Architecture for ES Receiver Systems Targeted at Commercial Wireless Communications

Warren P. du Plessis
Council for Scientific and Industrial Research (CSIR), Pretoria, 0001, South Africa

***Abstract*—Commercial wireless communications system are increasingly being used by criminal, paramilitary and military operators. The detection and location of such systems is thus crucially important in many applications. Modern electronic support (ES) systems are descended from systems intended for the detection of small numbers of high-power radar systems, and are thus not suitable for the low-power transmitters and dense signal environments typical of commercial communications networks. An ES system architecture suitable for commercial communications systems is proposed, and the benefits of this architecture are outlined.**

***Keywords*—Electronic support (ES), digital receiver, and communications intelligence (COMINT).**

I. Introduction

Commercial wireless communications systems, especially cellular networks, are increasingly being used by criminal, paramilitary and military operators. Examples of such use include rhino poaching [1], [2], guiding illegal immigrants [3] and insurgent attacks [4], [5]. These new uses of commercial cellular phones to co-ordinate complex operations are motivated by the low cost and wide availability of reliable cellular communications. Even the United States' military is evaluating the use of smartphones by its soldiers [6]. The location and tracking of cellular systems is thus becoming increasingly important, as evidenced by the passage of legislation such as Regulation of Interception of Communications and Provision of Communication-related Information Act (RICA) in South Africa [7].

While the natural approach to achieving the detection and tracking of cellular phones would appear to be the use of the cellular network itself, this is generally not possible. Firstly, a legal framework must exist to ensure that cellular network operators are required to provide the required information to security forces. However, privacy concerns in modern democracies mean that such a framework is difficult and time-consuming to establish – if it is possible at all. But even then, such a framework would only apply to network operators in one country, and many of the activities described above are perpetrated across the borders between nations. Nations are justifiably hesitant to grant other nations even limited access to information about and control over their industries (cellular network operators in this case) and citizens, especially before criminal activities have been proved. It is thus unlikely that the required level of access to cellular networks will be achieved within a reasonable time frame, if it can be achieved at all.

This reality leads directly to a requirement for communications intelligence (COMINT) electronic support (ES) receivers which can detect and locate cellular phones. However, this simple-sounding task is noticeably more challenging than it might appear. The success of cellular systems means that these systems have vast numbers of users, many of whom will be actively accessing the network at any given time. Separating individual users – let alone identifying criminal or paramilitary users – in such a dense signal environment is extremely challenging. Furthermore, cellular networks are designed to ensure that base transceiver stations (BTSs) and mobile devices transmit only the minimum power necessary to maintain a reliable connection. This means that all transmitters of interest will be operating at low power, further complicating their detection. Lastly, cellular transmissions tend to be very short, and slow frequency hopping (where a BTS and mobile devices gradually change their operating frequency) is sometimes implemented to reduce the effects of fading. The probability of intercept (POI) of a receiver is thus reduced unless all frequencies of interest are monitored continuously. Furthermore, integration times are limited by the duration of the transmitted signal rather than by the receiver system requirements.

Modern ES systems are descended from systems developed to detect and locate relatively limited numbers of high-power radar transmitters. As described above, commercial cellular systems comply with neither of these assumptions, suggesting that traditional ES systems will not be effective in this role. There is thus a requirement for ES receivers specifically developed for COMINT of cellular communications systems.

This paper describes the architecture of an ES system that is targeted at the detection and location of cellular phones. This architecture is based on the use of large numbers of relatively simple receiver elements. Modern Radio Frequency (RF) and digital signal processing (DSP) technologies mean that these receiver elements can be highly integrated, thereby achieving high performance while maintaining low cost. The use of a large number of independent channels achieves a number of benefits. High antenna gain can be realised by coherently processing the signals received by a large number of channels operating at the same frequency. Alternatively, a wide range of frequencies can be monitored by assigning different frequencies to each channel. Lastly, this approach is well matched to modern signal-processing technologies where high performance is achieved through parallelism (large numbers of relatively low-performance processing units operating together) allowing complex algorithms to be implemented.

