Communications Research Centre Canada
An Agency of Industry Canada

Centre de recherches sur les communications Canada
Un organisme d'Industrie Canada

Cognitive Radio Networking in the ISM Band

John Sydor
Siva Palaninathan
Bernard Doray
Jianxing Hu

THE RESEARCH BROAD BAND WIRELESS GROUP
www.crc.ca/coral

WWW.CRC.GC.CA

COMMUNICATIONS RESEARCH CENTRE CANADA | CENTRE DE RECHERCHES SUR LES COMMUNICATIONS CANADA

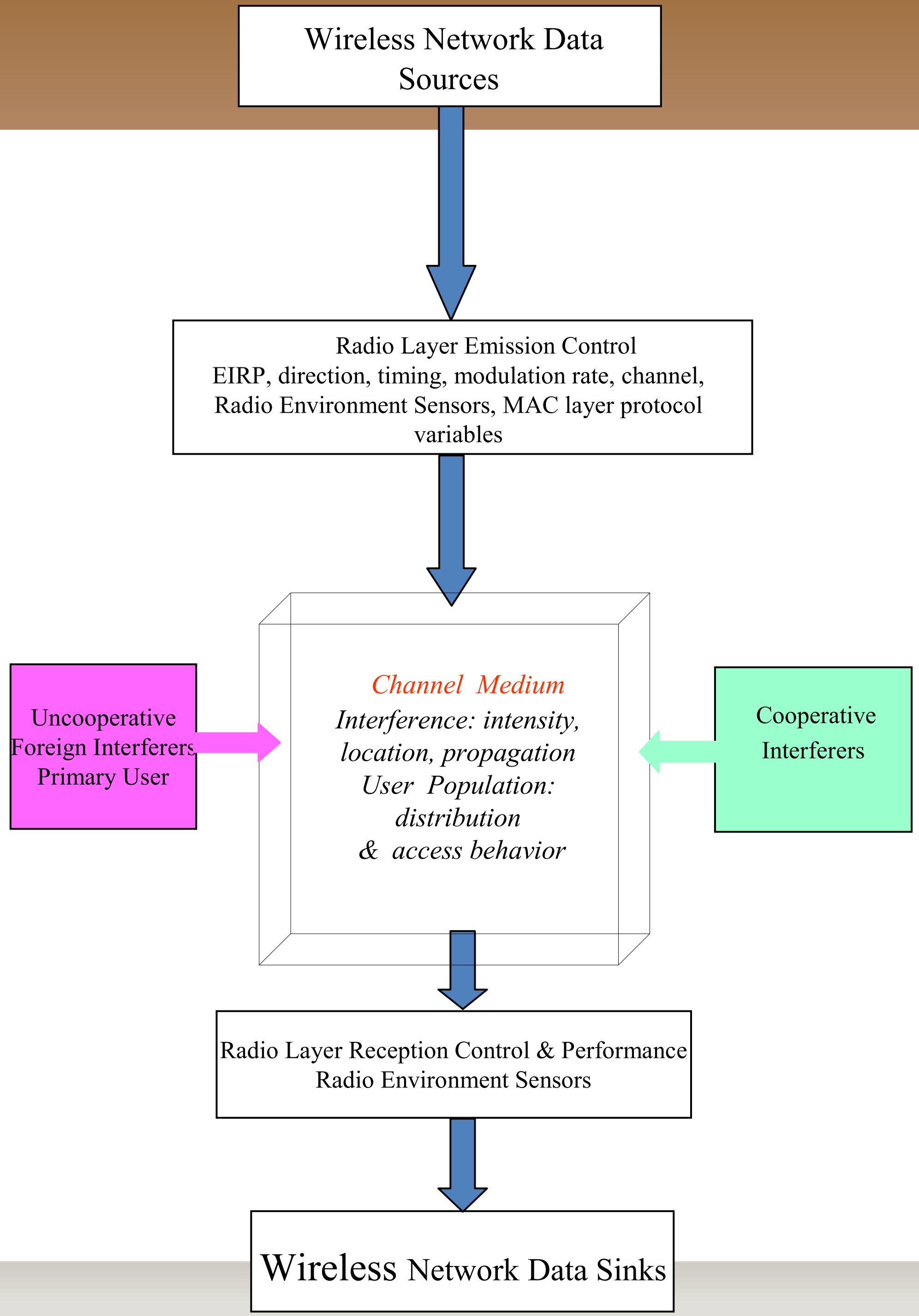
Canada

CRC

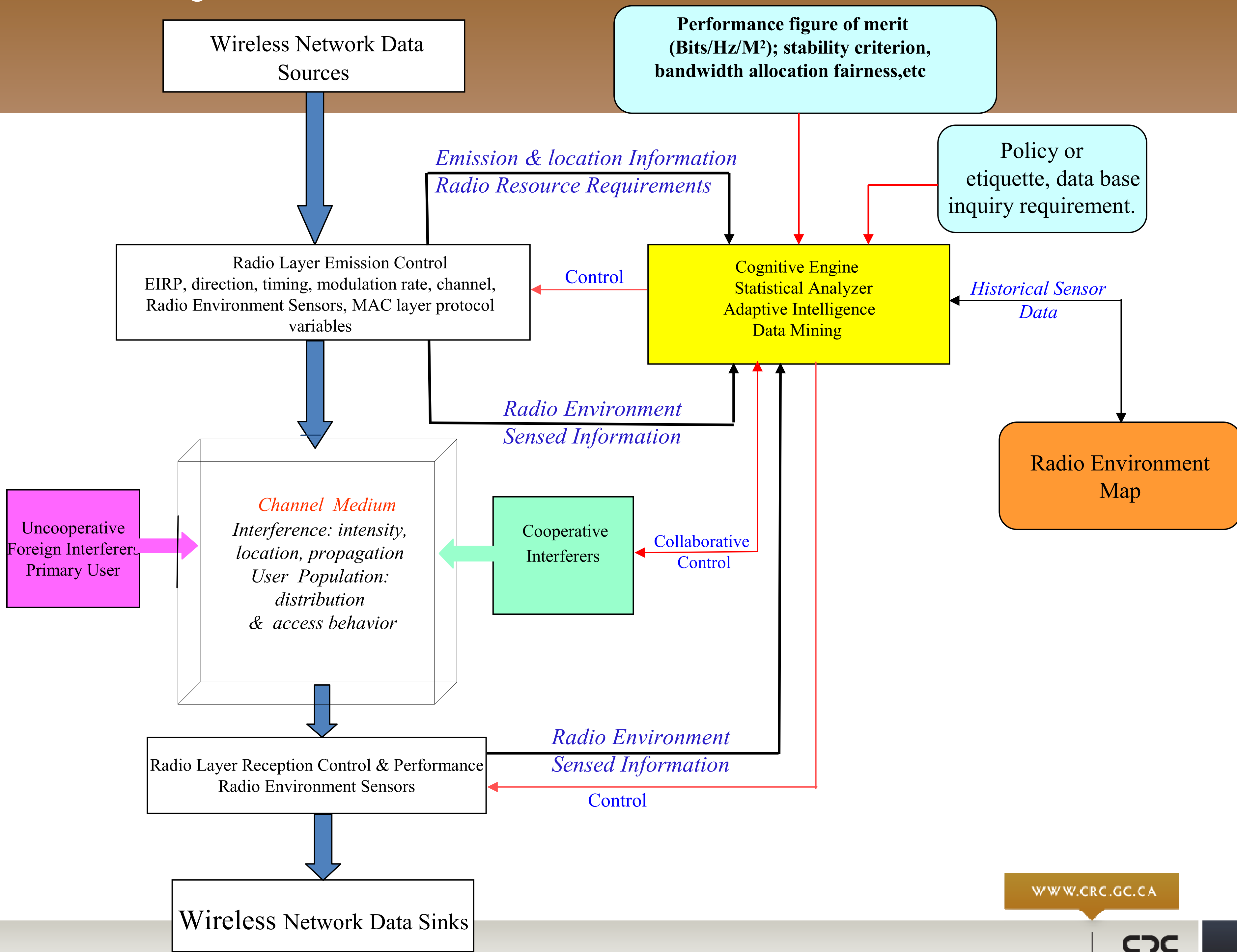
Webinar Overview

- Overview of Cognitive Radio concepts.
- The CRC-CORAL Wi-Fi Cognitive Radio Network Platform.
- Implementation of Cognitive control
- Software for control of sensing and WiFi packet emission in space, time, & channel
- The Radio Environment Awareness Map (REAM):
- Use of Cognitive Engines to control the Network.
- Applications: Dynamic Spectrum Access & Data mining in the REAM

