Software Defined Radio Implementation of CloudRAN GSM Emergency Service

Luca Simone Ronga[1] · Renato Pucci[1] · Enrico Del Re[2]

Received: 29 January 2015 / Revised: 22 May 2015 / Accepted: 7 September 2015
© Springer Science+Business Media New York 2015

Abstract The increasing availability of computing power enables new paradigms of radio communication services. The centralized baseband processing of cellular networks reveals some interesting features such as a high degree of reconfigurability, high efficiency in terms of processing power and consumed energy, fast deployment especially useful in the case of unplanned emergency networks. Moreover, in the last years free software implementation of the GSM cellular stack has been provided by the open source community, allowing the realization of custom GSM networks with off-the-shelf low cost products. This paper reports an indoor multi-cell experimental deployment of GSM voice and message communications services with low-cost SDR technology. The experimental setup is characterized by a centralized processing of baseband signals, delivered with optical fiber links to RF heads. Quality of experience and resources usage analysis has been performed and reported as an evaluation of the feasibility of this approach with low-cost HW and devices.

Keywords Emergency cellular networks · Cloud-RAN · Software defined radio · OpenBTS

1 Introduction

Stepping back from previous trends pushing network intelligence from core to edges, a new tension towards the centralization of higher network functions has initiated. The Software Defined Networking concept [1] produces a separation of control-plane from data plane in routing devices. The virtualization of network access allows more flexibility and reconfigurability of networking functions, increasing resiliency and robustness in case of failure. The availability of fast optical links feeding the radio base stations, suggested that a virtualization could also take place at PHY layer, by encapsulating baseband radio signals into network packets for a more efficient and flexible processing. The virtualization of radio access networks (RAN) functions in centralized abstract entities, namely Cloud-RAN [2], acts as a multiplier for features and configurations the new network can operate with. A relevant application which may benefit from this new architecture are the emergency cellular networks. Due to the circumstances of adoption, the opportunity to provide a "soft" configuration of deployed radio devices is a desired feature. In several emergency contexts the opportunity to provide emergency communication services over widespread cellular standards may result in increased rescued people and a faster reaction to events.

In this paper we report the results of an experiment of deployment of a multi OpenBTS base-station 2G radio network for emergency purposes in an indoor environment. OpenBTS is a free (under AGPL) software-based GSM access point that allows GSM-compatible mobile phones to make telephone calls, replacing the subsystem infrastructure of traditional GSM operator network and forwarding the data onto the Asterisk PBX via Session Initiation Protocol (SIP) and Voice-over-IP (VoIP). The experiment shows the feasibility and required network and computing resources for a centralized baseband processing of involved radio signals. The paper

✉ Luca Simone Ronga
luca.ronga@cnit.it

Renato Pucci
renato.pucci@cnit.it

Enrico Del Re
enrico.delre@unifi.it

[1] Florence Research Unit, CNIT, Florence, Italy

[2] Department of Information Engineering, University of Florence, Florence, Italy

Published online: 28 September 2015

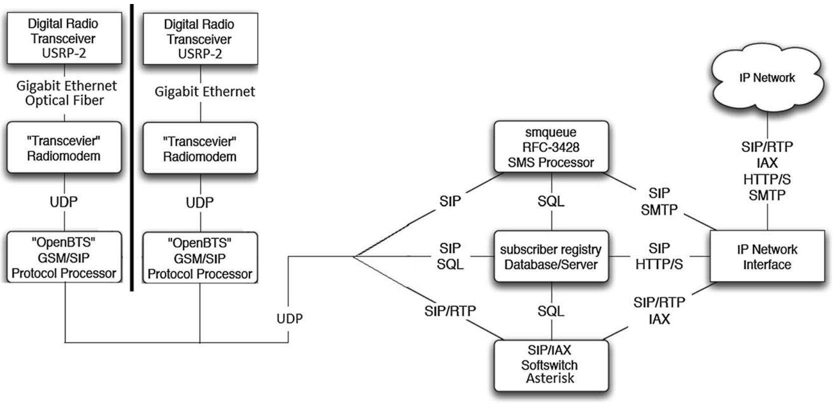

Digital Radio Transceiver USRP-2
Digital Radio Transceiver USRP-2
Gigabit Ethernet Optical Fiber
Gigabit Ethernet
"Transcevier" Radiomodem
"Transcevier" Radiomodem
UDP
UDP
"OpenBTS" GSM/SIP Protocol Processor
"OpenBTS" GSM/SIP Protocol Processor
UDP
SIP
SIP SQL
SIP/RTP
smqueue RFC-3428 SMS Processor
SQL
subscriber registry Database/Server
SQL
SIP/IAX Softswitch Asterisk
SIP SMTP
SIP HTTP/S
SIP/RTP IAX
IP Network
SIP/RTP IAX HTTP/S SMTP
IP Network Interface

