GE Transportation

Signal Fingerprinting in Cognitive Wireless Networks

Simone Soderi

CWC Oulu
CENTRE FOR WIRELESS COMMUNICATIONS
University of Oulu

Project co-funded by the Tuscany Region and European Community under the 2007-2013 POR CREO FESR program.

imagination at work

Agenda

- Context
- Motivation
- Security
- Scenario
- TX/RX Models
- I/Q Demodulation
- ARFF via I/Q
- Results
- Conclusions

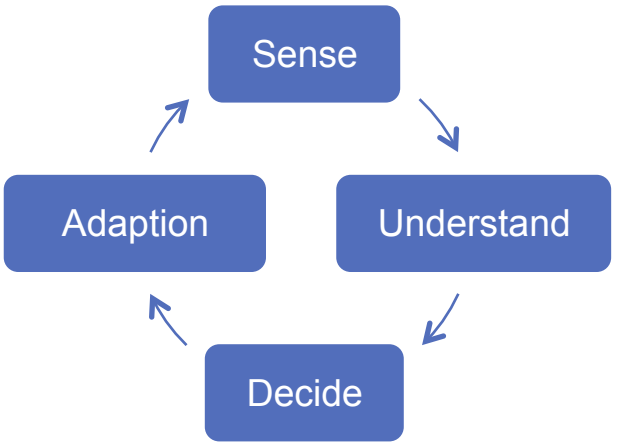
Context

Cognitive Radio

Air Interfaces:

- ✧ Multi-modality:
  - Different chip solutions;
- ✧ Flexible:
  - SDR.

Cognitive Network Loop



Benefits of CR

- ✧ Spectral efficiency improved;
- ✧ Energy saving;
- ✧ Flexibility.

Security

Electronic Attack: Jamming.

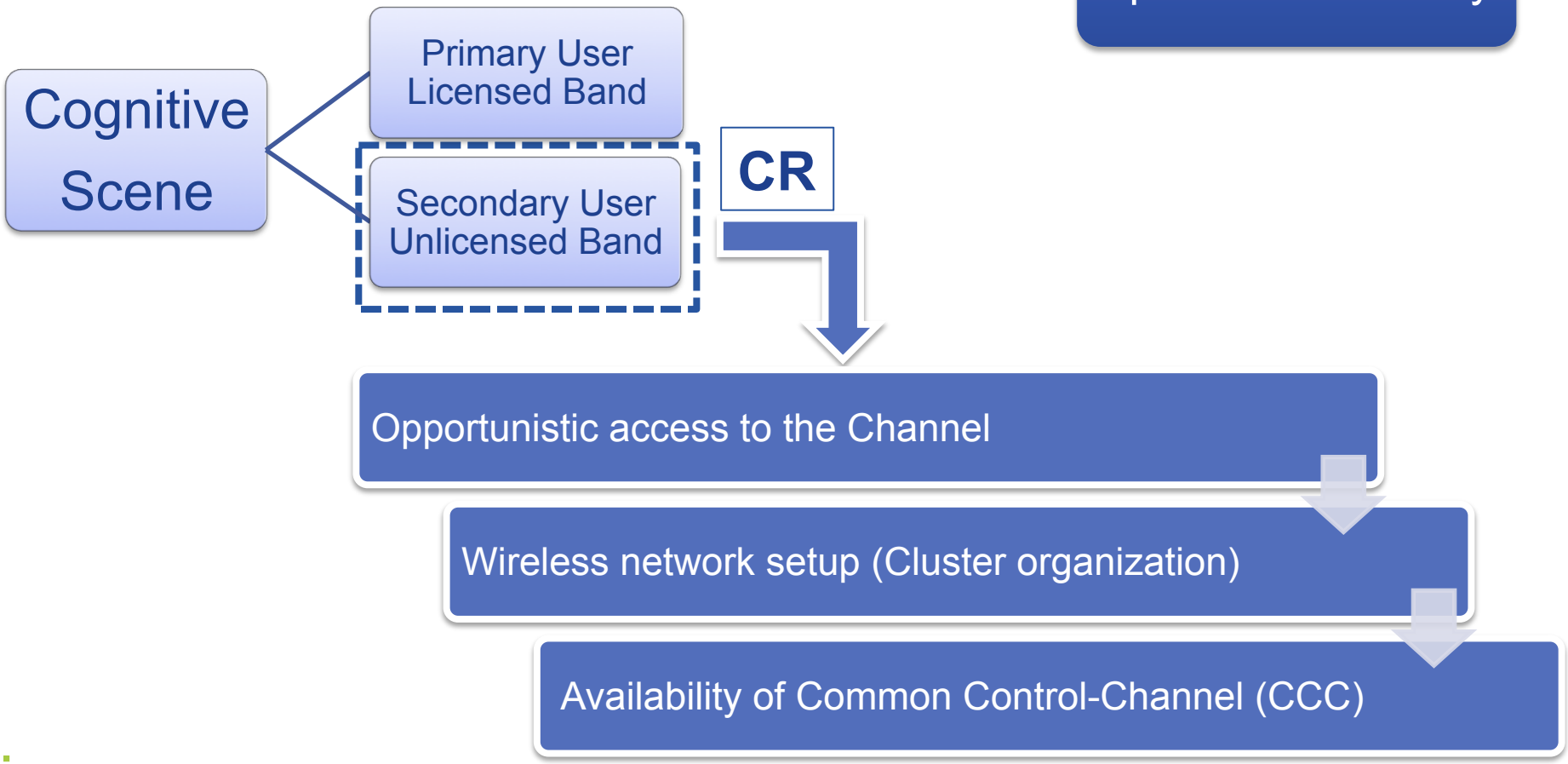
Hacking CR:

