Software Defined Radio (SDR)

INTRODUCTION
Outline of the course

- Advantages and usefulness with respect to traditional radio systems
- Architectures
- RF section and D/A conversion
- Filtering, decimation and interpolation algorithms
- Baseband processing, modulation-demodulation
- Wideband waveforms: OFDM
- From SDR to Cognitive Radio (architectures)
- Spectrum sensing
- Examples
- Radio description language – short overview
Brief history of radio systems

- 1860s - J.C. Maxwell predicted the existence of radio waves
- 1866 - H.R. Hertz demonstrated radio wave propagation in lab conditions
- 1866 – Mahlon Loomis demonstrated „wireless telegraphy”
- Around 1892 Tesla created a basic design for radio
- 1895 – Marconi sent and received his first radio signal
  - 1899 – he successfully sent the first wireless signal over La Manche
Brief history of radio systems (2)

- 1901 – US Navy adopts the wireless system as the communication method, replacing visual signalling and homing pigeons
- early 1900s – Lee Deforest develops the detector of EM radiation, allowing for the possibility to amplify the RF signal picked up by the antenna before application to the receiver detector
  - He is also the first person to use the term “radio”
- Sometimes between 1892 and 1906 (debatable) – the first time human voice was transmitted by radio
- 1906 – R.A. Fessenden deploys the system using AM
  - In 1912 he constructs the first superheterodyne circuit
- 1915 – speech first broadcasted over Atlantic
- 1927 – commercial radiotelephony linking North America with Europe was opened
- 1933 – E.H. Armstrong invented FM radio
- 1947 – Bell Labs invented the transistor
- 1954 – introduction of transistor radio by Sony Labs
- 1965 – first Master FM system deployed at the top of the Empire State Building
Brief history of radio systems (3)
Brief history of radio systems (4)

- 1948 - Claude Shannon publishes two benchmark papers on Information Theory, containing the basis for data compression (source encoding) and error detection and correction (channel encoding)
- Late 1950s - several ‘push-to-talk’ mobile systems established in big cities for CB-radio, taxis, police, etc.
- Early 1960s - Improved Mobile Telephone System (IMTS) developed with simultaneous transmit and receive, more channels, and greater power
- 1962 - The first communication satellite, Telstar, launched into orbit
- 1968 - Defense Advanced Research Projects Agency – US (DARPA) selected BBN to develop the Advanced Research Projects Agency Network (ARPANET), the father of the modern Internet
- 1977 - The Advanced Mobile Phone System (AMPS), invented by Bell Labs, first installed in the US with geographic regions divided into ‘cells’
- 1983 - January 1, TCP/IP selected as the official protocol for the ARPANET, leading to rapid growth
- 1994 - FCC licenses the Personal Communication Services (PCS) spectrum (1.7 to 2.3 GHz) for $7.7 billion
- Late 1990s - Virtual Private Networks (VPNs) based on the Layer 2 Tunneling Protocol (L2TP) and IPSEC security techniques become available
- 2000 - 802.11(b)-based networks are in popular demand
Motivation for digitalization

Advantages of digital systems are multiple:

- Digital signals are more tolerant to noise
- Less spectrum-demanding => possible to use more channels using less bandwidth => cost-effectiveness
- Possibility of using error detection and error correction techniques
- Flexibility in configuring – possible to use microprocessors, digital switching elements and layer scale
- Simpler circuitry
"Radio in which some or all of the physical layer functions are software defined"
- Wireless Innovation Forum

“A radio that includes a transmitter in which the operating parameters of frequency range, modulation type or maximum output power (either radiated or conducted), or the circumstances under which the transmitter operates can be altered by making a change in software without making any changes to hardware components that affect the radio frequency emissions.”
- Derived from the US FCC's Cognitive Radio Report and Order, adopted March 10, 2005

However, no unanimous definition of Software defined radio (technology never has nor will be standardized)
  ❑ The level of reconfigurability/reprogrammability for the radio to be considered as a software defined one is ambiguous
SDR – advantages