The unique ES challenges associated with commercial cellular systems are described in more detail in Section II as a motivation for a new ES architecture for COMINT. Section III describes the architecture of the proposed system and demonstrates how this architecture addresses the challenges described in Section II. The work is concluded in Section IV.

W. P. du Plessis, wduplessis@ieee.org, Tel: +27-12-841-3078, Fax: +27-12-841-2455.

II. Challenges Associated with ES for Cellular Communications

The challenges associated with ES for commercial cellular arise from low transmit power, a dense signal environment, short transmissions which change frequency and the scenario geometry. Each of these challenges is considered in more detail below with the emphasis on the Global System for Mobile Communications (GSM) standard due to its widespread adoption, and a simple link budget is developed to summarise the magnitude of the problem.

A. *Low Signal Power*

The power transmitted by a mobile device is extremely low both as a result of device limitations and due to power control.

Mobile devices have limited size and are powered by small batteries, limiting the available power. For GSM systems operating in the E-GSM 900 and DCS 1800 bands, mobile devices are required to have a maximum transmit power of 33 dBm (2 W) and 30 dBm (1 W) respectively [8], [9]. However, these specifications have a tolerance of ± 2 dB under normal conditions and ± 2.5 dB under extreme conditions [8], so these values could be as low as 30.5 dBm (1.1 W) and 27.5 dBm (0.56 W) in the E-GSM 900 and DCS 1800 bands respectively while still complying with the GSM specification.

However, a far greater concern for a cellular network is the interference caused by mobile devices and BTSs which transmit more power than is required for reliable communications. Modern cellular systems thus implement power control whereby the power transmitted by a device can be reduced to minimise interference. The GSM standard allows for power to be reduced by 15 steps of 2 dB each thereby allowing a power reduction of 30 dB [8]–[10]. However, these values are subject to tolerances of ± 5 dB under normal conditions and ± 6 dB under extreme conditions [8], so the power levels in the E-GSM 900 and DCS 1800 bands can be as low as -1 dBm (0.79 mW) and -6 dBm (0.25 mW) respectively.

B. *Dense Signal Environment*

In 2011, there were an estimated 5.6 billion mobile connections worldwide [11] with a global population of 7 billion people [12]. Africa had an estimated 649 million subscribers by the end of 2011, so roughly two out of three people on the continent have mobile connectivity in some form [13].

This extremely large number of users of commercial cellular systems coupled with the limited bandwidth available for such systems [14] leads to very dense signal environments. To further complicate matters, there is a high likelihood that users transmissions' will overlap in time and frequency, especially for newer systems like Universal Mobile Telecommunications System (UMTS) and Long-Term Evolution (LTE) which are based on techniques such as carrier-division multiple access (CDMA) and orthogonal frequency division multiplexing (OFDM). The traditional means for de-interleaving radar signals are inadequate in such dense signal environments.

C. *Short Signals With Changing Frequencies*

Communications signals tend to be very short mainly as a result of the use of time-division multiple access (TDMA) to support multiple users or time-division duplex (TDD) to separate the uplink from the downlink. Furthermore, mobile devices only transmit when data are available both to reduce interference and to improve battery life.

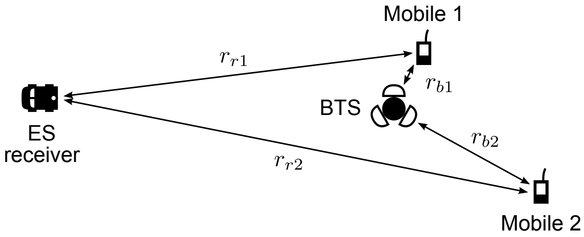


Fig. 1. Scenario geometry showing two important special cases.

GSM uses a combination of frequency-division multiple access (FDMA) and TDMA to support multiple users [9], [10]. FDMA is achieved by utilising a 200-kHz channel spacing over the available bands. TDMA is implemented by allowing each frequency channel to support eight logical channels with timeslots lasting 577 μs and a frame of eight timeslots lasts 4.615 ms. However, a GSM burst is shorter than a full timeslot at 547 μs to ensure some robustness to timing differences caused by range.