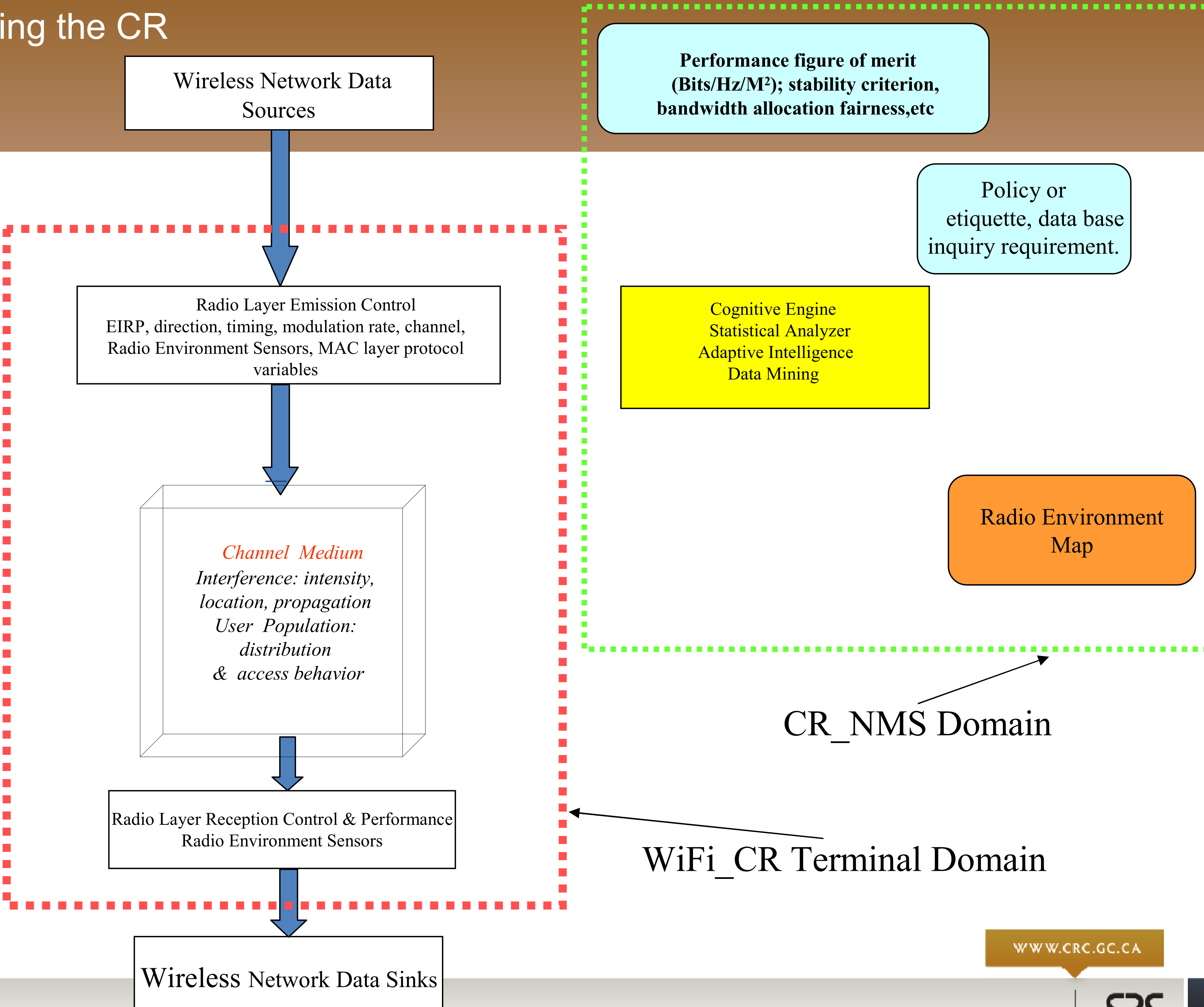
Generic Wireless Network



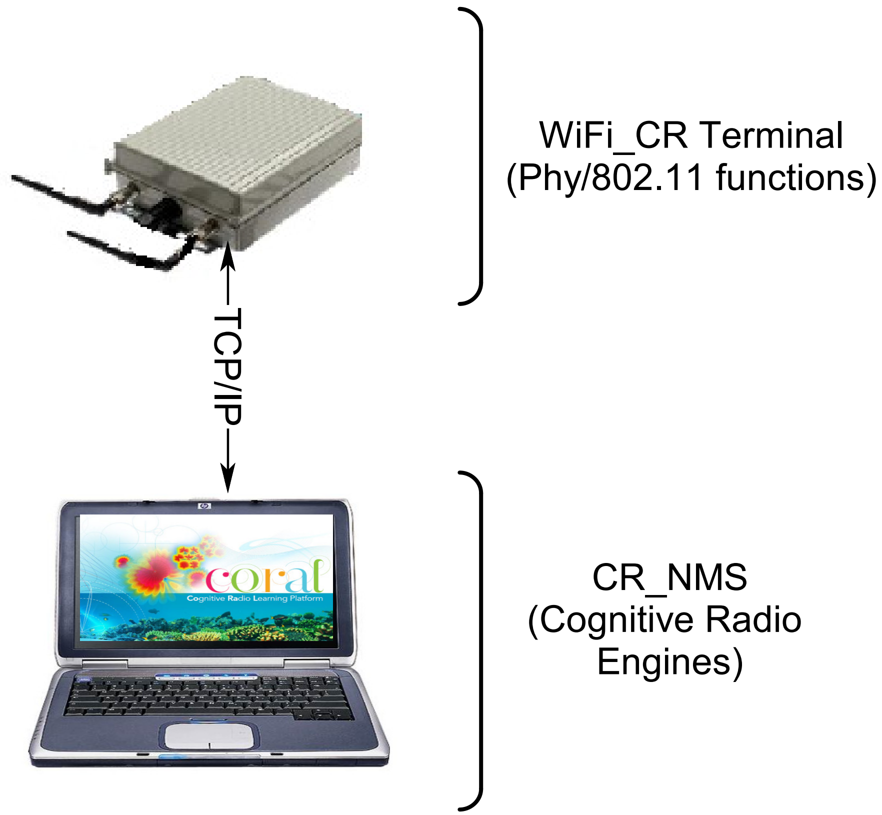
Formative Cognitive Radio Architecture