Figure 1 System architecture used in the experiment.

is structured as follows: Section II provides a brief overview on the available software solution to set up a GSM network, Section III reports the adopted system architecture and the environmental setup for the experiment along with the involved devices and radio configurations. Section IV describes the measurements acquisition and comments the main results and assessments, while Section V contains some concluding remarks.

2 GSM Open Software Solutions

Over the last few years, open source community has enabled the implementation of low cost cellular networks through the exploitation of the software-defined radio (SDR) [3] technology. At the current time, there are essentially two mature software solutions to build a 2G/3G network: OpenBTS (http://openbts.org/) and OpenBSC (http://openbsc.osmocom.org/).

OpenBTS (Open Base Transceiver Station) software is an open-source Linux application that uses a software-defined radio (SDR) as the hardware that presents a 2G/3G air interface to standard compliant handsets and user devices. Even though it is called "OpenBTS", this software does not actually represent the implementation of a conventional GSM BTS, but rather the "Um" interface in the GSM architecture. A GSM BTS is a front-ended device, externally managed by a base station controller (BSC) and connecting calls thanks to a remote mobile switching center (MSC), while OpenBTS uses the Asterisk Voice over Internet Protocol (VoIP) [4] private branch exchange (PBX) to connect calls. For this reason, mobile endpoints are actually managed as SIP endpoints and switching feature can be distributed over multiple switches, providing transcoding to and from GSM voice codecs. The implementation in OpenBTS of the SIP core cellular network allows the total compatibility with the 3GPP IP Multimedia Core Network Subsystem (IMS), that represents the core network for 3G and 4G/LTE mobile data and telephony.

Concerning common tasks typically done in GSM by a mix of analogue and digital circuitry such as complex modulation, time division multiplex timing and many more, in OpenBTS all tasks are managed exploiting SDR capability, handling them in the digital domain and by software running on an ordinary processor. For all this reason, it appears clear that OpenBTS realizes a radio interface that is fully compatible with GSM devices, even if its architecture does not reflect the one used in the GSM standard.

On the contrary, OpenBSC is a project aiming at creating a GPL-licensed software implementations for all the relevant