- Traditional hardware based radio devices limit cross-functionality and can only be modified through physical intervention
  - higher production costs and minimal flexibility in supporting multiple waveform standards
- SDR provides an efficient and comparatively inexpensive solution to this problem, allowing multi-mode, multi-band and/or multi-functional wireless devices that can be enhanced using software upgrades
  - The equipment is more versatile and cost-effective, increasing the hardware lifetime
  - Also, it can be upgraded with new software for new waveforms and new applications after sale, delivery, and installation
  - Thus, SDRs provide software control of a variety of modulation techniques, wideband and narrowband operation, transmission security (TRANSEC) functions (such as hopping), and waveform requirements
SDR – advantages (2)

- For manufacturers:
  - the development of SDR brings the possibility to concentrate R&D efforts on a reduced hardware platform set, applicable to every cellular system and market (not only on a national or regional basis)
    - mass production would allow for lowered costs
  - possibility to improve the software in successive steps, and the correction of software errors and bugs discovered during operation

- For network operators:
  - Ability to rapidly roll out new services tailored to the needs of each user and differentiated from those of other operators

- For end users:
  - Possibility to roam their communications to other cellular systems and take advantage of the worldwide mobility and coverage
  - Also, each user can configure their terminals according to their preferences
SDR – drawbacks

- Power consumption (for now)
- Initial development and deployment costs
- New security issues
- Software reliability issues
- Difficulty of writing software for various target systems
- Maximum interoperability only between SDR systems (e.g. both base systems and end-use terminals)
History and development of SDR

- Software defined radio is a term originally coined by Joseph Mitola (often referred to as “a grandfather of SDR”) back in 1991, while describing the possibilities of reconfigurability and reprogrammability of radio systems.

- The main motivation behind developing SDR was creating a technology that would be able to operate in the frequency band from 2 MHz to 2 GHz (so-called “Two-to-two band”).
  - Goal: achieving compatibility with all the other military radios used by American military – there were more than ten of those at that time.
  - 1987: Air Force Rome Labs’ ICNIA multiple-radio design, arguably be the predecessor of the technology.
  - 1992 – 1995: SPEAKeasy project - its architecture represents a paradigm for a basic structure of today’s SDRs.
    - A rather massive, hardly-portable equipment based on a programmable cryptography chip, allowing for communication over a range of different frequencies, cryptography techniques, modulation techniques, encoding methods and other parameters.
    - SPEAKeasy II solves the portability issues (more acceptable dimensions).
      - Also introduced the possibility of using programmable vocoder as well as a variety of ASP and DSP circuitry for handling different waveforms.
History and development of SDR (2)

- In terms of software programmability and reconfigurability, current state-of-the-art SDR technology is JTRS – a family of tactical software that uses the common SCA architecture
  - JTRS radios serve as a plug-and-play devices capable of working in 2 Mz – 2 GHz band, and should in foreseeable future replace all the existing US military radio technologies operating in that band
  - Digital Modular Radio (DMR) is a full SDR used by US Navy as a part of the Joint Maritime Communications System project
    - At the moment, it is interoperable with military systems such as SINCGARS and HaveQuick, however interoperability with JTRS is yet to be implemented (but should be possible in the future)
Evolution of software radio systems

- Historically, radios have been fixed-point designs
  - In order to increase capability, reduce life cycle costs, etc., software was added to the system design

- Software-capable radios
  - fixed modulation capabilities, relatively small number of frequencies, limited data and data rate capabilities, ability to handle data under software control

- Software-programmable radios
  - ability to add new functionality through software changes, advanced networking capability

Fig.: SDR technology continuum (Fette, [1])
Evolution of software radio systems (2)

- **Software defined radios**
  - full reconfigurability of air interfaces in software, including channel access and waveform synthesis

- **Aware radios**
  - environmental information is gathered using sensors implemented in both audio (microphone) and RF (receiver) frequencies

- **Adaptive radios**
  - Able to monitor its performance and autonomously modify its operating parameters (Frequency, instantaneous bandwidth, modulation scheme, error-correction coding, channel mitigation strategies, system timing, transmit power, etc.)