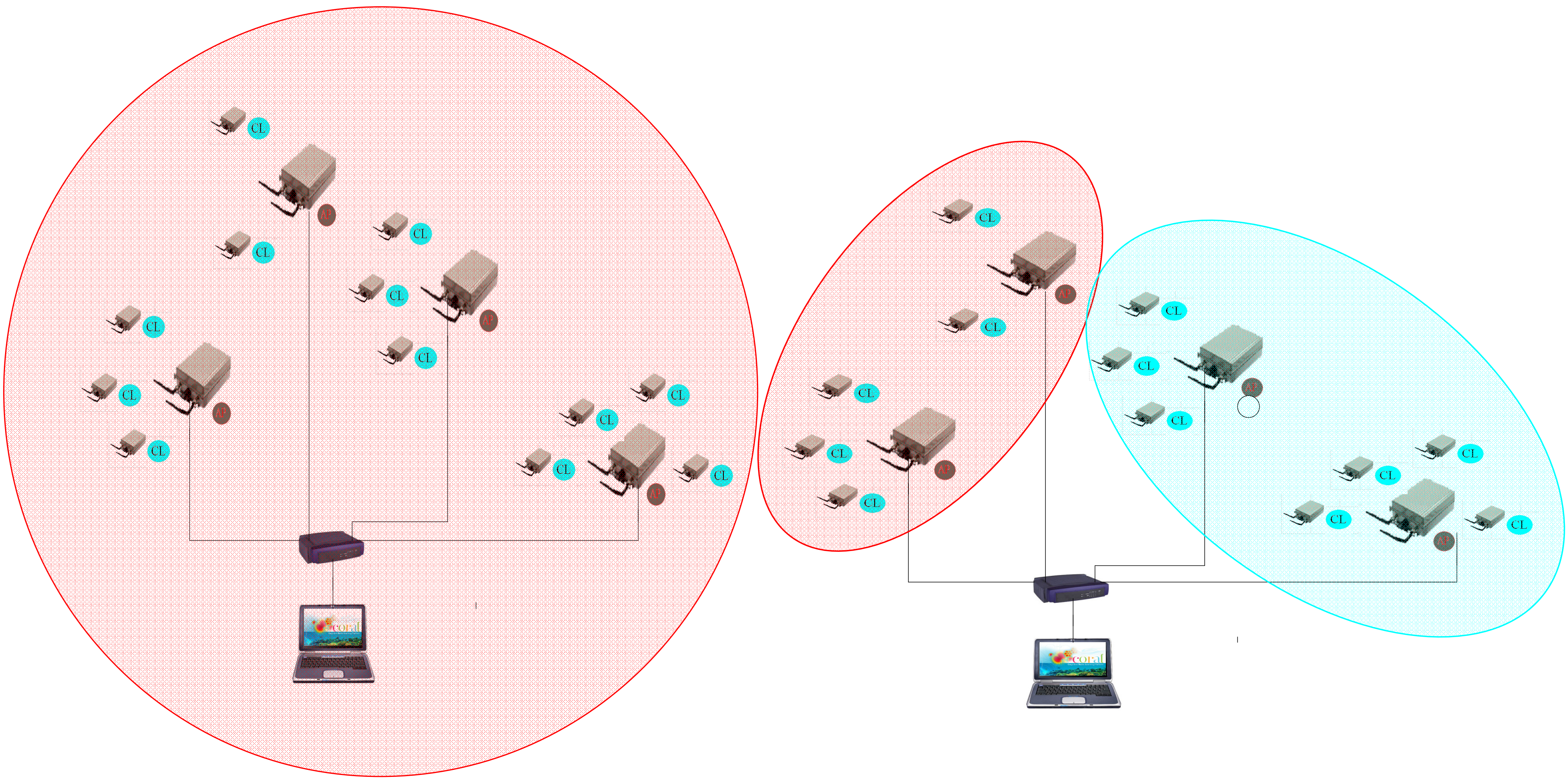
Partitioning the CR



Partitioned Components of CORAL



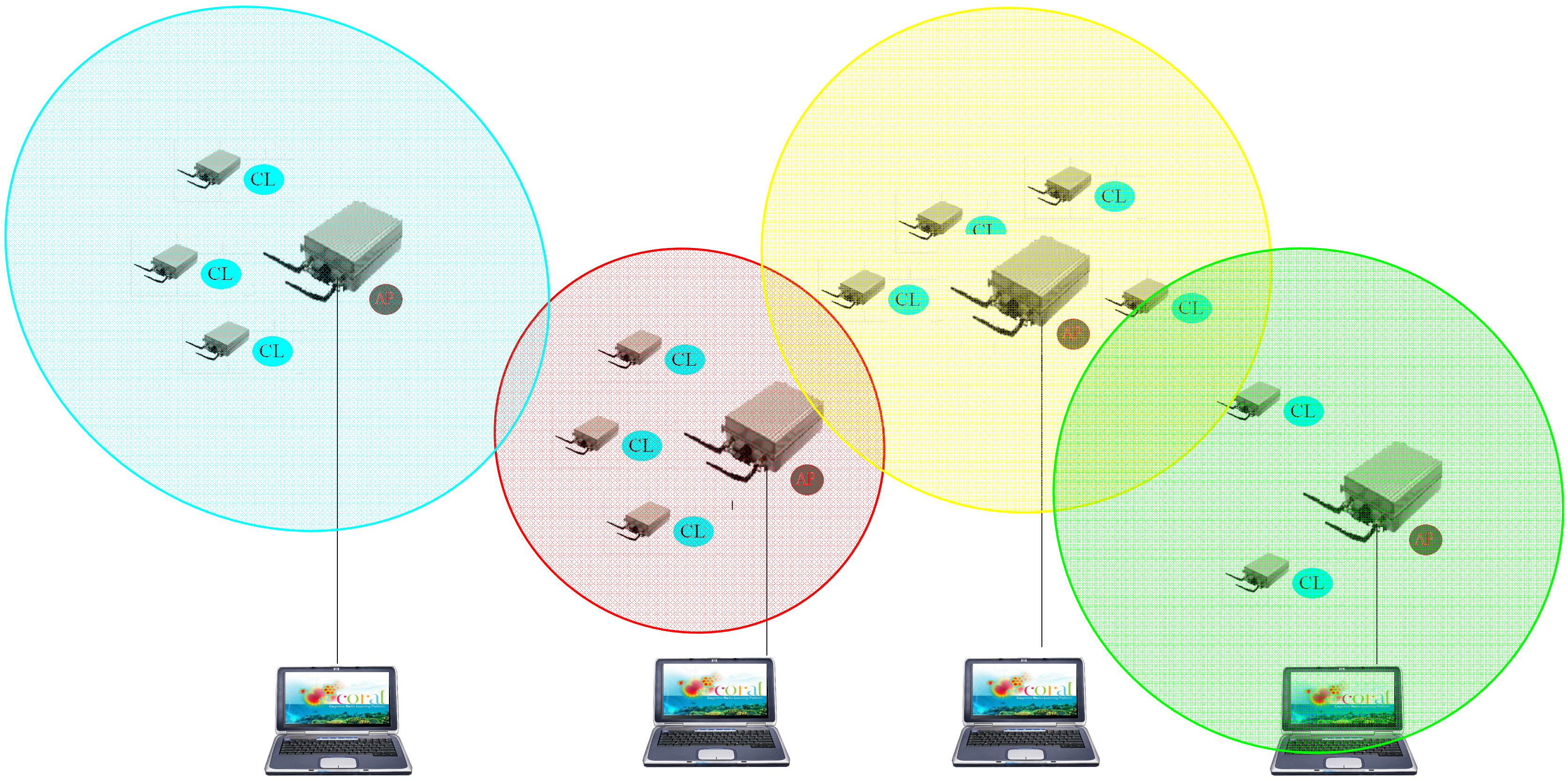
Examples of Modular Deployments



