4.27. Average phase representation for BLG GSM bursts generated on two Raphael R820T receivers and the Elonics E4000 receiver.

It is seen that when signals from the same phone are captured on the same receiver, the signals overlap each other with minimal differences in the signal characteristics recorded (as shown in Figures 4.16 to 4.19). However, the signal differences become apparent when the same phone is recorded

on different receivers of the same make and model (as shown in Figure 4.20), and even more so when phone is recorded on two different receivers of the same make and model (as shown in Figures 4.22 to 4.25). This holds true in the case where the cellular telephone was sampled simultaneously by two different receivers.

4.8.2.2.2 Feature Vector Representations and Analysis

In order to visualise the effect that different receivers had on feature vectors, the average representation of 100 feature vectors was taken for feature vectors generated by a specific receiver. For each of these average representations a spectrogram-like image was produced as shown in Figure 4.28. As seen in Figure 4.28, it is more difficult to determine differences between the feature vectors of BLG and WLG (which are nominally identical devices). However it is easier to distinguish between the feature vectors of either WLG or BLG and SXP, which are produced by cellphones from different manufacturers.



(a) BLG averaged feature vector representation for feature vectors generated from receiver A.

(b) WLG averaged feature vector representation for feature vectors generated from receiver A.

(c) SXP averaged feature vector representation for feature vectors generated from receiver A.

Figure 4.28. Spectral representations of averaged feature vectors.

In order to get a better view of the differences between the feature vectors from nominally identical devices, a stem plot of the average feature vector representation for BLG and WLG was made as seen in Figure 4.29. As seen in Figure 4.29, there are noticeable differences in the average feature vector representations of BLG and WLG. Considering the average representation of the test and training feature vectors of BLG shown in Figure 4.30, there are minor differences in the average feature vector representations. This indicates that feature vectors produced on the same receiver are robust and repeatable. However, when feature vectors are derived for the same device on two different but nominally identical receivers, moderate differences in the feature vectors are observed, as shown in Figure 4.31. These differences are almost as significant as when two devices of the same make and

model are recorded on the same receiver. These differences are exacerbated when receivers of a different make and model are used (i.e. the Raphael R820T receiver and the Elonics E4000 receiver) as shown in Figure 4.32.

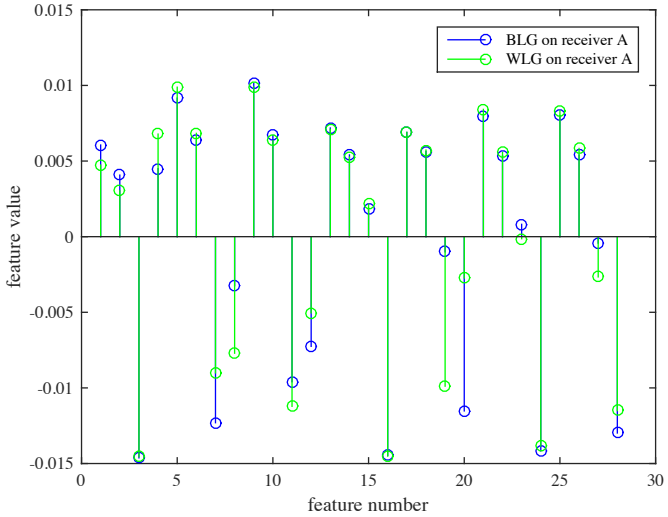


Figure 4.29. Average feature vector representation for WLG and BLG.

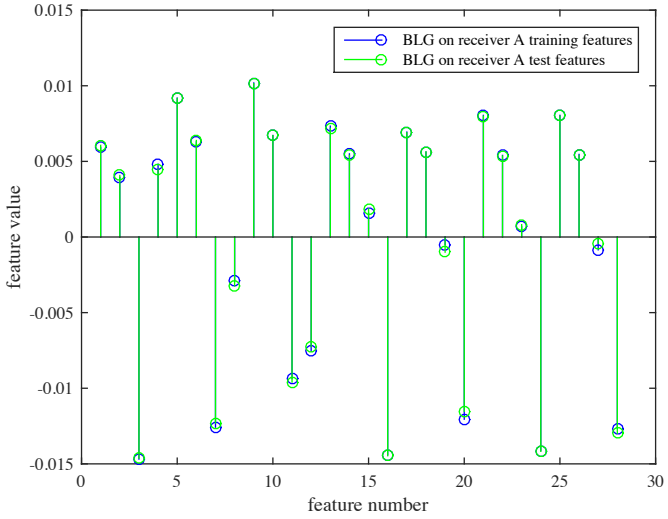


Figure 4.30. Average feature vector representation for BLG test and training feature vectors.

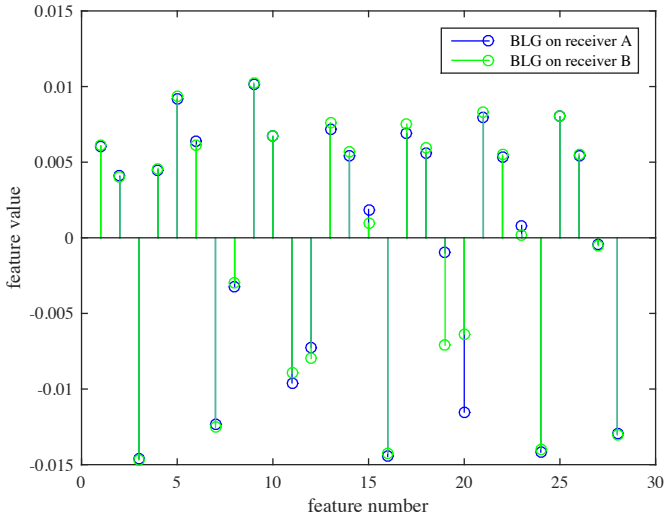


Figure 4.31. Average feature vector representation for BLG for feature vectors generated on receiver A and receiver B.