- ✧ DoS;
- ✧ New generation of attacks.

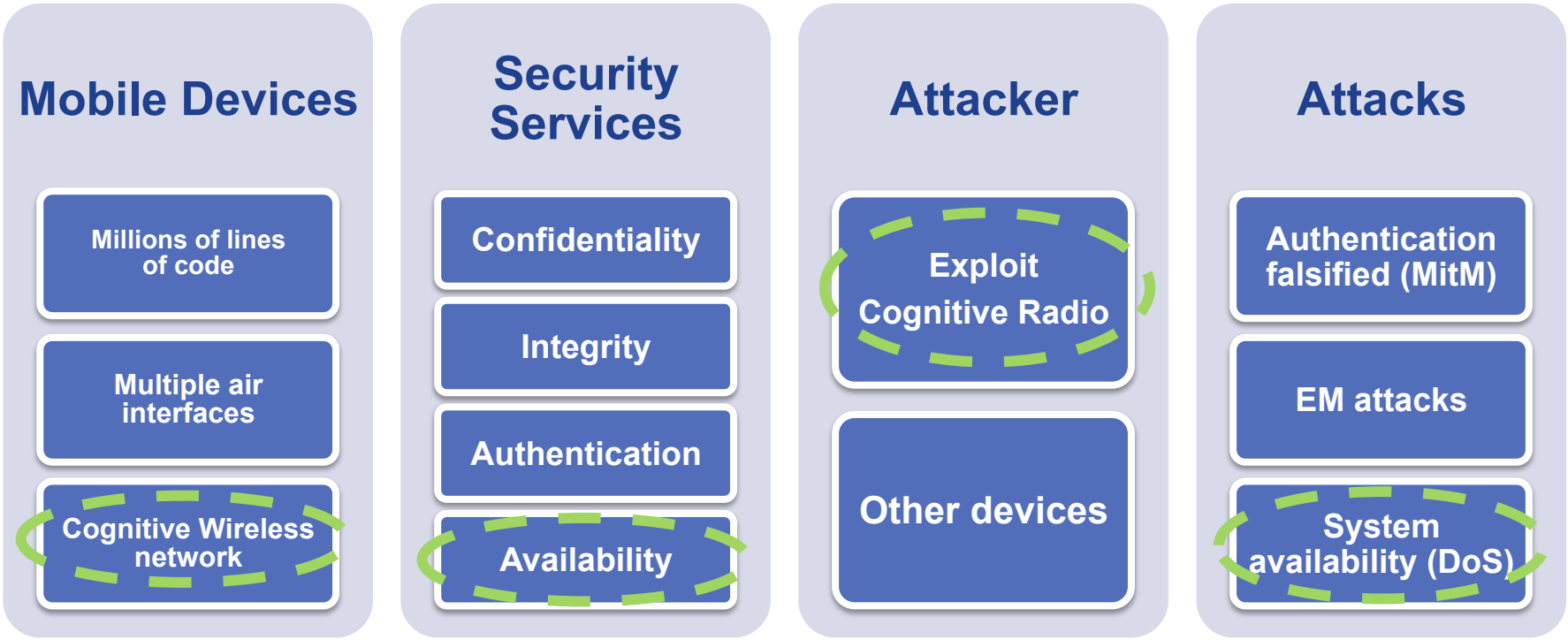
Motivation: Radio Spectrum

① Archaic pre-allocation scheme
② Dynamic allocation

Cognitive Radio for Spectrum Flexibility

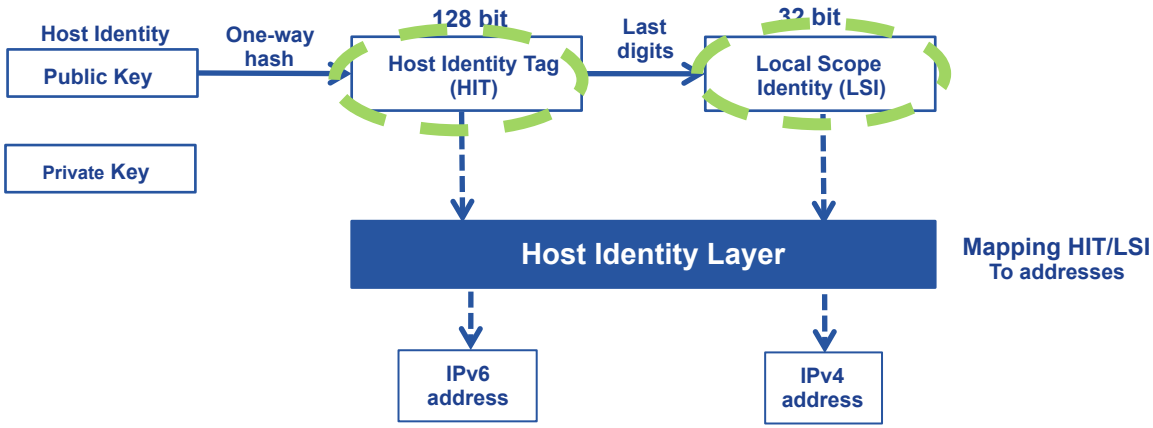


Motivation: Security



Active RFF proposal

Security: Active RFF application*



Host Identity Protocol (HIP):

- Separation between identification and localization;
- HIT/LSI introduction
- Host Identity Layer in TCP/IP
- Against DoS/MitM

HIP operation:

1. BEX:
   - 4-way handshake;
   - HIT Exchange;
   - Establish SA.
2. IPSec-ESP to secure communication

Active RF Fingerprinting (ARFF)

✓ Intentionally introduces EMS encoding such as a watermark at PHY

[*] S. Soderi, H. Viittala, J. Saloranta, A. Mancini, M. Hamalainen, and J. Iinatti, "Emulation of secure wi-fi communication: A performance gap analysis against a virtual test-bed," in *2013 13th International Conference on ITS Telecommunications (ITST)*, 2013, pp. 226–231.