Single CRN on one CR_NMS

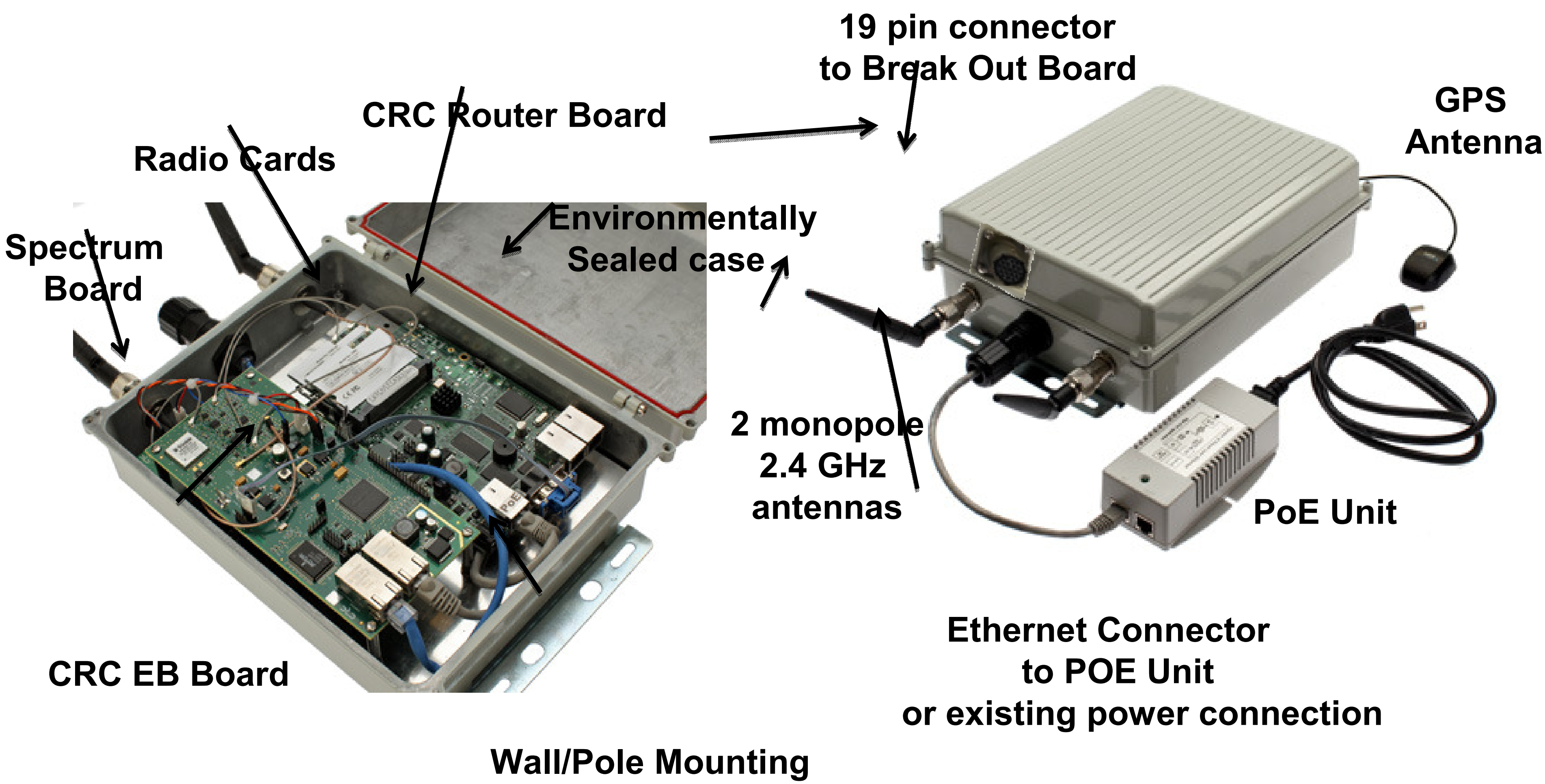
Two CRNs on one CR_NMS

Examples of Modular Deployments



4 CRNs on 4 CR_NMS

The CRC-CORAL Wi-Fi Cognitive