GSM also implements slow frequency hopping whereby the channel frequency changes from burst to burst [9], [10].

Lastly, GSM allows discontinuous transmission to reduce interference and improve battery life [9], [10]. This approach can be particularly effective as normal speech has pauses amounting to approximately 50% of the total conversation.

An ES system which is required to detect GSM signals thus has to contend with short transmissions of only 547 μs, so the long averaging typical of many ES systems is simply not possible.

Furthermore, each transmission could be on a different frequency due to slow frequency hopping, so the time between interception of transmissions can be large. Lastly, discontinuous transmission means that the mobile might not transmit when allocated to a frequency being monitored. The POI of a GSM signal can thus be extremely low.

D. *Scenario Geometry*

The relative positioning of a mobile phone, BTS and ES receiver has a major effect on the ES receiver requirements. Two important scenarios are shown in Fig. 1.

Mobile 1 in Fig. 1 is extremely close to the BTS (r_{b1} is small) and uplink power control will thus ensure that this device transmits the minimum allowable power. The ES receiver is thus tasked with detecting the mobile's extremely weak signal at long range (r_{r1}). This type of scenario can arise both in urban and rural environments. Cells tend to be small in urban environments to accommodate high user densities [9], so mobile devices will always be near a BTS. In a rural environment, a spotter on a hilltop could be underneath a BTS positioned on the same hilltop.

Mobile 2 in Fig. 1 is at the extreme edge of the BTS's coverage area (r_{b2} is at its largest value). The uplink power control problem associated with mobile 1 is thus avoided, but the range from the mobile to the receiver (r_{r2}) is extremely large. The ES receiver is thus required to detect the mobile at extremely long range, and importantly, the ES receiver is required to detect the mobile at a greater range than the BTS

TABLE I
LINK BUDGET FOR TYPICAL GSM SYSTEMS WITH BTS AND MOBILE HEIGHTS OF 30 M AND 1.5 M RESPECTIVELY.

Description	E-GSM 900		DCS 1800		Notes
	Uplink	Downlink	Uplink	Downlink	
Frequency	897.5 MHz	942.5 MHz	1747.5 MHz	1842.5 MHz	Centre of the band
Receiver	BTS	Mobile	BTS	Mobile	
Noise floor	-174 dBm	-174 dBm	-174 dBm	-174 dBm	kT with $T = 300$ K
Bandwidth	54 dBHz	54 dBHz	54 dBHz	54 dBHz	270,833 Hz
Noise figure	7.5 dB	9.5 dB	7.5 dB	9.5 dB	Achieves specified sensitivities
Cable loss	2 dB		2.5 dB		Feeder loss, two jumper cables and lightning protection
TMA noise figure	2 dB		2.5 dB		Jumper-cable loss included
TMA gain	12 dB		12 dB		
System noise figure	3.5 dB	9.5 dB	4 dB	9.5 dB	Cascade noise figure computation (see e.g. [15])
System noise floor	-116.5 dBm	-110 dBm	-116 dBm	-110 dBm	Noise floor + bandwidth + noise figure
Receiver antenna gain	15 dBi	0 dBi	15 dBi	0 dBi	
Diversity gain	5 dB		5 dB		
Transmitter	Mobile	BTS	Mobile	BTS	
Transmitter power	33 dBm	43 dBm	30 dBm	40 dBm	
Cable loss		2 dB		2.5 dB	Feeder loss, two jumper cables and lightning protection
Losses	9 dB		9 dB		Antenna and body loss
Transmit antenna gain	0 dBi	15 dBi	0 dBi	15 dBi	
EIRP	24 dBm	56 dBm	21 dBm	52.5 dBm	Transmit power - losses + antenna gain
Required SNR	8 dB	8 dB	8 dB	8 dB	
Losses		9 dB		9 dB	Antenna and body loss
Interference degradation	3 dB	3 dB	3 dB	3 dB	Effect of interference with other signals
Maximum allowable path loss	149.5 dB	146 dB	146 dB	142.5 dB	EIRP - SNR - loss - interference degradation - noise floor
Range (large city)	4.5 km	3.5 km	1.6 km	1.2 km	
Range (medium/small city)	4.5 km	3.5 km	1.6 km	1.5 km	
Range (suburban)	8.7 km	6.7 km	2.0 km	1.5 km	
Range (rural quasi-open)	21.1 km	16.4 km	11.2 km	8.7 km	
Range (rural open)	29.2 km	22.7 km	15.6 km	12.0 km	