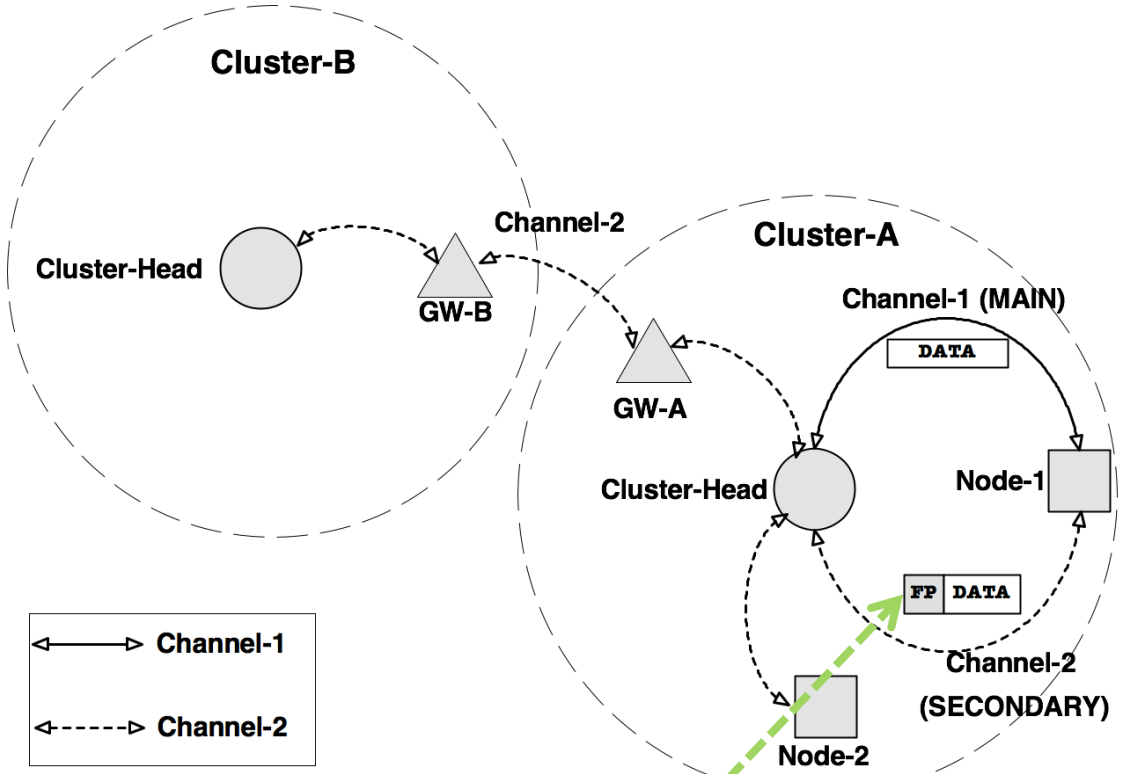
Scenario

CogMesh :

- Multi-channel/Multi-access network
- Channels → discover neighbors

Hypothesis:

- 2 Channels active and used:
  - MAIN
  - SECONDARY
- Without any dedicated CCC or not available.

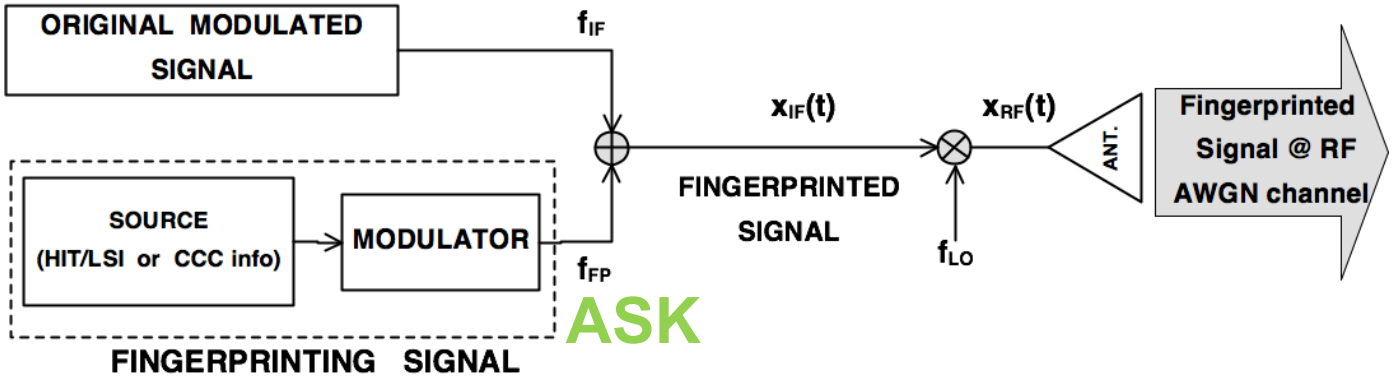


Proposed Method:

- CRs **sense** environment → Detect SECONDARY comm.;
- CRs **adapt** internal parameter to exploit Channel-2;
- **ARFF** used on Channel-2 to:
  - Encapsulating CCC information;

  Or
  - Exchanging HIT/LSI tags (HIP application)