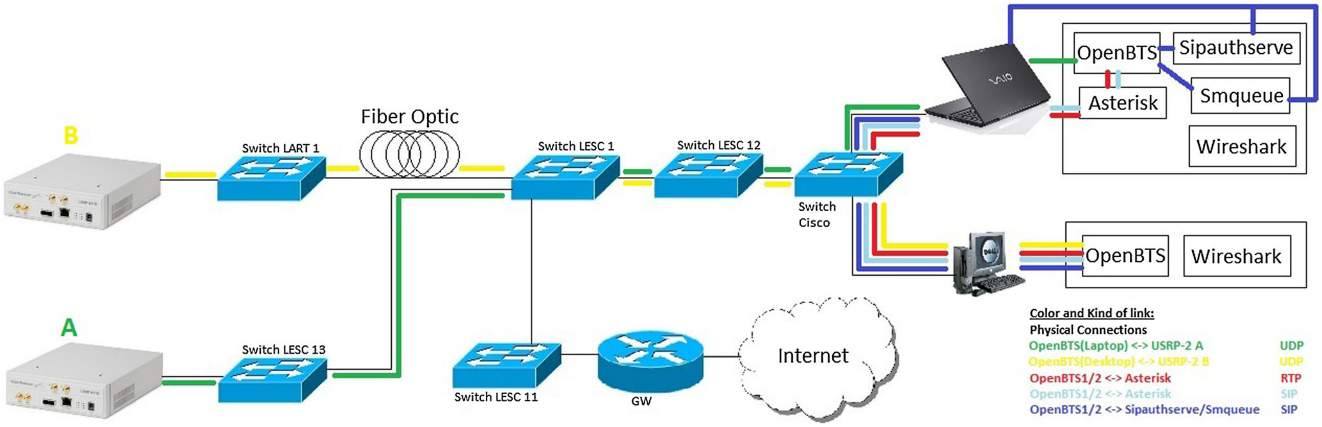
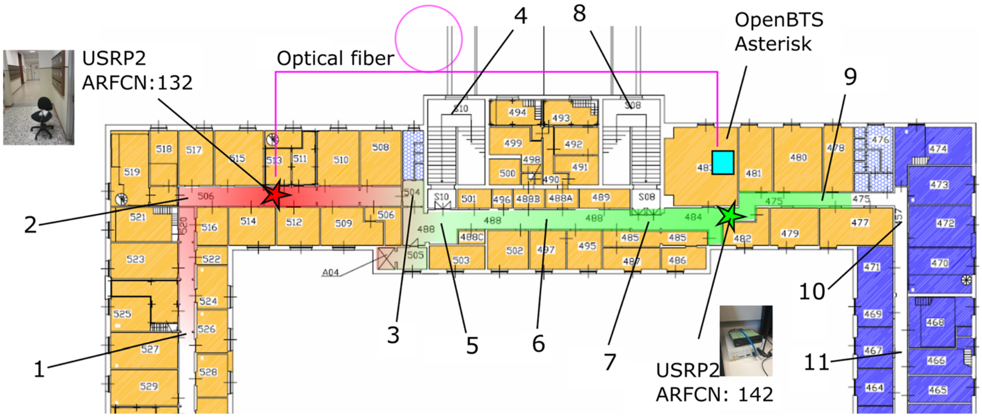


Figure 2 Detailed traffic paths.

Figure 3 Experiment deployment.



elements of a complete GSM/3GPP architecture. It realize the minimal necessary parts of a base station controller (BSC), in addition to additional network components such as MSC (Mobile Switching Center), HLR (Home Location Register), AuC (Authentication Center), VLR (Visitor Location Register), EIR (Equipment Identity Register). OpenBSC can be run on a commodity Linux PC and can be combined with off-the-shelf BTS hardware to provide network service. Used as BSC-only, OpenBSC operates as a conventional GSM BSC and it has to be necessarily located between a MSC and a BTS to exploit its GSM functionalities. However, OpenBSC can be also used in the NITB (Network In The Box) mode, working as BSC plus all the aforementioned additional network components. Looking at it from a functional point of view, OpenBSC in NITB mode roughly equals to an OpenBTS setup.

In addition to the aforementioned solutions, other software implementations of the GSM standard based on SDR technology are available. However, they are implemented for different aims, as is in the case of IMSI (International Mobile Subscriber Identity) catchers [6], that are largely used both for security and hacking purposes. They realize essentially a Man-In-The-Middle (MITM) attack, pretending to be false base stations acting between the target mobile phones and the real base stations of service providers. In this way, an IMSI catcher is able to not only steal the IMSI numbers, but also to intercept calls and messages of nearby phones, as well as track handsets, deliver geo-target spam [5], send reconfiguring messages and many other privacy-arming actions [6].

3 Experimental Setup

During an emergency caused by a natural disaster or socio-political event, regular communication infrastructures could be unavailable. In order to provide a reliable communication network able to connect the population with responders and authorities, a possible solution is the activation of a temporary radio network following widespread standards like 2G/3G cellular telephony. In the experiment an emergency situation has been simulated where a software 2G (GSM) emergency network has been deployed indoor, at the second floor of the Department of Information Engineering (DINFO) at the University of Florence.