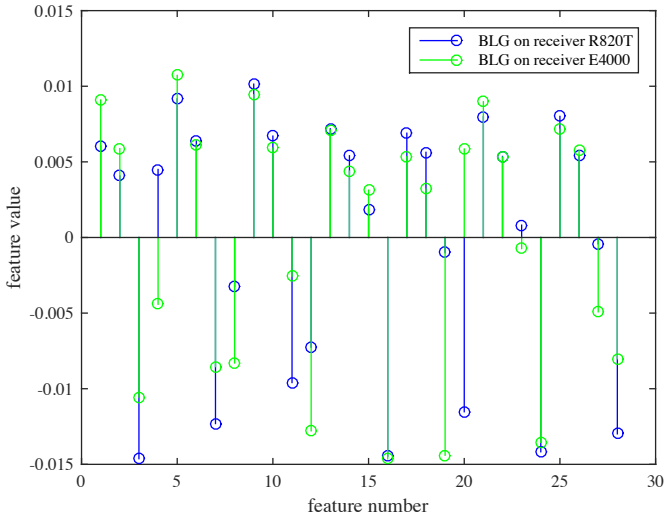


Figure 4.32. Average feature vector representation for BLG for feature vectors generated on the Raphael R820T receiver and the Elonics E4000 receiver.

4.8.3 Discussion of results

Considering the classification accuracy results in Table 4.10, it is observed that classification between cellphones of a different make and model was accurate regardless of whether the feature vectors

were derived from different receivers. Classification between nominally identical cellphones on the other hand was poorer with an average classification accuracy of 63.67% when feature vectors are derived from the same receiver. The classification accuracy of nominally identical devices drops further when test feature vectors are derived from a different receiver than the training feature vectors. This is demonstrated in classification scenarios B and C where features were derived from two nominally identical receivers and two different receivers respectively. The average classification accuracy between the nominally identical cellphones for classification scenarios B and C was 32.17% and 41.45% respectively. Note that while the classification accuracy appears to be higher for scenario C compared to scenario C, the results for scenario C are actually poorer. This is because for scenario C each classifier biases towards a particular cellular telephone. For instance, Table 4.10 shows that the KNN classifier biases towards WLG whereas the Mahalanobis classifier biases towards BLG. This bias leads to poorer classification as only one cellular telephone can be discerned between the two cellular telephones of the same make and model. This poor classification accuracy when features were derived from different receivers indicates that each receiver produces its own unique signal characteristics during the sampling process as a result of its hardware component tolerances. Given that all the receivers considered during this experiment were low-cost it can be assumed that the hardware tolerances for these receivers are higher than those for higher quality receivers. Consequently, high quality receivers may not exhibit a degradation in classification accuracy when feature vectors are derived from nominally identical high quality receivers.

The signal characteristics produced by each receiver are demonstrated in Figures 4.20 to Figures 4.25. For instance, in Figure 4.20 and Figure 4.21 it is observed that the differences in the signal forms produced by BLG is more noticeable when recorded on two different receivers than when recorded on the same receiver as seen in Figure 4.18 and 4.19. These differences are more significant in phase than for amplitude. Furthermore, these differences become more noticeable when the receivers are not of the same make and model (see Figures 4.22 to 4.25). These signifcant differences are because, in the case of different make and model receivers, the hardware comprising the receivers is different. Hence, the signal forms produced by the receivers are expected to differ significantly.

Furthermore, comparing the classification accuracy from Table 4.10 to classification accuracy seen in Table 4.11 (which was performed for the same features but at a sampling rate of 8 MHz on a more expensive BladeRF SDR with 12-bit ADC resolution), it can be deduced that sampling rate and ADC resolution affects classification accuracy. That is to say, the higher the sampling rate and/or ADC resolution, the higher the classification accuracy provided transmission power and frequency is held constant. The higher sampling rate and ADC resolution of the BladeRF SDR allows for the

Table 4.11. Confusion matrix for LG KS360 cellphones recorded a on BladeRF SDR with a sampling rate of 8 MHz.

	Kth Nearest Neighbour Classifier	
	BLG	**WLG**
BLG	81	19
WLG	26	74
	Accuracy = 77.5%	
	Mahalanobis Classifier	
	BLG	**WLG**
BLG	75	25
WLG	43	57
	Accuracy = 66.0%	
	Ensemble Classifier	
	BLG	**WLG**
BLG	80	20
WLG	37	63
	Accuracy = 71.5%	

signal of a cellular telephone to be recorded with greater detail. Consequently, more differences in the signals from two cellular telephones can be picked up by the feature extractor. This would explain the higher classification in the case of the BladeRF setup compared to the RTL-SDR setup. However, the Mahalanobis classifier performance is roughly the same in both cases. It would then appear that the statistical nature of the features are unaffected by the increased sampling rate and ADC resolution as the Mahalanobis metric is statistical in nature.

4.8.4 Conclusion

It can be concluded that higher the sampling rate and/or ADC resolution used during signal acquisition the higher the accuracy during classification. Furthermore, it was observed that different receivers (especially those of different make and model) produce significant differences in signals captured from the same cellphone. The aforementioned differences are detrimental to classification accuracy when trying to classify feature vectors produced by different receivers. This indicates that training data must be recorded on the same receiver that will be used in the SEI system.

CHAPTER 5 CONCLUSION

5.1 SUMMARY OF THE WORK

A GSM SEI proof-of-concept software system was successfully designed and developed to:

- Determine whether GSM cellular telephones could be successfully identified using SEI.
- Determine how GSM signal characteristics were affected by variations in transmission power, transmission frequency and the cellular telephone's position relative to the acquisition system's antenna.
- Determine whether degradations in signal quality affected the classification accuracy of the SEI system.
- Determine whether SEI can be successfully applied through the use of multiple receivers (i.e. one receiver to train the SEI system and another receiver to test the SEI system).