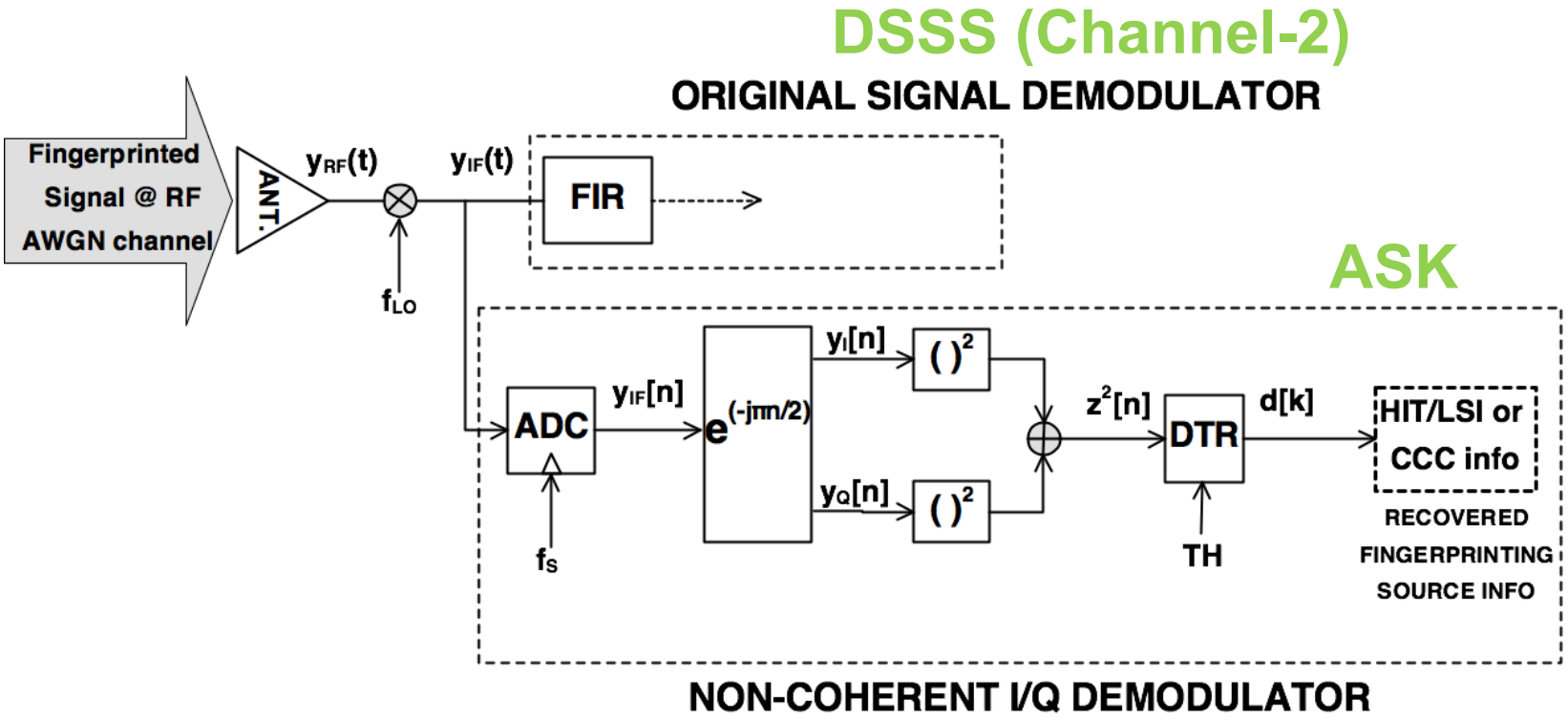
TX model: DSSS (Channel-2)



Parameter	Parameter	Value
ADC	Sampling rate (f_s)	25.6 MHz
DSSS	Carrier Frequency (f_{IF})	19.2 MHz
	Energy of signal waveform	0 dB
	Bit-Rate (R_b)	100 kbps
	Processing Gain (M)	128
	Chip-Rate (R_c)	12.8 MHz
	Number of bits (N)	32
	Modulation	QPSK
ASK	Carrier Frequency (f_{FP})	19.2 MHz
	Energy of signal waveform	[15 ÷ 20] dB
	Number of bits	32
	Bit-Rate ($R_{b\text{-}ASK}$)	320 kbps
Other	SNR	[0 ÷ 12] dB
	Channel	AWGN
	FP information	32 bits

- Simulation Parameters:
  - DSSS → f_{IF};
  - ASK → f_{FP};
  - CRs adapt parameters of FP sensing existing comm.;
  - Fingerprinting DSSS with ASK.