- **Cognitive radios**
  - radio in which communication systems are aware of their internal state and environment, such as location and utilization on RF frequency spectrum at that location
  - they can make decisions about their radio operating behavior by mapping that information against predefined objectives
  - Cognitive radios capable of machine learning are sometimes referred to as „intelligent radios”
## Evolution of software radio systems

(3)

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Frequency hopping</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Automatic link establishment (i.e., channel selection)</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Programmable crypto</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Networking capabilities</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Multiple waveform interoperability</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>In-the-field upgradable</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Full SW control of all signal-processing, crypto, and networking functionality</td>
<td>X</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td></td>
<td></td>
</tr>
<tr>
<td>QoS measuring/channel state information gathering</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Modification of radio parameters as function of sensor inputs</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Learning about environment</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Optimizing with different settings</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

* The industry standards organizations are in the process of determining the details of what properties should be expected of aware, adaptive, and cognitive radios.
Wireless data standards – a brief overview

- IEEE 802.11 – a group of IEEE norms that deals with network technologies, as follows:
  - IEEE 802.11 WLAN (Wireless Local Area Network)
  - IEEE 802.15 WPAN (Wireless Personal Area Network)
  - IEEE 802.16 WMAN (Wireless Metropolitan Area Network)
  - IEEE 802.18 RR TAG (Radio Regulatory Technical Advisory Group)
  - IEEE 802.20 MBWA (Mobile Broadband Wireless Access)
  - IEEE 802.21 Media Independent Handoff Working Group
  - IEEE 802.22 WRAN (Wireless Regional Area Network)

- IEEE 802.11 WLAN
  - 802.11 FHSS (Frequency Hopping Spread Spectrum)
    - 2.4 GHz band; GFSK (2-GFSK; 4-GFSK); up to 2Mbps
  - 802.11 DSSS (Direct Sequence Spread Spectrum)
    - 2.4 GHz band; DBPSK and DQPSK; up to 2 Mbps
  - 802.11b – uses CCK (Complementary Code Keying)
    - CCK is based on DSSS; allows data rate up to 11 Mbps
Wireless data standards – a brief overview (2)

- IEEE 802.11 WLAN (ctd.)
  - 802.11n – 2.4 GHz and 5 GHz band
    - Up to 600 Mbps; usage of MIMO up to 4x4; modulation up to 64-QAM
  - 802.11ac – 5 GHz band
    - >500 Mbps; usage of 8x8 MIMO; 256-QAM modulation

- BRAN (Broadband Radio Access Networks) – working group within ETSI (European Telecommunication Standards Institute), with norms:
  - HiperLAN2 (High Performance Radio Local Area Network)
  - HiperAccess
  - HiperMAN (High Performance Radio Metropolitan Area Network)
  - HiperLINK

- HiperLAN2
  - On PHY layer almost equal to 802.11a (OFDM; data rate up to 54 Mbps)
  - DFS – Dynamic Frequency Selection
Wireless data standards – a brief overview (3)

- **WiMax**
  - Most represented technology within 802.16 standard; includes everything covered by 802.16-2004 and 802.16e
  - Operability in 3.4 GHz (main) and 24.5 GHz bands
  - Uses OFDM and OFDMA
  - Modulation techniques: BPSK, QPSK, 16QAM, 64QAM
  - 802.16m – 4x4 MIMO, SOFDMA up to 365 Mbps (theoretical)

- **LTE and LTE-Advanced (3GPP)**
  - OFDM in Downlink; DFTS-OFDM in Uplink
  - MIMO application
  - Variable BW: 1.4, 3, 5, 10, 15 and 20 MHz
  - Modulation techniques: QPSK, 16QAM, 64QAM
  - Up to 1 Gbps download; 500 Mbps upload (theoretical)

- **HSPA+ (3GPP)**
  - CDMA
  - MIMO
  - Modulation techniques: 16QAM, 64QAM
  - Up to 672 Mbps download (theoretical)
OFDM radio interface