Radio Network Platform
WiFi_CR Layout



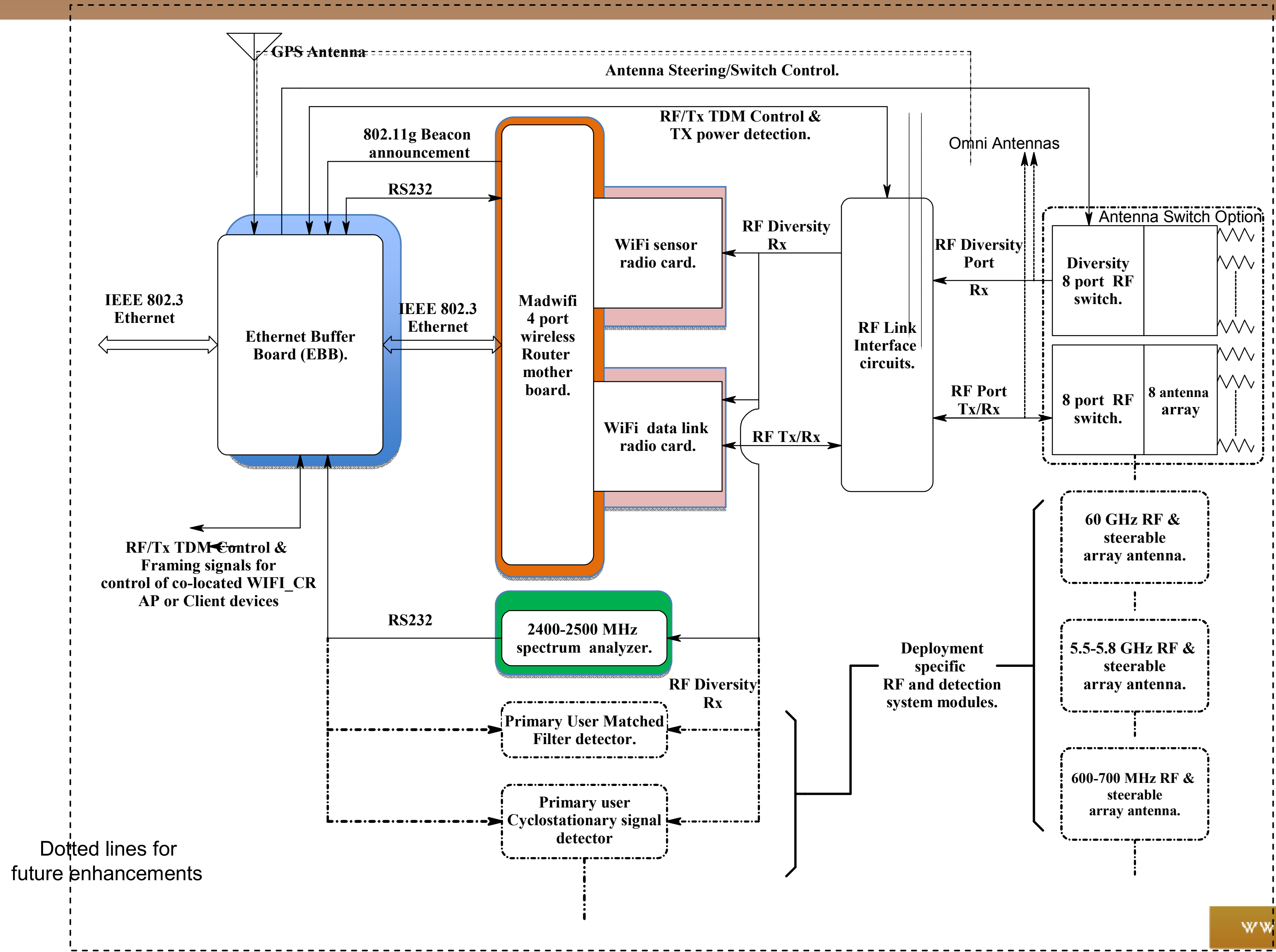
The CRC-CORAL Wi-Fi Cognitive Radio Network Platform
PHY Layer Emission Control