The logical map of involved devices in the access segment is depicted in Fig. 1. It consists of two RF heads, one directly connected through a gigabit Ethernet link to a baseband CPU hosting OpenBTS [7], the other is remotely deployed and fed through an optical LX Gigabit Ethernet connection from a second baseband CPU unit. Both CPUs are then interconnected by a SIP PABX (Session Initiation Protocol based Private

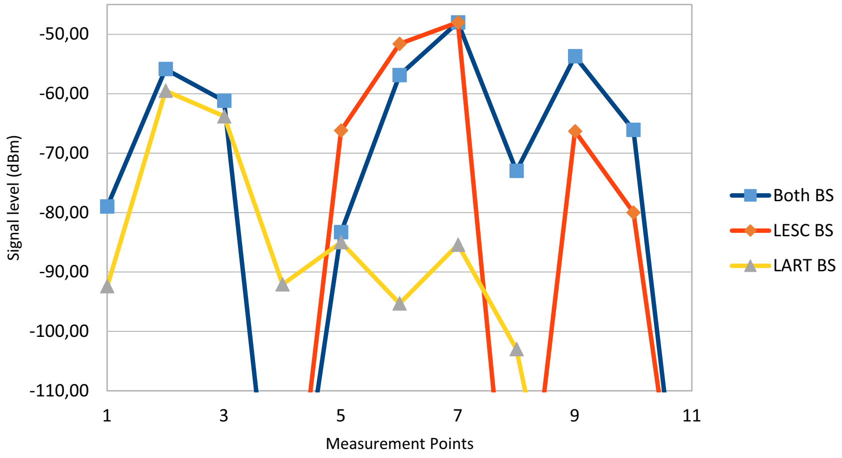
Table 1 Experiment parameters.

Parameters		
name	value	unit
Downlink Frequency BS1	870,0	MHz
Uplink Frequency BS1	825,0	MHz
Downlink Frequency BS2	872,0	MHz
Uplink Frequency BS2	827,0	MHz
Noise Figure	8,0	dB
Max RF power	200,0	mW

Table 2 Voice call network usage.

Measurements		
name	value	unit
GSM voice payload bitrate	13,0	kbps
RTP payload bitrate	13,2	Kbps
Mean RTP packet delay	20,0	ms
RTCP overhead (5 s)	0,41	%
Baseband IP traffic	13,0	Mbps

Figure 4 Measured received signal power (dBm) at different test points.



Automatic Branch Exchange), for call routing and user authentication.

The details of the flowing IP traffic in the experimental setup is shown in Fig. 2. Radio devices are implemented with two Ettus Research Universal Software Radio Peripheral-2 USRP2 [8] equipped with a RFX900 daughter boards. The RFX900 is a high-performance transceiver designed specifically for operation in the 900 MHz band.

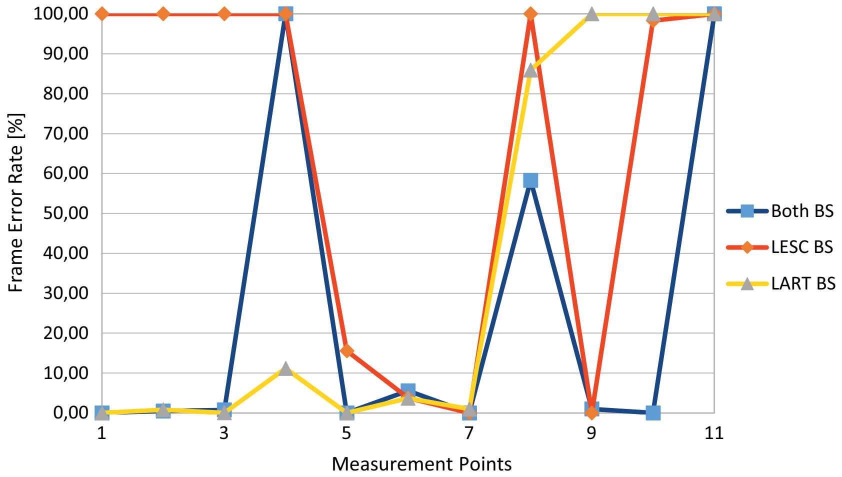
The two baseband CPUs consists of a Sony VAIO (Intel I5@2.5GHz, 4 cores), namely CPU1 and Dell (P4@3GHz), called CPU2. The first CPU is hosting one OpenBTS module, the Asterisk PABX [4] and the SIP authorization module. The second one is hosting the remote OpenBTS module. Figure 2 also reports the main traffic components colored depending on the link role during the radio access operation after a connection with a mobile has been established. The deployment map is shown in Fig. 3. The stars represent the location of the two RF devices corresponding to the two GSM base stations. Numbers (1–11) indicate the location of mobiles where the measurements have been acquired.