($r_{r2} > r_{b2}$). This scenario will arise most frequently in rural environments where cell sizes are maximised due to low user densities [9].

E. Link Budget

A link budget for a typical GSM system is presented in Table I. The values in the table are based on those presented in the GSM standards [8], [16], and the ranges are computed using the Hata/COST-231 model described in the GSM standards [16].

Table I shows that lower frequencies lead to larger cells, mainly as a result of lower path loss at a specified range. This suggests that E-GSM 900 transmissions will be more prevalent in rural areas where cell sizes are large.

However, the important most observation from Table I is that maximum ranges over which effective communications are possible are surprisingly small. This is despite the high gain of the BTS antennas (15 dBi), diversity gain (5 dB), the low BTS receiver noise (noise figure of 3 dB to 4 dB) and the low signal-to-noise ratio (SNR) required (8 dB). A typical ES receiver will have an antenna gain of 5 dBi or less, no diversity gain, a noise figure of 3 dB to 4 dB, and an SNR requirement of 10 dB. A typical ES system thus has a maximum allowable path loss which is 15 dB to 20 dB worse than a BTS.

Clearly, some means of significantly improving the performance of ES systems needs to be developed if detection of the mobile devices in the scenarios in Fig. 1 is to be achieved.

III. PROPOSED ES ARCHITECTURE FOR CELLULAR COMMUNICATIONS

The proposed ES architecture attempts to overcome the challenges described in Section II. The main challenge is the extremely low power which will reach an ES receiver, so the primary focus of the proposed architecture is to maximise the system sensitivity. However, the proposed architecture is also able to overcome other challenges as highlighted below.

The proposed system architecture is described in Fig. 2. The underlying concept is to integrate the antenna and the complete receiver front end into single unit. A large number of such integrated receiver systems will then be combined into an ES system to achieve good system-level performance.

While this system resembles a channelised receiver [17], [18], it differs in two important respects. Firstly, each receiver element contains a complete receiver which can act independently of the other receiver elements. By way of example, this means that the frequency of each receiver element can be independently controlled, unlike channelised receivers where the operating frequencies of the channels are fixed relative to each other. Secondly, the signals received by multiple receiver elements operating at the same frequency can be processed coherently in the proposed system. Coherent processing allows antenna gain to be achieved, accurate phase-based direction finding (DF) to be performed, and opens the possibility of the development of advanced signal-processing algorithms for improved detection of signals.

A system based on the proposed architecture in Fig. 2 will have a number of benefits including the following.

- Large numbers of elements mean that large antenna arrays with high antenna gain can be constructed by coherently processing the signals from a number of receiver elements.
- The large number of elements also offers the potential to obtain more independent samples of the environment, thereby allowing better de-interleaving of signals.
- The integration of the antenna and the RF front end will help to reduce the receiver noise figure.
- The use of lower-rate analogue-to-digital converters (ADCs) offers the opportunity to utilise devices with