PHY Layer Capabilities of WiFi_CR

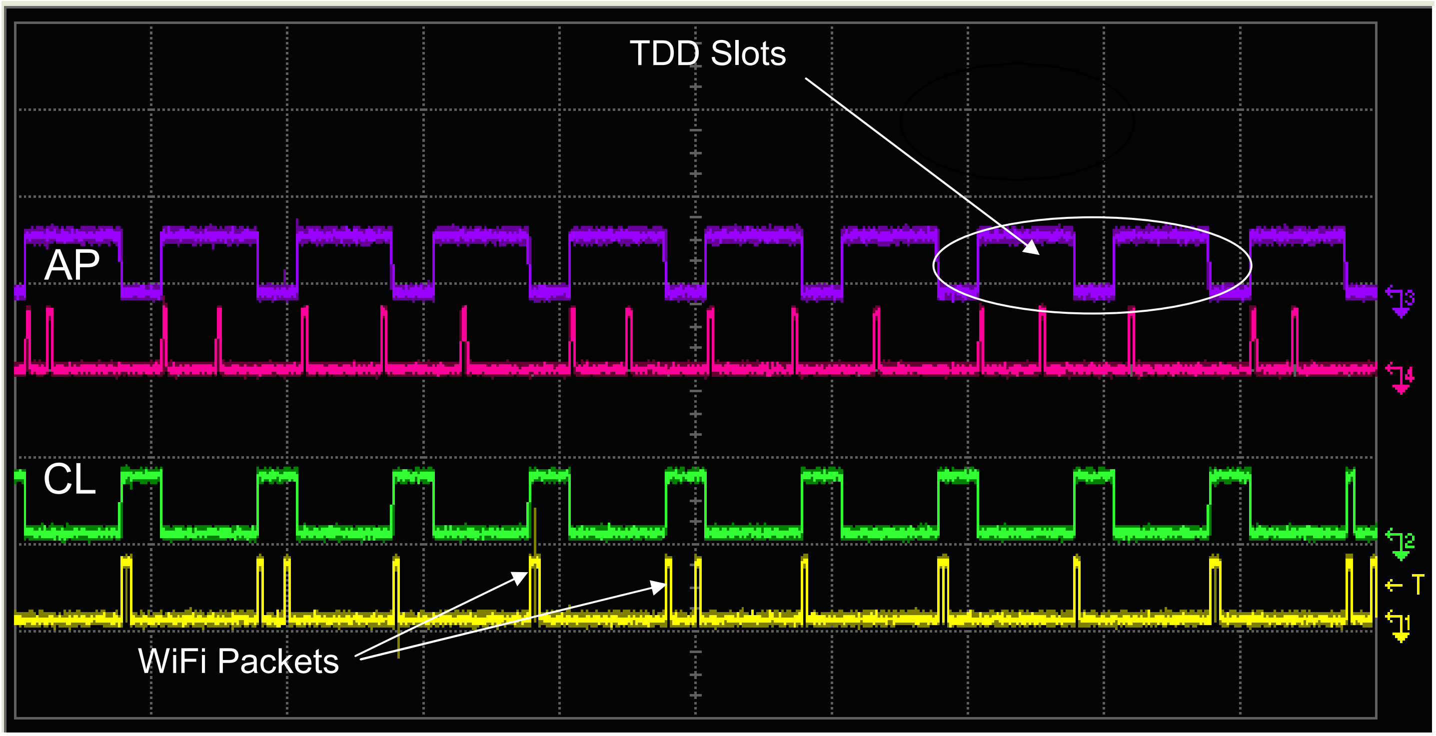
- Standard IEEE 802.11g operation, Infrastructure Mode
- TDD/TDMA constrained CSMA/CA
- Per packet beam steering (8 Beams)
- Per Slot antenna beam steering
- Control of EIRP, channel, Ack policy, modulation rate,etc
- GPS, Beacon based, and ARP based TDD slot synchronization