5.2 SUMMARY OF THE FINDINGS

The results and findings of the dissertation are summarised as follows.

- With the use of dimensionality reduction, a peak classification accuracy of 88.26% was achieved at a MS transmission power of 9 dBm. The higher classification accuracy at lower transmission power is likely due to the fact that signal wave form is more consistent at lower power than at higher transmission power as shown in Figure 4.11.
- It was generally observed that as the transmission power of a MS increased, the ability to identify it diminished. The implication of this finding is that SEI will work poorly in situations where BTSs are far from users, which is typical in some rural South African settings.
- Distance-based classifiers outperformed a LIBSVM SVM classifier using a radial-basis kernel function. An ensemble classifier was able to produce slightly better classification accuracies than the KNN and Mahalanobis distance classifiers that compose it. This is because the base classifiers behaved in a complementary manner thus allowing the ensemble classifier to make improved classifications for the majority of classifications scenarios. In the remainder of scen-

arios, the ensemble classifier provided performance that was slightly less than the better performing base classifier.

- Transmission frequency and cellular telephone position relative to the acquisition antenna had little to no effect on the signal characteristics. Thus, there is no need to compensate for changes in signal characterstics when frequency changes.
- The classification accuracy of a set of nominally identical cellular telephones was poorer when using low-cost RTL-SDR receivers as compared to when the BladeRF SDR was utilised. The primary difference between these two receivers is that the BladeRF has a higher sampling rate and a higher ADC resolution. From this it is inferred that reductions in sampling rate and ADC resolution can result in a reduction in classification accuracy. Furthermore, this finding imposes a restriction on the minimum ADC resolution and sampling rate to be used by the receiver of an SEI system so that it can reliably identify cellular telephones.
- GSM SEI cannot be successfully implemented over multiple receivers. It was observed that cellular telephones trained on one receiver could not be successfully identified when new signals were captured on a different receiver. This holds true even if the receivers are nominally identical. This infers that each receiver produces unique characteristics to the signal as a result of its own unique hardware tolerances. The implication here is that cellular telephones will have to be individually characterised on each BTS it operates on.
- Classification accuracy (without dimensionality reduction applied) is reduced when signal quality is degraded. SNR values of lower than 12 dB result in poor classification accuracy. Classification accuracy is adequate and does not improve significantly for SNR values greater than or equal to 15 dB. Furthermore, phase derived features are least affected by SNR degradation as they produce higher classification accuracies compared to amplitude features. This implies that the SEI technique holds promise for usage in real-world scenarios because the minimum SNR in GSM networks is typically above 9 dB [15].

5.3 SUGGESTIONS FOR FUTURE WORK

The following points can be considered for future work.

- The application of channelisation and time-slot de-interleaving to the system in order to be able to classify multiple cellular telephones simultaneously. Since real GSM BTSs use TDMA and frequency hopping, this avenue of research is essential if SEI is to be applied to real-world systems.
- Investigate the effect of multi-path on classification accuracy. In order to apply SEI in a real-

world environment, it is essential to understand the effects multi-path would have on signal characteristics.

- Investigate whether features are susceptible to emitter age and battery life of the MS. Since cellular telephones are expected to be identified over long periods of time, it is necessary to determine whether emitter age affects the recorded signal features. Secondly, in a real-world scenario, cellular telephones will have varying battery life when trying to be identified. This makes it necessary to determine whether battery life has an effect on recorded signal features.
- Investigate whether signal characteristics caused by the receiver of a SEI system can be calibrated out of the system. This is particularly important as the findings of this research show that it is not possible to reliably identify cellular telephones over multiple receivers.

BIBLIOGRAPHY

[1] J. Hoy, "Subscriber and Device Identifiers," in *Forensic Radio Survey Techniques for Cell Site Analysis*. John Wiley Sons, 2015, ch. 4, pp. 55–56.

[2] L. Dryburgh and J. Hewett, "GSM and ANSI-41 Mobile Application Part (MAP)," in *Signaling System No. 7 (SS7/C7): Protocol, Architecture, and Services*, ser. Cisco press networking technology series. Cisco, 2005, ch. 13, pp. 389–391.

[3] A. Jain. (2014, Sep. 10) How to Change IMEI Number of Your Android Easily (Rooting Required). *TechnoStall*. [Online]. Available: http://www.technostall.com/how-to-change-imei-number-android/

[4] L. Marshall, "Record 618 South African rhinos poached for horns in 2012, so far," National Geographic News Watch, 11 Dec 2011. [Online]. Available: http://newswatch.nationalgeographic.com/2012/12/11/record-618-south-african-rhinos-poached-for-horns-in-2012-so-far/

[5] C. Beaudufe, "South African success story under threat," Sowetan Live, 7 May 2012. [Online]. Available: http://www.sowetanlive.co.za/news/2012/05/07/south-african-success-story-under-threat

[6] "Mexico to fingerprint all mobile phone users," The Telegraph, 9 Feb 2009. [Online]. Available: http://www.telegraph.co.uk/news/worldnews/centralamericaandthecaribbean/mexico/4573514/Mexico-to-fingerprint-all-mobile-phone-users.html

[7] M. J. Riezenman, "Cellular security: better, but foes still lurk," *IEEE Spectrum*, vol. 6, pp. 39–42, June 2000.

[8] "Regulation of Interception of Communications and Provision of Communication-Related Information Act, 2002," Government gazette, Government of the Republic of South Africa, 22 January 2003.

[9] K. I. Talbot, P. R. Duley, and M. H. Hyatt, "Specific emitter identification and verification," *Technology Review Journal*, vol. 11, pp. 113–133, Jun. 2003.

[10] D. Zanetti, V. Lenders, and S. Capkun, "Exploring the physical-layer identification of gsm devices," ETH, Department of Computer Science, Zurich, Germany, Tech. Rep. 1, 2012.