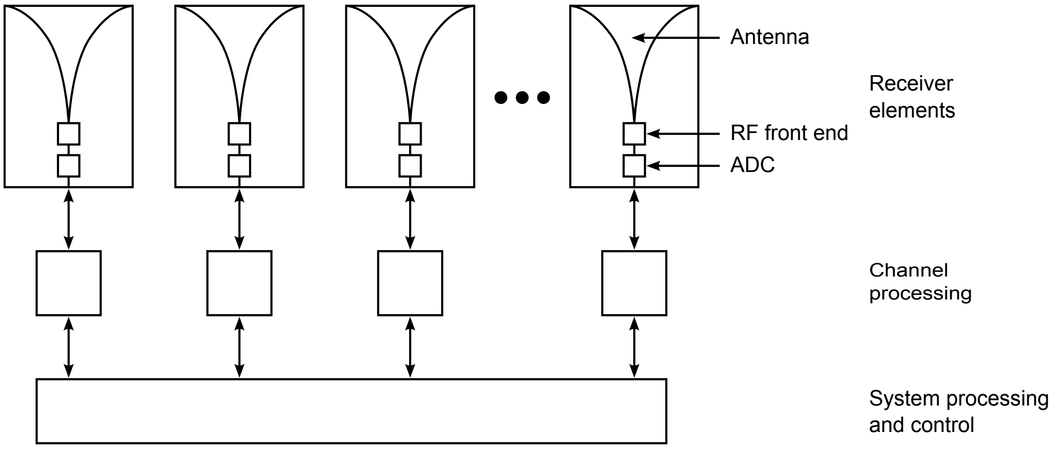
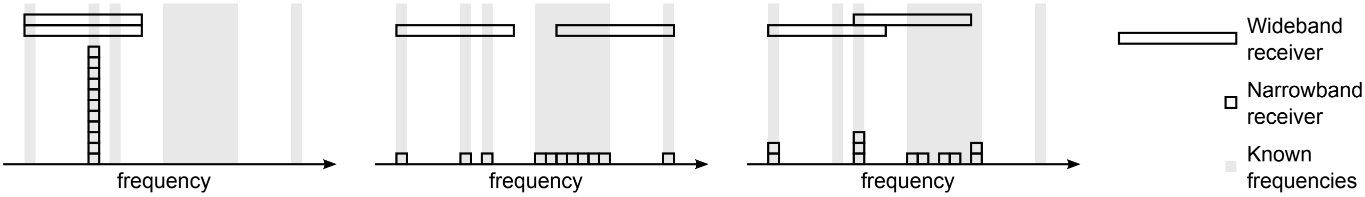


Fig. 2. System block diagram.



(a) High antenna gain. (b) Wide frequency coverage. (c) Combination. (d) Key.

Fig. 3. Demonstration of the versatility of the proposed ES system architecture.

higher dynamic range (more bits), thereby improving the system dynamic range.

- Each receiver element produces a digital output, removing the need for low-loss, phase-matched RF cables. A power-supply line, a low-frequency local oscillator signal, digital control lines and a digital output are all that each receiver element requires to function.
- The use of a large number of low data-rate streams of data is ideally suited to modern, highly parallel signal-processing technologies.
- The concept is inherently scalable depending on the number of receiver elements used to construct a system.
- The large number of elements makes the system extremely versatile.
- Large numbers of elements lead to redundancy which will improve system reliability.

The ability to achieve high antenna gain and low system noise figure can narrow the gap between ES receiver performance and BTS uplink performance.

Furthermore, this architecture is a natural match to modern DSP hardware technologies (including field-programmable gate arrays (FPGAs)). DSP devices are increasingly achieving high performance through the use of large numbers of relatively low-performance processors operating in parallel. Such parallel processing is ideally suited to the proposed architecture where large numbers of relatively low-rate data streams are generated. It might even be possible to integrate a low-cost digital signal processor (DSP) into each receiver element to perform channel-specific processing like calibration.

However, the greatest benefit of the natural match between the proposed architecture and modern DSP hardware is that it will be possible to better exploit the full processing power of existing DSP technologies. This ability to better exploit available DSP hardware creates the opportunity to allow the development and implementation of complex detection algorithms which will lower the SNR required for a mobile device to be detected.

Over and above the benefits highlighted above, the versatility of the proposed architecture is one of its main attractions. A number of examples of this versatility are shown in Fig. 3 along with comparisons to a conventional wideband ES system.