4 Field Trials and Results

The experiment consists in providing voice and SMS service to up to 2 real GSM mobiles in the area of coverage of the two emergency cells. The main adopted parameters are represented in Table 1.

Several voice call and text message tests has been conducted with mobiles located in various positions of the coverage area. For each setup, the exchanged IP traffic among the network functional entities has been captured and analyzed with Wireshark. The voice latency has been also measured through the analysis of the audio echoes of a sequence of audible

Figure 5 Uplink Frame Error Rate with mobiles placed at different test-points.



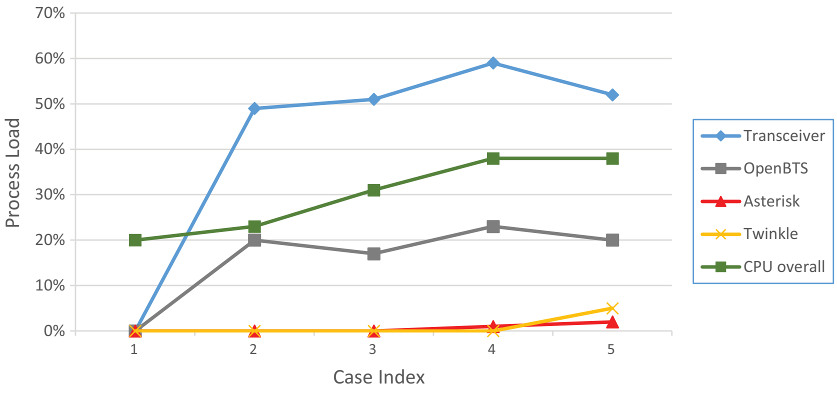


Figure 6 Process load for the various modules in the baseband processing host (CPU1, 1=idle, 2–5 during a call).

"ping" transmitted from a modified software phone to the mobiles.

4.1 Aggregated Network Results

The required network resources for completing a voice call with the experimental setup is reported in Table 2. for a single mobile and considering the outbound traffic only (from mobile to BS).

4.2 Received Signal and Frame Errors for Various Test Points

For various mobile locations, a series of measurements have been conducted. In Fig. 4, the received signal power for the downlink in various locations of the terminal along the corridor and stairs is reported. This figure has been obtained combining the measurements of the received signal power for three different conditions. The first one is represented by the exclusive transmission of the BS1 (BS2 is turned off) and it is illustrated by the red line in the figure, showing the dependency between the measurement points and the received power. On the contrary, the yellow line is related to the second condition, when only the BS2 is transmitting. Finally, the blue line is the measured power when both BSs are transmitting. The measured received signal strength follows the expected behavior, decreasing as receiver distances the transmitter and being severely reduced down the stairs.

In Fig. 5 the frame errors for uplink transmission during a call are reported for the same measurement points considered in Fig. 4. As for the previous figure, the red trace refers to the case of the transmission of the BS1 only, while the yellow one to the exclusive transmission of the BS2 and the blue one to the presence of both the BS. As might have been expected, figure lines show that if a mobile is within the coverage of a BS, the related frame errors are low. Moreover, red line also shows a signal saturation issue caused by an unfavorable location of mobile with respect to the BS1 (test point 11).

During this test no automatic handover procedure has been activated, nevertheless the identification of the feasible roaming points has been exploited. For a mobile moving along the corridor from BS1 to BS2, location 3 represents

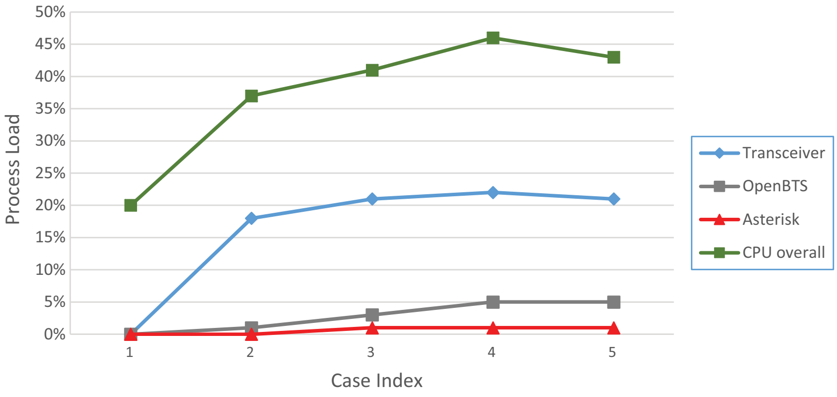


Figure 7 Process load in the baseband secondary processing host (CPU2, 1=idle, 2–5 during a call).