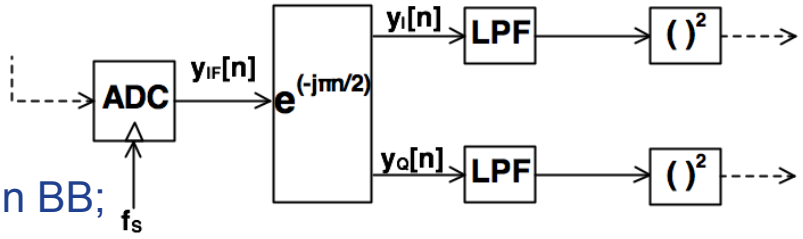
RX model



- RX characteristics:

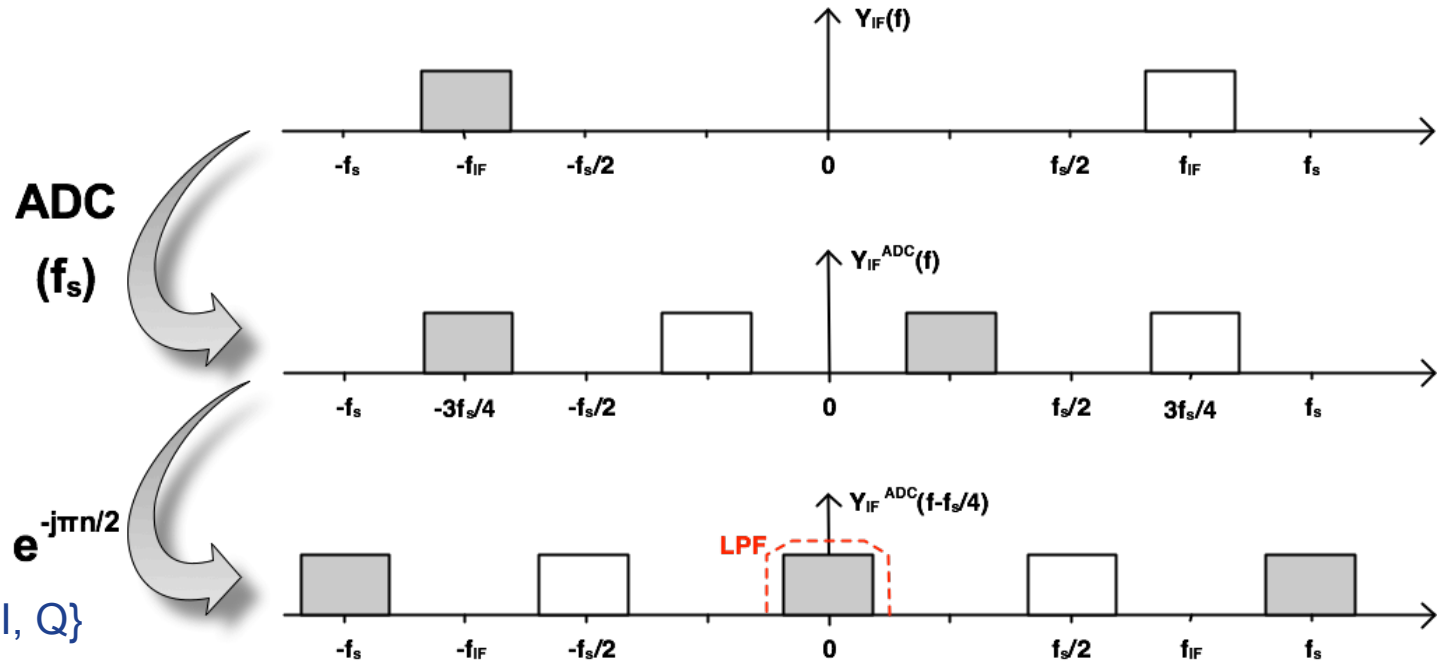
  - Digital I/Q demodulator;
  - High speed ADCs → direct down-conversion;
  - Reduced number of inputs to digital signal processing device

Digital IQ Demodulation*



- Idea of IF sampling → understand IF signal → replica in BB;
- No additional down-conversion;
- Relationships for f_{IF} and f_s

$$\begin{cases} f_{FP} = f_{IF} = k f_s \pm \dfrac{f_s}{4}, & \forall k \in \mathbb{Z} \mid k \geq 1, \\ f_s \geq 4B, \end{cases}$$



- After sampling one replicas is down-converted with frequency shift
- $f_s/4$ shift equal to {1, -j, -1, j} or {I, -Q, -I, Q}

[*] D. Bernal, P. Closas, J. A. Fernandez-Rubio, "Digital I/Q Demodulation in array processing: theory and implementation," in 16th European Signal Processing Conference (EUSIPCO 2008), Lausanne, Switzerland„ 2008.