- OFDM symbol consists of a large no. of modulated subcarriers, each of whom are results of DFT (Discrete Fourier Transform)
  - WiMAX uses 256 subcarriers
  - Subcarriers can be of type:
    - Data (192 subcarriers)
    - Pilot (8) – always modulated using pre-known codes with BPSK modulation scheme
    - Supressed – role: securing the band towards the neighboring channel on the frequency axis

Fig.: Subcarriers spectrum overlapping
OFDM radio interface (2)

- OFDM is one of the most used transmission techniques thanks to its benefits:
  - High data rate in severe multipath channel
  - Less sensitive to multipath with respect to single carrier mod
  - Less complex equalization with respect to single carrier mod
  - Easy implementation thanks to IFFT
  - Digital implementation

Fig.: Example of an OFDM modulator
A history of dynamic RF spectrum sharing

- Dynamic sharing refers to spectrum access systems that maintain the spectrum resource in a pool and permit users to access it on a demand basis
  - It is the main utility of the currently studied Cognitive Radios
- Traditional Maritime Radio
  - From the very beginning of wireless, maritime radio has used shared channels
  - For example:
    - 2,182 KHz is used today as a calling as well as an emergency signaling frequency (ships keep watch of this frequency) and other frequencies are used as working frequencies
    - If Ship A wishes to communicate with Ship B, Ship A identifies a working frequency and then places a call to Ship B on the calling frequency (2,182 KHz)
    - Communications on the calling frequency serve to alert Ship B that Ship A is calling and to tell Ship B which working channel is to be used
  - Such channel sharing was necessary and effective because there were not sufficient channels to give each ship a separate channel and the typical ship required far less than a full channel of capacity
A history of dynamic RF spectrum sharing (2)

- **Traditional Land Mobile Radio**
  - FCC has long authorized the use of shared channels in land mobile
  - Example (from 1960s):
    - A single channel covering a city is being used by both a plumbing company and a pizza delivery company
    - Neither firm has sufficient demand to justify an entire channel
    - Simple protocols (listen before talking) and short messages allowed for reasonably efficient sharing using the FM

- **Citizen’s Band Radio**
  - Radio service at 27 MHz, extremely popular in early 1970s
  - There are 40 shared CB channels used on a "take-turns" basis. There are no channels authorized in the CB Radio Service above 27.405 MHz or below 26.965 MHz
  - Users must never talk with another station for more than 5 minutes continuously and then must wait at least one minute before starting another communication
In the mid-1970s, in order to expand land mobile service, the FCC permitted land mobile operation on some of the lower UHF channels in several large cities.

Britain’s CT2
- In the mid-1980s, British industry and government developed a new standard for digital cordless phones: Cordless Telephone, 2nd generation (CT2)
- A pool of 40 channels is used - to establish a call, the equipment automatically identifies a vacant channel or the channel with the least interference and begins operation on that channel
- Never „caught on” in the UK, but was popular in Hong Kong and Singapore

FCC’s Part 15
- Adopted in 1985, Part 15 covers the use of low-powered devices such as garage door openers, as well as higher power digital devices operating in the ISM bands (up to 1 W)
- Permits the use of any digital modulation provided that the resulting signal has a sufficiently wide spectrum and does not contain strong spectral lines
A history of dynamic RF spectrum sharing (4)

- **Air-Ground Telephone Service**
  - In the 800 MHz Air-Ground Telephone Service each licensee is given exclusive access to a dedicated control channel (for setting up calls) and shared access to a pool of working channels (for carrying conversations).
  - Although initially fairly popular, there was no easy way to upgrade to improved technologies, hence the popularity dwindled.

- A number of SS proposals (1991 Jackson’s proposal; early 90’s Big LEOS; 1994 Gilder’s proposal; 1995 Apple Computer’s NII Band; 1995 Noam’s proposal)

- Today’s focus: opportunistic spectrum sharing in Cognitive Radio Networks
References