[11] J. N. Samuel and W. P. du Plessis, "Specific emitter identification for enhanced access control security," *SAIEE African Research Journal (ARJ)*, vol. 108, pp. 71–79, June 2017.

[12] J. N. Samuel, *Specific Emitter Identification for GSM Cellular Telephones - 2013 Final Year Project*, Pretoria, South Africa, 2013.

[13] D. R. Reising, M. A. Temple, and M. J. Mendenhall, "Improving intra-cellular security using air monitoring with RF fingerprints," in *IEEE Wireless Communications and Networks Conference (WNC10)*, Sydney, Australia, Apr. 2010.

[14] L. Harte, *Introduction to the Global System for Mobile Communication (GSM): Physical Channels, Logical Channels, Network and Operation*. United States of America: ALTHOS publishing, 2005.

[15] S. M. Redl, M. K. Webber, and M. W. Oliphant, *An Introduction to GSM*. 685 Canton Street, Norwood, MA 02062, United States of America: Artech House, 1995.

[16] *3GPP TS 45.001 V11.0.0 Release 11*, ETSI Std., Sep. 2012. [Online]. Available: http://www.3gpp.org/ftp/Specs/html-info/45001.htm

[17] B. Danev, D. Zanetti, and S. Capkun, "On physical-layer identification of wireless devices," *ACM Computing Surveys*, vol. 45, no. 1, pp. 6:1–6:29, Dec. 2012.

[18] J. Hasse, T. Gloe, and M. Beck, "Forensic Identification of GSM Mobile Phones," in *Proceedings of the First ACM Workshop on Information Hiding and Multimedia Security*, Montpellier, France, 2013, pp. 131–140.

[19] D. R. Reising, M. A. Temple, and M. J. Mendenhall, "Improved wireless security for GMSK based devices using RF fingerprinting," *International Journal of Electronic Security and Digital Forensics*, vol. 3, no. 1, pp. 41–59, Mar. 2010.

[20] M. Williams, M. A. Temple, and D. Reising, "Augmenting Bit-Level Network Security Using Physical Layer RF-DNA Fingerprinting," in *Global Telecommunications Conference (GLOBECOM 2010)*, Dec 2010, pp. 1–6.

[21] V. Brik, S. Banerjee, M. Gruteser, and S. Oh, "Wireless device identification with radiometric signatures," in *Proceedings of the 14th ACM International Conference on Mobile Computing and Networking*, ser. MobiCom '08, San Francisco, California, 2008, pp. 116–127.

[22] R. O. Duda, P. E. Hart, and D. G. Stork, *Pattern Classification 2.ed.* 605 Third Avenue, New York, N.Y.: Wiley-Interscience, 2000.

[23] D. Read, "Object classification: Goals and problems, dimensionality reduction," in *Artifact Classification: A Conceptual And Methodological Approach*, 1st ed. San Francisco, CA: Left Coast Press, 2009, vol. 1, ch. 5, pp. 140–143.

[24] P. Norvig and S. Russell, "Learning from examples," in *Artificial Intelligence: A Modern Approach*, 3rd ed. Upper Saddle River, NJ: Pearson, 2010, vol. 1, ch. 18, pp. 693–757.

[25] J. Jedrzejowicz and P. Jedrzejowicz, "A family of the online distance-based classifiers," in *Intelligent Information and Database Systems*, ser. Lecture Notes in Computer Science, N. Nguyen, B. Attachoo, B. Trawiski, and K. Somboonviwat, Eds. Springer International Publishing, 2014, vol. 8398, pp. 177–186.

[26] N. C. Oza, "Ensemble data mining methods," online, NASA, Tech. Rep., 2013.

[27] R. A. Jacobs, M. I. Jordan, S. J. Nowlan, and G. E. Hinton, "Adaptive mixtures of local experts," *Neural Comput.*, vol. 3, no. 1, pp. 79–87, Mar. 1991. [Online]. Available: http://dx.doi.org/10.1162/neco.1991.3.1.79

[28] M. I. Jordan, "Hierarchical mixtures of experts and the em algorithm," *Neural Computation*, vol. 6, pp. 181–214, 1994.

[29] R. Maclin and D. Opitz, "An empirical evaluation of bagging and boosting," in *In Proceedings of The Fourteenth National Conference on Artificial Intelligence*, Providence, Rhode Island, 2006, pp. 546–552.

[30] S. U. Rehman, K. W. Sowerby, and C. Coghill, "Analysis of impersonation attacks on systems using RF fingerprinting and low-end receivers," *Journal of Computer and System Sciences*, vol. 80, no. 3, pp. 591–601, 2014.

[31] B. Danev, H. Luecken, S. Capkun, and K. El Defrawy, "Attacks on physical-layer identification," in *Proceedings of the Third ACM Conference on Wireless Network Security*, Hoboken, NJ, 2010, pp. 89–98.

[32] A. Rencher, *Methods of Multivariate Analysis*. Wiley, 2003.

[33] G. McLachlan, "Discrimination via normal models," in *Discriminant Analysis and Statistical Pattern Recognition*, pp. 61–64.

[34] H. Liu and H. Motoda, *Feature Extraction, Construction and Selection: A Data Mining Perspective*, ser. Kluwer international series in engineering and computer science. Kluwer Academic, 1998.

[35] I. Guyon and A. Elisseeff, "An introduction to variable and feature selection," *Journal of Machine Learning Research*, vol. 3, pp. 1157–1182, Mar. 2003.

[36] R. Kohavi and D. Sommerfield, "Feature subset selection using the wrapper method: Overfitting and dynamic search space topology," 1995.

[37] R. W. Klein, M. A. Temple, and M. J. Mendenhall, "Application of wavelet-based rf fingerprinting to enhance wireless network security," *Journal of Communications and Networks*, vol. 11, pp. 544–555, December 2009.