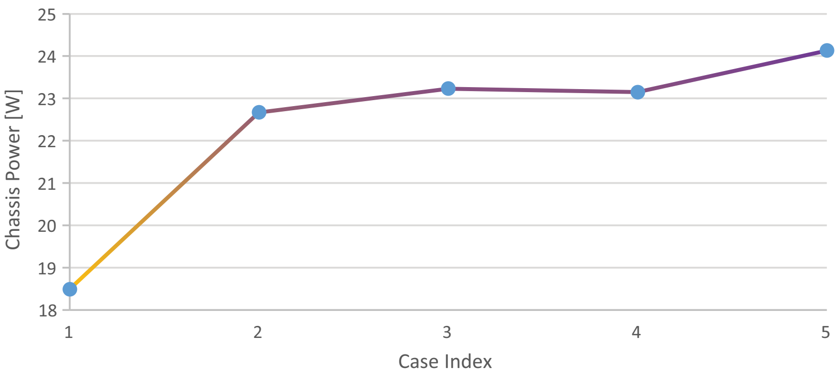


Figure 8 Measured power consumption for CPU1 (1=idle, 2–5 during a call).

the handover point for roaming from BS1 to BS2. On the contrary, for a mobile moving backward, the roaming point from BS2 to BS1 is located at position 5, referring to Fig. 3.

4.3 Computing and Energy Resources Usage

An evaluation of computing complexity for the software realization of GSM radio access is reported in Figs. 6 and 7 for both the CPUs. The y-axis reports the CPU load fraction for various modules of OpenBTS and Asterisk (single BS). The x-axis iterates the measurements in different conditions: case index 1 refers to idle operating system with no OpenBTS modules running, cases 2 to 5 refer to CPU load sampling during calls generated from different locations. CPU load takes into account the default CPU services. As expected the baseband processing (Transceiver) is the process with the highest load to serve.

Load differences are related to the different positions of the mobile terminal during the call, that may cause an elevate number of retransmissions in case of bad propagation conditions. In Fig. 8 the averaged power consumption is reported for CPU1 considering the same five test cases. Averaged power consumption trend of CPU2 is similar to CPU1 and not reported for the sake of simplicity.

Table 3 Audio RTT.

Measurements		
name	value	unit
Twinkle mean RTT time	274,4	ms
Twinkle RTT standard deviation	64,5	ms
“Bumps” mean RTT time	172,2	ms
“Bumps” RTT st. deviation	6,5	ms
GSM mean RTT time	278,3	ms
GSM RTT standard deviation	1,6	ms

4.4 Audio Latency

Audio perceived delay through the experimental system has been evaluated by injecting both artificial and natural sounds and capturing the received echo produced by the analogic coupling of speakers and microphone in the mobile phone. The sounds adopted are of three kind: synthetic sounds injected by Twinkle SIP softphone, short analogic “bumps” generated on microphones and a portion of a speech during a call. By autocorrelation analysis an estimated of round-trip latency is reported in Table 3.

Estimated one-way latency can be obtained by halving the measured RTT, resulting in values aligned with conventional digital telephony.

5 Concluding Remarks

The described field trial successfully confirmed the feasibility of software virtualization of baseband signal processing with ordinary CPUs. Software implementations of 2G/3G radio stack, along with compact and powerful SDR hardware makes it possible for the availability of deployable emergency communication services. The involved network resources in the experimented context are small (less than 15Mbps) and does not require complex devices to operate. The remote RF head has been connected with a small portion of the optical link, so that over 60 GSM base stations can share a single Gigabit optical link. Computing resources and power consumption stay within the capability of conventional laptop/desktop. With dedicated computing hardware a more computational efficiency can be achieved. The experiment considered 2G cellular technology because of the limited bandwidth and complexity of the standard. The same experimented concepts however apply to 3G and later generations with more computing and transport resources available.