- Fig. 3(a) shows how high antenna gain can be achieved by allocating all the receiver elements to the same frequency and performing coherent processing. A system comprising a smaller number of wideband receiver elements is unable to achieve a comparable antenna gain.
- Fig. 3(b) shows how a wide range of frequencies can be covered by a number of independent receivers. The key point here is that commercial communications systems are allocated to relatively narrow bands which are separated by wide frequency ranges. Even then, not all allocated frequencies will be used in a specific area, so the ability to monitor a large number of narrowband channels can help improve system POI. Attempting to use wideband receivers to cover commercial frequency bands is inefficient as the majority of the frequencies covered have no signals of interest.
- Fig. 3(c) shows how a combination of the above two approaches is also possible whereby high antenna gain can be achieved at certain frequencies while still allowing other frequencies to be monitored. A wideband system is simply too restricted to achieve similar performance.

They key to the success of such a system is that the cost of each receiver element should be as low as possible to ensure that systems can consist of large numbers of receiver

TABLE II
COST ESTIMATE OF AN INDIVIDUAL RECEIVER ELEMENT.

Component	Type	Cost (USD)
Substrate	Rogers RO4003C substrate, 64 mil, 18"x24"	200
Low-noise amplifiers (LNAs)	Minicircuits PSA-5453+ and RFMD SGC4563Z	5
Limiter	Minicircuits RLM-33+	10
Variable attenuator	Minicircuits DAT-15R5-SP+	5
Synthesiser	3x RFMD RFFC5072	30
Mixers	3x Minicircuits LAVI-362VH+	75
Filters	Minicircuits HFTC-16+, HFCN-740D+, RHP-180+	20
ADC	Analog Devices AD9446-100	50
Additional components	Capacitors, resistors, regulators, etc.	125
Etching and assembly		625
Total		1150

elements. A conservative cost estimate for a single receiver element is given in Table II. The low cost of each receiver element was ensured in the following ways:

- The system is limiting to operation in the range of frequencies most desirable for mobile communications (below 3.5 GHz [14]). Current microwave monolithic integrated circuit (MMIC) technology means that the cost of system components in this range of frequencies is low.
- The bandwidth of each ADC is relatively low, allowing cheaper devices to be used. Wide system bandwidth is achieved through the use of large numbers of such narrow instantaneous bandwidth receiver elements.
- Mass production techniques including the automated assembly of receiver elements will further reduce the element cost.

It should also be noted that the cost estimate in Table II is conservative for the following reasons:

- It might be possible to utilise a cheaper substrate.
- Further cost reductions might be possible if all the RF components could be integrated into a single chip.
- It might be possible to use two mixing stages instead of three.
- The use of etched filters rather than separate components could be viable.
- The synthesisers specified include mixers, thereby removing the need for separate mixers.

The goal of realising low-cost receiver elements thus appears achievable. For example, Ettus Research [19] currently allows a system comprising a 100 MS/s ADC, a 400 MS/s digital-to-analogue converter (DAC), a 50 MHz to 2.2 GHz RF front end including a receiver and a transmitter, an antenna and an FPGA capable of 32 billion multiply-accumulate (MAC) operations per second to be purchased for USD 2195. And this Ettus system is far more capable, and thus expensive, than the receiver elements proposed here as it contains a transmitter as well as a receiver.

IV. CONCLUSION

Commercial wireless communications systems are becoming an increasingly important consideration due to their increasingly widespread adoption by criminal, paramilitary and even military users. The use of information gleaned from cellular network operators to monitor and track mobile devices faces a host of legal and political challenges which are unlikely to be overcome in the short term, if ever. There is thus a requirement for ES systems designed to perform COMINT for commercial communications systems.

Commercial wireless communications present major challenges to ES systems due to the low power transmitted and extremely dense signal environments. From a detection standpoint, a simple link budget shows that even a GSM BTS is only able to communicate with mobile devices over surprisingly short ranges, and ES systems have 15 dB to 20 dB poorer performance than a BTS. Furthermore, short transmission times, slow frequency hopping and discontinuous transmission can lead to an extremely low POI. Lastly, isolating a single user among the millions of users of such services is a daunting task.