[38] M. Connor and P. Kumar, "Parallel construction of k-nearest neighbor graphs for point clouds," in *Proceedings of the Fifth Eurographics / IEEE VGTC Conference on Point-Based Graphics*, ser. SPBG'08. Aire-la-Ville, Switzerland, Switzerland: Eurographics Association, 2008, pp. 25–31.

[39] J. Richards, *Remote Sensing Digital Image Analysis: An Introduction*. Springer, 2012.

[40] J. Johnson and P. Picton, *Mechatronics Volume 2: Concepts in Artifical Intelligence*. Elsevier Science, 1995, no. v. 2.

[41] M. J. Riezenman, "Regularized linear discriminant analysis and its application in microarrays," *Oxford Biostatistics Journal*, vol. 8, pp. 86–100, March 2006.

[42] (2013) Discriminant analysis classification. MathWorks. [Online]. Available: http://www.mathworks.com/help/stats/classificationdiscriminantclass.html

[43] J. Ye, R. Janardan, V. Cherkassky, T. Xiong, J. Bi, and C. Kambhamettu, "Efficient model selection for regularized linear discriminant analysis," in *Proceedings of the 15th ACM International Conference on Information and Knowledge Management*, 2006, pp. 532–539.

[44] F. Camastra and A. Vinciarelli, "Whitening transformation," in *Machine Learning for Audio, Image and Video Analysis: Theory and Applications*, ser. Advanced Information and Knowledge Processing. Springer London, 2015.

[45] (2010) R. W. Picard, extra notes for MAS622J/1.126J. MIT. [Online]. Available: http://courses.media.mit.edu/2010fall/mas622j/whiten.pdf

[46] X. Wang and X. Tang, "Dual-Space Linear Discriminant Analysis for Face Recognition," in *Computer Vision and Pattern Recognition, 2004. CVPR 2004. Proceedings of the 2004 IEEE Computer Society Conference on (Volume:2)*, Washington, DC, USA, 2004.

[47] C.-C. Chang and C.-J. Lin, "LIBSVM: A library for support vector machines," *ACM Transactions on Intelligent Systems and Technology (TIST)*, vol. 2, no. 3, May 2011.

[48] (2015) RTL-SDR.com - About RTL-SDR. [Online]. Available: http://www.rtl-sdr.com/about-rtl-sdr/

[49] (2013) Oscocom SDR - rtlsdr. [Online]. Available: http://www.sdr.osmocom.org/trac/wiki/rtl-sdr

[50] (2015) RTL-SDR and GNU Radio with Realtek RTL2832U [Elonics E4000/Raphael Micro R820T] software defined radio receivers. Superkuh. [Online]. Available: http://superkuh.com/rtlsdr.html

CHAPTER 6 APPENDIX

6.1 APPENDIX 1 - CONFUSION MATRICES

All entries in the confusion matrix are the percentage classifications for each class considered. The diagonals are thus the percentage correct classifications per class.

Table 6.1. Confusion matrix for KNN classifier when the cellular telephone GSM bursts were recorded at a transmission power of 9 dBm.

	bb0	**bb1**	**bb2**	**bb3**	**bb4**	**ss20**	**ss21**	**ss22**	**ss23**	**ss24**	**ss30**	**ss31**	**ss32**	**ss34**	**ss35**
bb0	**62**	0	1	0	37	0	0	0	0	0	0	0	0	0	0
bb1	0	**100**	0	0	0	0	0	0	0	0	0	0	0	0	0
bb2	9	0	**91**	0	0	0	0	0	0	0	0	0	0	0	0
bb3	0	0	0	**100**	0	0	0	0	0	0	0	0	0	0	0
bb4	16	0	2	0	**82**	0	0	0	0	0	0	0	0	0	0
ss20	0	0	0	0	0	**93**	2	0	1	4	0	0	0	0	0
ss21	0	0	0	0	0	1	**99**	0	0	0	0	0	0	0	0
ss22	0	0	0	0	0	0	0	**100**	0	0	0	0	0	0	0
ss23	0	0	0	0	0	4	0	0	**79**	17	0	0	0	0	0
ss24	0	0	0	0	0	29	0	0	10	**61**	0	0	0	0	0
ss30	0	0	0	0	0	0	0	0	0	0	**95**	0	0	5	0
ss31	0	0	0	0	0	0	0	0	0	0	0	**79**	0	0	21
ss32	0	0	0	0	0	0	0	0	0	0	0	0	**100**	0	0
ss34	0	0	0	0	0	0	0	0	0	0	11	0	0	**89**	0
ss35	0	0	0	0	0	0	0	0	0	0	0	16	0	0	**84**

Table 6.2. Confusion matrix for KNN classifier when the cellular telephone GSM bursts were recorded at a transmission power of 19 dBm.

	bb0	**bb1**	**bb2**	**bb3**	**bb4**	**ss20**	**ss21**	**ss22**	**ss23**	**ss24**	**ss30**	**ss31**	**ss32**	**ss34**	**ss35**
bb0	**17**	0	8	0	75	0	0	0	0	0	0	0	0	0	0
bb1	0	**100**	0	0	0	0	0	0	0	0	0	0	0	0	0
bb2		0	**60**	0	35	0	0	0	0	0	0	0	0	0	0
bb3	0	0	0	**100**	0	0	0	0	0	0	0	0	0	0	0
bb4	59	0	6	0	**35**	0	0	0	0	0	0	0	0	0	0
ss20	0	0	0	0	0	**56**	0	0	44	0	0	0	0	0	0
ss21	0	0	0	0	0	0	**53**	0	0	47	0	0	0	0	0
ss22	0	0	0	0	0	0	0	**100**	0	0	0	0	0	0	0
ss23	0	0	0	0	0	25	0	0	**75**	0	0	0	0	0	0
ss24	0	0	0	0	0	0	18	0	0	**82**	0	0	0	0	0
ss30	0	0	0	0	0	0	0	0	0	0	**20**	0	0	3	77
ss31	0	0	0	0	0	0	0	0	0	0	11	**42**	0	47	0
ss32	0	0	0	0	0	0	0	0	0	0	0	0	**100**	0	0
ss34	0	0	0	0	0	0	0	0	0	0	1	13	0	**85**	1
ss35	0	0	0	0	0	0	0	0	0	0	71	2	0	15	**12**