Active RFF

Fingerprint an existing wireless communication between CRs with a modulated signal.

Received signal:

ASK with $f_{FP} = f_{IF}$

$$y_{IF}(t) = x_{DSSS}(t) + x_{FP}(t) + \nu(t)$$

After ADC:

$$y_{IF}[n] = V[n] \cdot cos(2\pi f_{IF} \cdot nT_s + \theta[n]) + g[n],$$

$$V[n] = A_a\sqrt{\frac{2}{T_{sa}}}, \quad \theta[n] = pT_s, \quad g[n] = x_{DSSS}[n] + \nu[n]$$

After Digital I/Q demodulation:

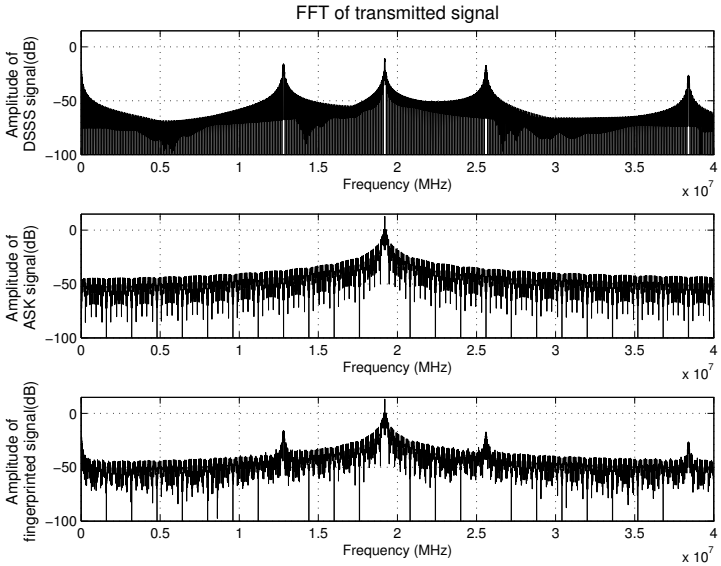
$$y_I[n] = \frac{V[n]}{2} \cdot cos(p) \cdot (1 + (-1)^n) + \tilde{g}_I[n],$$

$$y_Q[n] = \frac{V[n]}{2} \cdot sin(p) \cdot (1 - (-1)^n) + \tilde{g}_Q[n]$$

Detector:

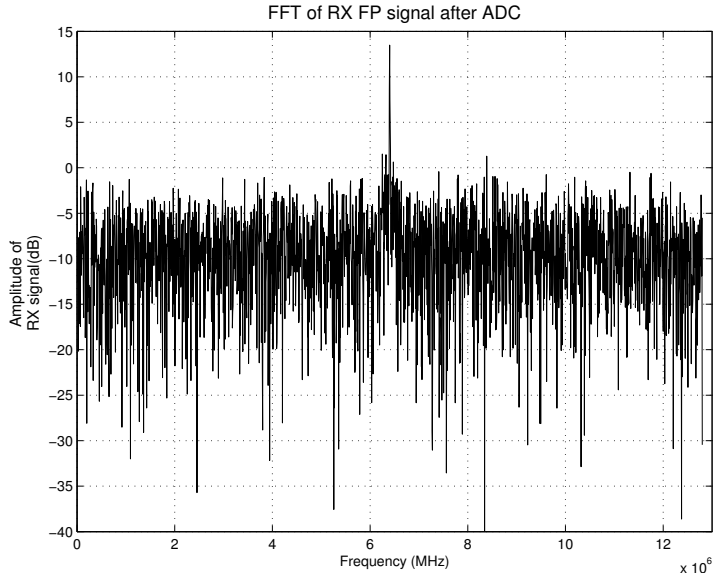
$$d[k] = \begin{cases} 1, & \text{if } z^2[kT_s] \geq \frac{E_s}{2}, \\ 0, & \text{otherwhise} \end{cases}$$