A new system architecture which overcomes these difficulties is proposed. This architecture is based on the use of large numbers of low-cost receiver elements to achieve high system performance. This approach allows the potential to achieve high antenna gain, low receiver noise figure and is well-matched to modern signal-processing technologies allowing computationally-expensive algorithms to be implemented. Furthermore, this new architecture is extremely versatile allowing many of the challenges associated with commercial communications systems to be overcome.

REFERENCES

[1] 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

[2] (2011) Rhino poaching crisis. [Online]. Available: http://www.projectrhinokzn.org/?page_id=76

[3] M. Lacey, "Smugglers guide illegal immigrants with cues via cellphone," New York Times, 9 May 2011. [Online]. Available: www.nytimes.com/2011/05/09/us/09coyotes.html

[4] T. Strother, "Cell phone use by insurgents in Iraq," Urban Warfare Analysis Center, 14 May 2007. [Online]. Available: http://www.babylonscovertwar.com/Terrorist%20Groups/Weapon%20Systems/Cell%20Phone%20Use%20by%20Insurgents%20in%20Iraq.pdf

[5] J. N. Shapiro and N. B. Weidmann, "Talking about killing: Cell phones, collective action, and insurgent violence in Iraq," Social Science Research Network (SSRN), 31 May 2011. [Online]. Available: http://ssrn.com/abstract=1859638

[6] M. Milian, "U.S. government, military to get secure Android phones," Cable News Network (CNN), 3 February 2012. [Online]. Available: http://edition.cnn.com/2012/02/03/tech/mobile/government-android-phones/index.html

[7] "Regulation of interception of communications and provision of communication-related information act," in *Government Gazette*, vol. 451, no. 24286. Republic of South Africa, 22 January 2002, pp. 2–96, Act 70 of 2002.

[8] *Technical Specification Group GSM/EDGE Radio Access Network; Radio transmission and reception (Release 1999)*, 3rd Generation Partnership Project Std. 05.05, Rev. 8.20.0, November 2005. [Online]. Available: http://www.3gpp.org/ftp/Specs/html-info/0505.htm

[9] S. M. Redl, M. K. Weber, and M. K. Oliphant, *An Introduction to GSM*. Artech House, 1995.

[10] J. Eberspächer, H.-J. Vögel, and C. Bettstetter, *GSM Switching, Services and Protocols*, 2nd ed. John Wiley & Sons, Ltd, 1999.

[11] "Gartner says worldwide mobile connections will reach 5.6 billion in 2011 as mobile data services revenue totals $314.7 billion," Gartner, 4 August 2011. [Online]. Available: http://www.gartner.com/it/page.jsp?id=1759714

[12] *2011 World Population Data Sheet*. Population Reference Bureau, 2011. [Online]. Available: www.prb.org

[13] "Africa's mobile phone industry 'booming'," BBC News, 9 November 2011. [Online]. Available: http://www.bbc.co.uk/news/world-africa-15659983

[14] M. Lazarus, "The great radio spectrum famine," *IEEE Spectrum*, vol. 40, no. 10 (INT), pp. 26–31, October 2010. [Online]. Available: http://spectrum.ieee.org/telecom/wireless/the-great-radio-spectrum-famine/

[15] G. Gonzalez, *Microwave Transistor Amplifiers*, 2nd ed. Prentice Hall, 1997.

[16] *Technical Specification Group GSM/EDGE Radio Access Network; Radio network planning aspects (Release 1999)*, 3rd Generation Partnership Project Std. 03.30, Rev. 8.20.0, November 2005. [Online]. Available: http://www.3gpp.org/ftp/Specs/html-info/0330.htm

[17] D. L. Adamy, *EW 101: A first course in electronic warfare*. Artech House, 2001.

[18] D. L. Adamy, *EW 103: Tactical Battlefield Communications Electronic Warfare*. Artech House, 2009.

[19] (2012, 6 May) Ettus Research. [Online]. Available: http://ettus.com/