Table 6.3. Confusion matrix for KNN classifier when the cellular telephone GSM bursts were recorded at a transmission power of 29 dBm.

	bb0	**bb1**	**bb2**	**bb3**	**bb4**	**ss20**	**ss21**	**ss22**	**ss23**	**ss24**	**ss30**	**ss31**	**ss32**	**ss34**	**ss35**
bb0	**93**	1	0	0	6	0	0	0	0	0	0	0	0	0	0
bb1	96	**1**	0	0	3	0	0	0	0	0	0	0	0	0	0
bb2	0	3	**97**	0	0	0	0	0	0	0	0	0	0	0	0
bb3	0	0	0	**100**	0	0	0	0	0	0	0	0	0	0	0
bb4	0	47	43	0	**10**	0	0	0	0	0	0	0	0	0	0
ss20	0	0	0	0	0	**76**	0	0	24	0	0	0	0	0	0
ss21	0	0	0	0	0	0	**86**	2	0	12	0	0	0	0	0
ss22	0	0	0	0	1	0	7	**82**	0	10	0	0	0	0	0
ss23	0	0	0	0	0	12	0	0	**88**	0	0	0	0	0	0
ss24	0	0	0	0	0	0	4	0	0	**96**	0	0	0	0	0
ss30	1	0	5	3	0	26	0	0	5	0	**60**	0	0	0	0
ss31	0	0	0	0	0	0	0	0	0	0	10	**81**	1	7	1
ss32	0	0	0	0	0	0	0	0	0	0	0	0	**96**	0	4
ss34	0	0	0	0	0	0	0	0	0	0	21	76	0	**3**	0
ss35	0	0	0	0	0	0	0	0	0	0	0	3	1	28	**6**

Table 6.4. Confusion matrix for Mahalanobis distance classifier when the cellular telephone GSM bursts were recorded at a transmission power of 9 dBm.

	bb0	**bb1**	**bb2**	**bb3**	**bb4**	**ss20**	**ss21**	**ss22**	**ss23**	**ss24**	**ss30**	**ss31**	**ss32**	**ss34**	**ss35**
bb0	**61**	1	0	0	38	0	0	0	0	0	0	0	0	0	0
bb1	0	**100**	0	0	0	0	0	0	0	0	0	0	0	0	0
bb2	9	0	**91**	0	0	0	0	0	0	0	0	0	0	0	0
bb3	0	0	0	**100**	0	0	0	0	0	0	0	0	0	0	0
bb4	16	0	1	0	**83**	0	0	0	0	0	0	0	0	0	0
ss20	0	0	0	0	0	**90**	3	0	1	6	0	0	0	0	0
ss21	0	0	0	0	0	3	**97**	0	0	0	0	0	0	0	0
ss22	0	0	0	0	0	0	0	**100**	0	0	0	0	0	0	0
ss23	0	0	0	0	0	11	0	0	**63**	26	0	0	0	0	0
ss24	0	0	0	0	0	14	0	0	2	**84**	0	0	0	0	0
ss30	0	0	0	0	0	0	0	0	0	0	**87**	0	1	12	0
ss31	0	0	0	0	0	0	0	0	0	0	0	**86**	0	0	14
ss32	0	0	0	0	0	0	0	0	0	0	0	0	**100**	0	0
ss34	0	0	0	0	0	0	0	0	0	0	7	0	0	**93**	0
ss35	0	0	0	0	0	0	0	0	0	0	0	20	0	0	**80**

Table 6.5. Confusion matrix for Mahalanobis distance classifier when the cellular telephone GSM bursts were recorded at a transmission power of 19 dBm.

	bb0	**bb1**	**bb2**	**bb3**	**bb4**	**ss20**	**ss21**	**ss22**	**ss23**	**ss24**	**ss30**	**ss31**	**ss32**	**ss34**	**ss35**
bb0	**10**	0	19	0	71	0	0	0	0	0	0	0	0	0	0
bb1	0	**100**	0	0	0	0	0	0	0	0	0	0	0	0	0
bb2	3	0	**64**	0	33	0	0	0	0	0	0	0	0	0	0
bb3	0	0	0	**100**	0	0	0	0	0	0	0	0	0	0	0
bb4	35	0	9	0	**56**	0	0	0	0	0	0	0	0	0	0
ss20	0	0	0	0	0	**88**	0	0	12	0	0	0	0	0	0
ss21	0	0	0	0	0	0	**60**	0	0	40	0	0	0	0	0
ss22	0	0	0	0	0	0	0	**100**	0	0	0	0	0	0	0
ss23	0	0	0	0	0	67	0	0	**33**	0	0	0	0	0	0
ss24	0	0	0	0	0	0	11	0	0	**89**	0	0	0	0	0
ss30	0	0	0	0	0	0	0	0	0	0	**13**	0	0	2	85
ss31	0	0	0	0	0	0	0	0	0	0	6	**36**	1	55	2
ss32	0	0	0	0	0	0	0	0	0	0	0	0	**100**	0	0
ss34	0	0	0	0	0	0	0	0	0	0	3	9	1	**86**	1
ss35	0	0	0	0	0	0	0	0	0	0	68	3	0	11	**18**

Table 6.6. Confusion matrix for Mahalanobis distance classifier when the cellular telephone GSM bursts were recorded at a transmission power of 29 dBm.