Spectrum



Spectrum of TX signal:

- The combination of these two signals is reasonable because it exploits built-in rejection of SS against narrow-band;

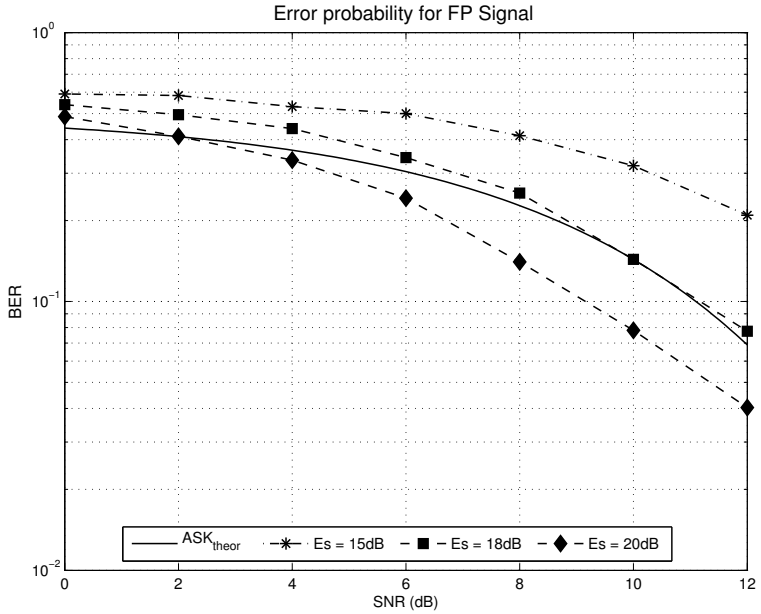


Spectrum of RX signal after ADC:

- This signal has to be down-converted in BB with frequency shift.

Results

Goal: Feasibility of ARFF to encapsulate data in host wireless comm.

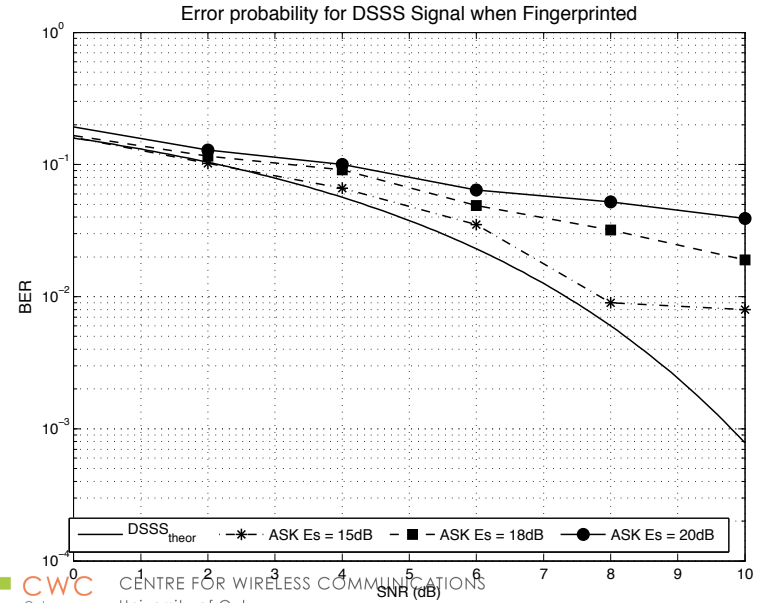


$$\frac{E_s}{N_0} = 10log_{10}(k) + 3 + SNR$$

k = samples for symbol

Error probability for FP signal:

- ✓ Comparison against theoretical ASK curve changing the Es value.



Error probability of DSSS with ARFF

- ✓ Minimal perturbation of DSSS signal when FP has higher Es.

Conclusions:

① Active RFF was proposed as innovative method to encapsulate data inside host wireless comm. Cognitive network;

② The proposed method refers to stenography transmitting securely data hidden in SS communication.

③ Advantages:

A. Active RFF improve spectrum efficiency;
B. Attractive solution using I/Q demodulation using lower number of inputs for digital signal processing;
C. Valuable technique for Cognitive Resource Manager (CRM) facilitating data exchange without any additional resources.

THANK YOU!

Questions?

(Simone.Soderi@ge.com)