Acknowledgments The authors thank Rodrigo Isidro Lopez for his support in the execution of the reported experiment, the director of the Department of Information Engineering (DINFO) of University of Florence for the availability of the experiment area.

References

1. (2012). Software defined networking: The new norm for networks, White Paper, Open Networking Foundation.
2. CMCC (2011) C-RAN the road towards green RAN, CMCC white paper.
3. Arslan, H. (Ed.). (2007). *Cognitive radio, software defined radio, and adaptive wireless systems* (Vol. 10). Berlin: Springer.
4. Qadeer, M.A., & Imran, A. (2008) Asterisk Voice Exchange: An Alternative to Conventional EPBX, Computer and Electrical Engineering, 2008. ICCEE 2008. International Conference on, 20–22 Dec. 2008.
5. Muncaster, P. (2014). Chinese cops cuff 1,500 in fake base station spam raid. The Register, 26 Mar 2014. http://www.theregister.co.uk/2014/03/26/spam_text_china_clampdown_police/.
6. Dabrowski, A., Pianta, N., Klepp, T., Mulazzani, M., & Weippl, E. (2014). IMSI-catch me if you can: IMSI-catcher-catchers. In Proceedings of the 30th annual computer security applications Conference (pp. 246–255). ACM.
7. Pace, P., Loscri, V. (2012) OpenBTS: a step forward in the cognitive direction. 2012 21st International Conference on Computer Communications and Networks (ICCCN), vol., no., pp.1,6.
8. Ettus Research ltd, http://home.ettus.com/Acknowledgements.

Luca Simone Ronga [IEEE S89-M94-SM04] received his M.S. degree in electronic engineering in 1994 and his Ph.D. degree in telecommunications in 1998 from the University of Florence, Italy. In 1997 joined the International Computer Science Institute of Berkeley, California, as a visiting scientist. In 1998 obtained a post-doc position in the engineering faculty of the University of Florence. In 1999 he joined Italian National Consortium for Telecommunications, where he is currently head of research. He conducts research activity and project management in various telecommunications areas, mainly in the satellite and terrestrial wireless fields. He has been leader of national and international research groups. He authored over 50 papers published in international journals and conference proceedings. He has been editor of EURASIP Newsletter for 4 years. His interests range from satellite communications to Software Defined Radio and Cognitive Radio techniques.

Renato Pucci received the M.S. degree in Telecommunication Engineering in 2008, winning with his thesis three international awards, confirming the high quality of the work performed. In 2012 Renato completes his Ph.D. sponsored by Thales Alenia Space S.p.A. at University of Florence discussing his dissertation titled "Advanced technique based on game theory for resource allocation in cognitive radio networks". During his Ph.D. carrier, Renato focused his research activity on advanced and cognitive radio networks, applications of game theory, large data management and several other different topics in the area of telecommunications. He has been the leader of research activity in national research projects, COST and EDA (European Defence Agency) projects on heterogeneous terrestrial and cognitive communication systems. He is a member of NATO task force IST-077 RTG-035 and IST-104 RTG-050 devoted to coordination of Cognitive Radio research activities among coalition partners.

Enrico Del Re was born in Florence, Italy. He received the Dr. Ing. degree in electronics engineering from the University of Pisa, Pisa, Italy, in 1971. Since 1975 he has been with the Department of Electronics Engineering of the University of Florence, Florence, Italy, first as a Research Assistant, then as an Associate Professor, and since 1986 as Professor. During the academic year 1987–1988 he was on leave from the University of Florence for a 9-month period of research at the European Space Research and Technology Centre of the European Space Agency, The Netherlands. His main research interest are digital signal processing, mobile and satellite communications, on which he has published more than 300 papers, in international journals and conferences. He is author and co-editor several academic books and chairman of many workshop. He received the 1988/89 premium from the IEE (UK) for the paper "Multicarrier demodulator for digital satellite communication systems". He is the head of the Signal Processing and Communications Laboratory of the Department of Information Engineering (DINFO) of the University of Florence. Presently he is President of the Italian Interuniversity Consortium for Telecommunications (CNIT), having served before as Director. Presently he is the Director of the Department of Information Engineering (DINFO) of the University of Florence, Italy. Professor Del Re is a Senior Life Member of the IEEE and a member of the European Association for Signal Processing (EURASIP).