	bb0	**bb1**	**bb2**	**bb3**	**bb4**	**ss20**	**ss21**	**ss22**	**ss23**	**ss24**	**ss30**	**ss31**	**ss32**	**ss34**	**ss35**
bb0	**96**	0	0	0	4	0	0	0	0	0	0	0	0	0	0
bb1	97	**1**	0	0	2	0	0	0	0	0	0	0	0	0	0
bb2	0	5	**95**	0	0	0	0	0	0	0	0	0	0	0	0
bb3	0	0	0	**100**	0	0	0	0	0	0	0	0	0	0	0
bb4	0	52	47	0	**1**	0	0	0	0	0	0	0	0	0	0
ss20	0	0	0	0	0	**81**	0	0	19	0	0	0	0	0	0
ss21	0	0	0	0	0	0	**84**	4	0	12	0	0	0	0	0
ss22	0	1	0	0	0	0	2	**96**	0	1	0	0	0	0	0
ss23	0	0	0	0	0	22	0	0	**78**	0	0	0	0	0	0
ss24	0	0	0	0	0	0	9	0	0	**91**	0	0	0	0	0
ss30	7	0	0	33	0	0	0	0	0	0	**60**	0	0	0	0
ss31	0	0	0	0	0	0	0	0	0	0	11	**76**	0	12	1
ss32	0	0	0	0	0	0	0	0	0	0	1	1	**95**	0	3
ss34	0	0	0	0	0	0	0	0	0	0	26	59	0	**15**	0
ss35	0	0	0	0	0	0	0	0	0	0	0	6	0	28	**66**

Table 6.7. Confusion matrix for ensemble classifier when the cellular telephone GSM bursts were recorded at a transmission power of 9 dBm.

	bb0	**bb1**	**bb2**	**bb3**	**bb4**	**ss20**	**ss21**	**ss22**	**ss23**	**ss24**	**ss30**	**ss31**	**ss32**	**ss34**	**ss35**
bb0	**59**	1	0	0	40	0	0	0	0	0	0	0	0	0	0
bb1	0	**100**	0	0	0	0	0	0	0	0	0	0	0	0	0
bb2	9	0	**91**	0	0	0	0	0	0	0	0	0	0	0	0
bb3	0	0	0	**100**	0	0	0	0	0	0	0	0	0	0	0
bb4	15	0	2	0	**83**	0	0	0	0	0	0	0	0	0	0
ss20	0	0	0	0	0	**92**	2	0	1	5	0	0	0	0	0
ss21	0	0	0	0	0	1	**99**	0	0	0	0	0	0	0	0
ss22	0	0	0	0	0	0	0	**100**	0	0	0	0	0	0	0
ss23	0	0	0	0	0	7	0	0	**76**	17	0	0	0	0	0
ss24	0	0	0	0	0	19	0	0	10	**71**	0	0	0	0	0
ss30	0	0	0	0	0	0	0	0	0	0	**95**	0	1	4	0
ss31	0	0	0	0	0	0	0	0	0	0	0	**86**	0	0	14
ss32	0	0	0	0	0	0	0	0	0	0	0	0	**100**	0	0
ss34	0	0	0	0	0	0	0	0	0	0	8	0	0	**92**	0
ss35	0	0	0	0	0	0	0	0	0	0	0	20	0	0	**80**

Table 6.8. Confusion matrix for the ensemble classifier when the cellular telephone GSM bursts were recorded at a transmission power of 19 dBm.

	bb0	**bb1**	**bb2**	**bb3**	**bb4**	**ss20**	**ss21**	**ss22**	**ss23**	**ss24**	**ss30**	**ss31**	**ss32**	**ss34**	**ss35**
bb0	**15**	0	11	0	74	0	0	0	0	0	0	0	0	0	0
bb1	0	**100**	0	0	0	0	0	0	0	0	0	0	0	0	0
bb2	3	0	**61**	0	36	0	0	0	0	0	0	0	0	0	0
bb3	0	0	0	**100**	0	0	0	0	0	0	0	0	0	0	0
bb4	42	0	9	0	**49**	0	0	0	0	0	0	0	0	0	0
ss20	0	0	0	0	0	**65**	0	0	35	0	0	0	0	0	0
ss21	0	0	0	0	0	0	**54**	0	0	46	0	0	0	0	0
ss22	0	0	0	0	0	0	0	**100**	0	0	0	0	0	0	0
ss23	0	0	0	0	0	40	0	0	**60**	0	0	0	0	0	0
ss24	0	0	0	0	0	0	17	0	0	**83**	0	0	0	0	0
ss30	0	0	0	0	0	0	0	0	0	0	**19**	0	0	3	78
ss31	0	0	0	0	0	0	0	0	0	0	12	**41**	1	46	0
ss32	0	0	0	0	0	0	0	0	0	0	0	0	**100**	0	0
ss34	0	0	0	0	0	0	0	0	0	0	1	11	1	**86**	1
ss35	0	0	0	0	0	0	0	0	0	0	71	2	0	14	**13**

Table 6.9. Confusion matrix for the ensemble classifier when the cellular telephone GSM bursts were recorded at a transmission power of 29 dBm.

	bb0	**bb1**	**bb2**	**bb3**	**bb4**	**ss20**	**ss21**	**ss22**	**ss23**	**ss24**	**ss30**	**ss31**	**ss32**	**ss34**	**ss35**
bb0	**93**	1	0	0	6	0	0	0	0	0	0	0	0	0	0
bb1	96	**1**	0	0	3	0	0	0	0	0	0	0	0	0	0
bb2	0	3	**97**	0	0	0	0	0	0	0	0	0	0	0	0
bb3	0	0	0	**100**	0	0	0	0	0	0	0	0	0	0	0
bb4	0	47	43	0	**10**	0	0	0	0	0	0	0	0	0	0
ss20	0	0	0	0	0	**76**	0	0	24	0	0	0	0	0	0
ss21	0	0	0	0	0	0	**87**	2	0	11	0	0	0	0	0
ss22	0	0	0	0	1	0	7	**85**	0	7	0	0	0	0	0
ss23	0	0	0	0	0	12	0	0	**88**	0	0	0	0	0	0
ss24	0	0	0	0	0	0	5	0	0	**95**	0	0	0	0	0
ss30	7	0	0	33	0	0	0	0	0	0	**60**	0	0	0	0
ss31	0	0	0	0	0	0	0	0	0	0	10	**81**	1	7	1
ss32	0	0	0	0	0	0	0	0	0	0	0	0	**96**	0	4
ss34	0	0	0	0	0	0	0	0	0	0	21	75	0	**4**	0
ss35	0	0	0	0	0	0	0	0	0	0	0	3	1	26	**70**

Table 6.10. Confusion matrix for SVM classifier when the cellular telephone GSM bursts were recorded at a transmission power of 9 dBm.

	bb0	**bb1**	**bb2**	**bb3**	**bb4**	**ss20**	**ss21**	**ss22**	**ss23**	**ss24**	**ss30**	**ss31**	**ss32**	**ss34**	**ss35**
bb0	**62**	0	2	0	36	0	0	0	0	0	0	0	0	0	0
bb1	0	**100**	0	0	0	0	0	0	0	0	0	0	0	0	0
bb2	1	0	**90**	0	9	0	0	0	0	0	0	0	0	0	0
bb3	0	0	0	**100**	0	0	0	0	0	0	0	0	0	0	0
bb4	41	0	2	0	**57**	0	0	0	0	0	0	0	0	0	0
ss20	0	0	0	0	0	**92**	2	0	2	4	0	0	0	0	3
ss21	2	0	0	0	0	4	**100**	0	0	0	0	0	0	0	0
ss22	1	0	0	0	0	0	0	**100**	0	0	0	0	0	0	0
ss23	0	0	0	0	0	2	0	0	**92**	6	0	0	0	0	0
ss24	2	0	0	0	0	27	0	0	28	**45**	0	0	0	0	0
ss30	1	0	0	0	0	0	0	0	0	0	**92**	0	0	8	0
ss31	0	0	0	0	0	0	0	0	0	0	0	**72**	0	0	28
ss32	0	0	0	0	0	0	0	0	0	0	0	0	**100**	0	0
ss34	0	0	0	0	0	0	0	0	0	0	12	0	0	**88**	0
ss35	0	0	0	0	0	0	0	0	0	0	0	9	0	0	**91**

Table 6.11. Confusion matrix for SVM classifier when the cellular telephone GSM bursts were recorded at a transmission power of 19 dBm.

	bb0	**bb1**	**bb2**	**bb3**	**bb4**	**ss20**	**ss21**	**ss22**	**ss23**	**ss24**	**ss30**	**ss31**	**ss32**	**ss34**	**ss35**
bb0	**21**	0	10	0	69	0	0	0	0	0	0	0	0	0	0
bb1	0	**100**	25	0	1	0	0	0	0	0	0	0	0	0	0
bb2	7	0	**56**	0	37	0	0	0	0	0	0	0	0	0	0
bb3	0	0	0	**100**	0	0	0	0	0	0	0	0	0	0	0
bb4	45	0	10	0	**45**	0	0	0	0	0	0	0	0	0	0
ss20	0	0	0	0	0	**60**	0	0	40	0	0	0	0	0	0
ss21	0	0	0	0	0	0	**51**	0	0	49	0	0	0	0	0
ss22	0	0	0	0	0	0	0	**100**	0	0	0	0	0	0	0
ss23	0	0	0	0	0	13	0	0	**87**	0	0	0	0	0	0
ss24	0	0	0	0	0	0	26	0	0	**74**	0	0	0	0	0
ss30	0	0	0	0	0	0	0	0	0	0	**23**	0	0	1	76
ss31	0	0	0	0	0	0	0	0	0	0	6	**41**	0	53	0
ss32	0	0	0	0	0	0	0	0	0	0	0	0	**99**	0	1
ss34	0	0	0	0	0	0	0	0	0	0	0	27	0	**66**	1
ss35	0	0	0	0	0	0	0	0	0	0	75	2	0	16	**7**

Table 6.12. Confusion matrix for SVM classifier when the cellular telephone GSM bursts were recorded at a transmission power of 29 dBm.

	bb0	**bb1**	**bb2**	**bb3**	**bb4**	**ss20**	**ss21**	**ss22**	**ss23**	**ss24**	**ss30**	**ss31**	**ss32**	**ss34**	**ss35**
bb0	**93**	0	0	0	7	0	0	0	0	0	0	0	0	0	0
bb1	95	**0**	0	0	5	0	0	0	0	0	0	0	0	0	0
bb2	0	6	**94**	0	0	0	0	0	0	0	0	0	0	0	0
bb3	0	0	0	**100**	0	0	0	0	0	0	0	0	0	0	0
bb4	0	72	25	0	**3**	0	0	0	0	0	0	0	0	0	0
ss20	0	0	0	0	0	**78**	0	0	22	0	0	0	0	0	0
ss21	0	0	0	0	0	0	**83**	2	0	15	0	0	0	0	0
ss22	0	0	0	0	4	0	10	**81**	0	5	0	0	0	0	0
ss23	0	0	0	0	0	19	0	0	**81**	0	0	0	0	0	0
ss24	0	0	0	0	0	0	11	0	0	**89**	0	0	0	0	0
ss30	35	0	0	0	0	5	0	0	0	0	**60**	0	0	0	0
ss31	0	0	0	0	0	0	0	0	0	0	4	**89**	1	4	2
ss32	0	0	0	0	0	0	0	0	0	0	0	0	**94**	0	6
ss34	0	0	0	0	0	0	0	0	11	83	0	0	0	**6**	0
ss35	0	0	0	0	0	0	0	0	0	0	0	13	1	13	**73**