The CRC-CORAL Wi-Fi Cognitive Radio Network Platform

WiFi_CR: block signal processing subsystem layout

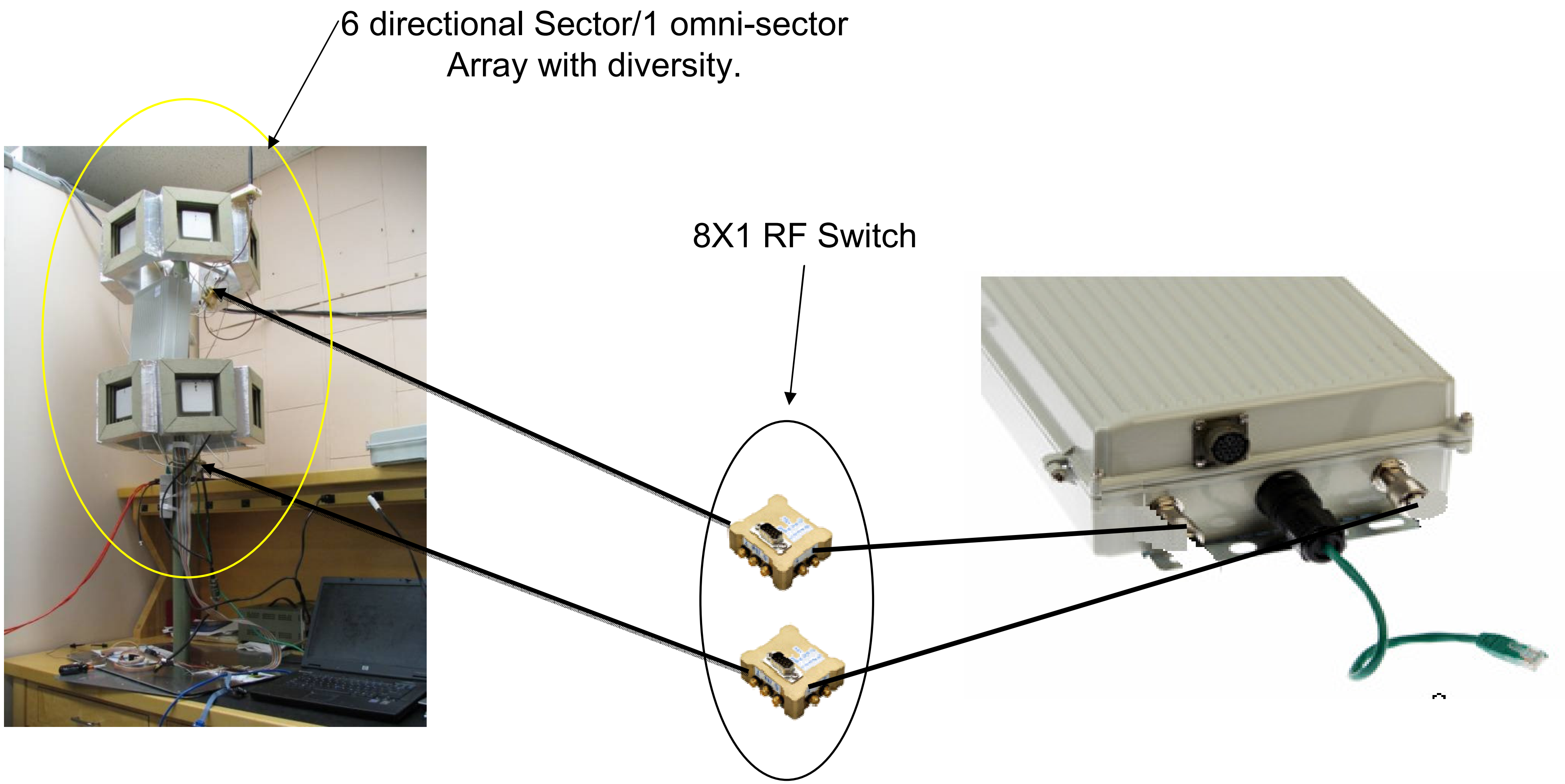


The CRC-CORAL Wi-Fi Cognitive Radio Network Platform TDD/TDMA synchronized slots

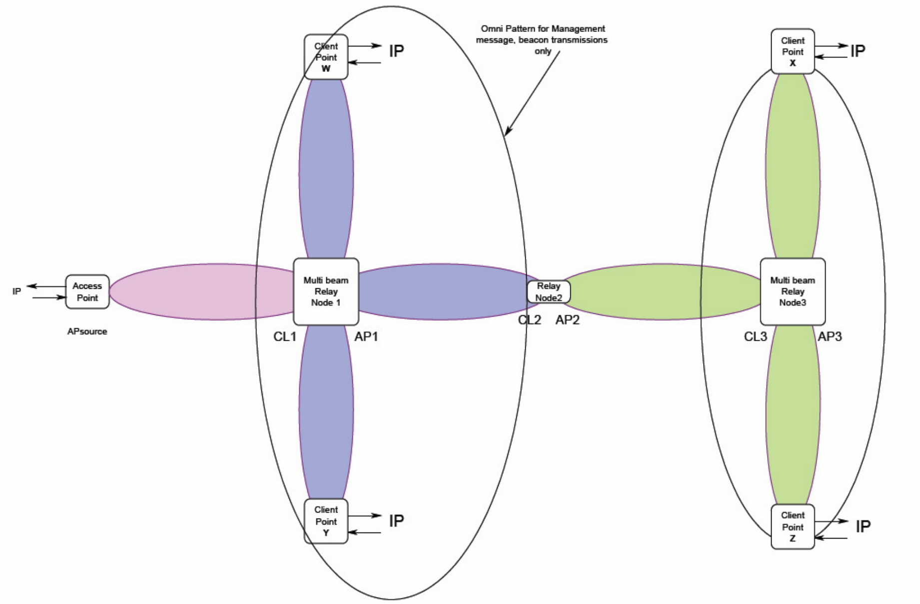


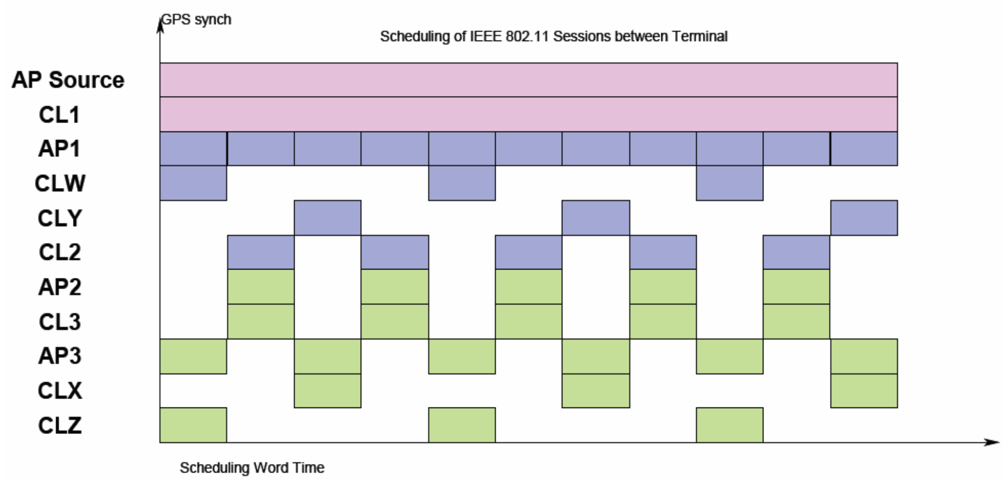
WiFi TDD with No ACK data transmission between
An Access Point and Client terminal.

Multi-Sector Beam Antenna



Example:Relay and Multiple Beam Steering Configurations





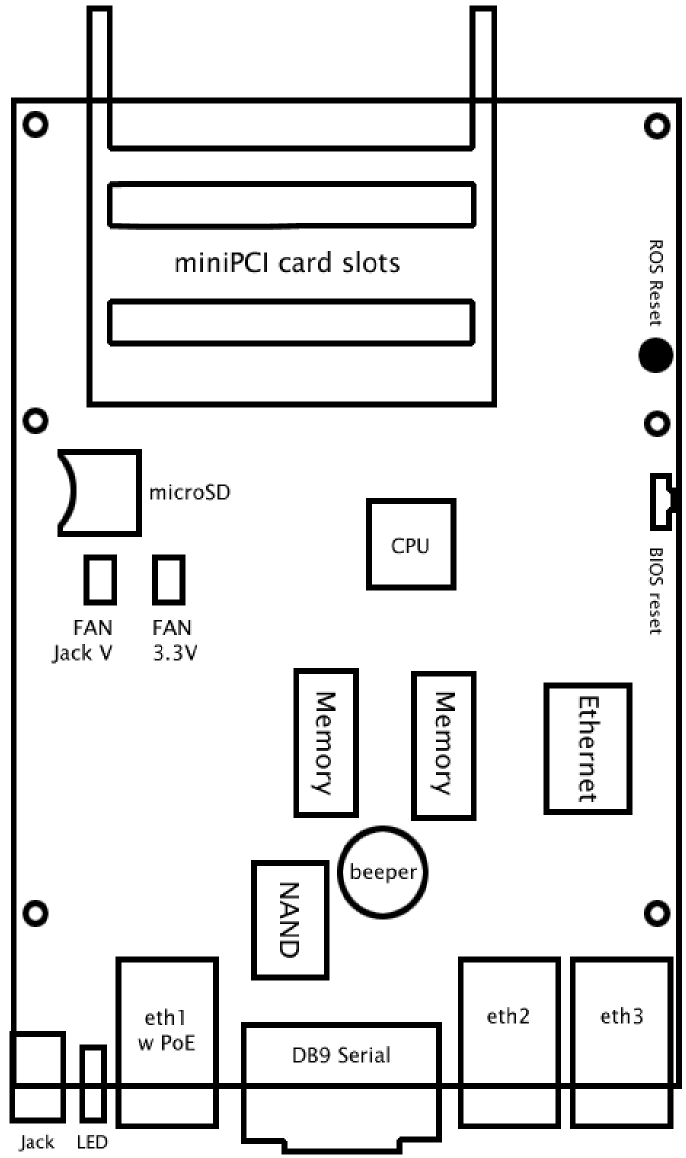
Agenda - RouterBoard

- RouterBoard Hardware
- RouterBoard Software
- Wireless Sniffer

RouterBoard Hardware

Mikrotik RB433 (AH, UAH)

- MIPS-based AR7100 300 MHz
- 64 MB RAM
- 64 MB NAND
- 3 Ethernet ports, 1 PoE, Auto MDI/X
- 1 Serial port
- LED GPIO, used for beacon alerts
- 3 MiniPCI slots



RouterBoard Hardware cont.

Wistron CM9 MiniPCI 80211a/b/g

- Atheros AR5212 based
- Infrastructure mode – Link Interface
- Monitor mode – Sniffer Interface
- Madwifi Driver

RouterBoard Software

- RouterBOOT Booter
- Linux – Customized OpenWRT
- Modified Madwifi Driver
- NetSNMP
- Wireless sniffer (Kismet Based)

RouterBOOT Booter

Available via serial port by pressing DELETE key during boot cycle

- **BOOT Device Menu**
  your choice: o - boot device

  Select boot device:
  e - boot over Ethernet
  * n - boot from NAND, if fail then Ethernet
  1 - boot Ethernet once, then NAND
  o - boot from NAND only
  b - boot chosen device

- **Board Info Menu**
  Board type: 433
  Serial number: 21FE01987F32
  Firmware version: 2.20
  CPU frequency: 300 MHz
  Memory size: 64 MB
  eth1 MAC address: 00:0C:42:45:27:85
  eth2 MAC address: 00:0C:42:45:27:86
  eth3 MAC address: 00:0C:42:45:27:87

Linux - OpenWRT

- Kernel 2.6.32
- Kamikaze 8_09
- Real time extension

Modifications for CORAL

- GPIO for Beacon alerts
- Various init scripts

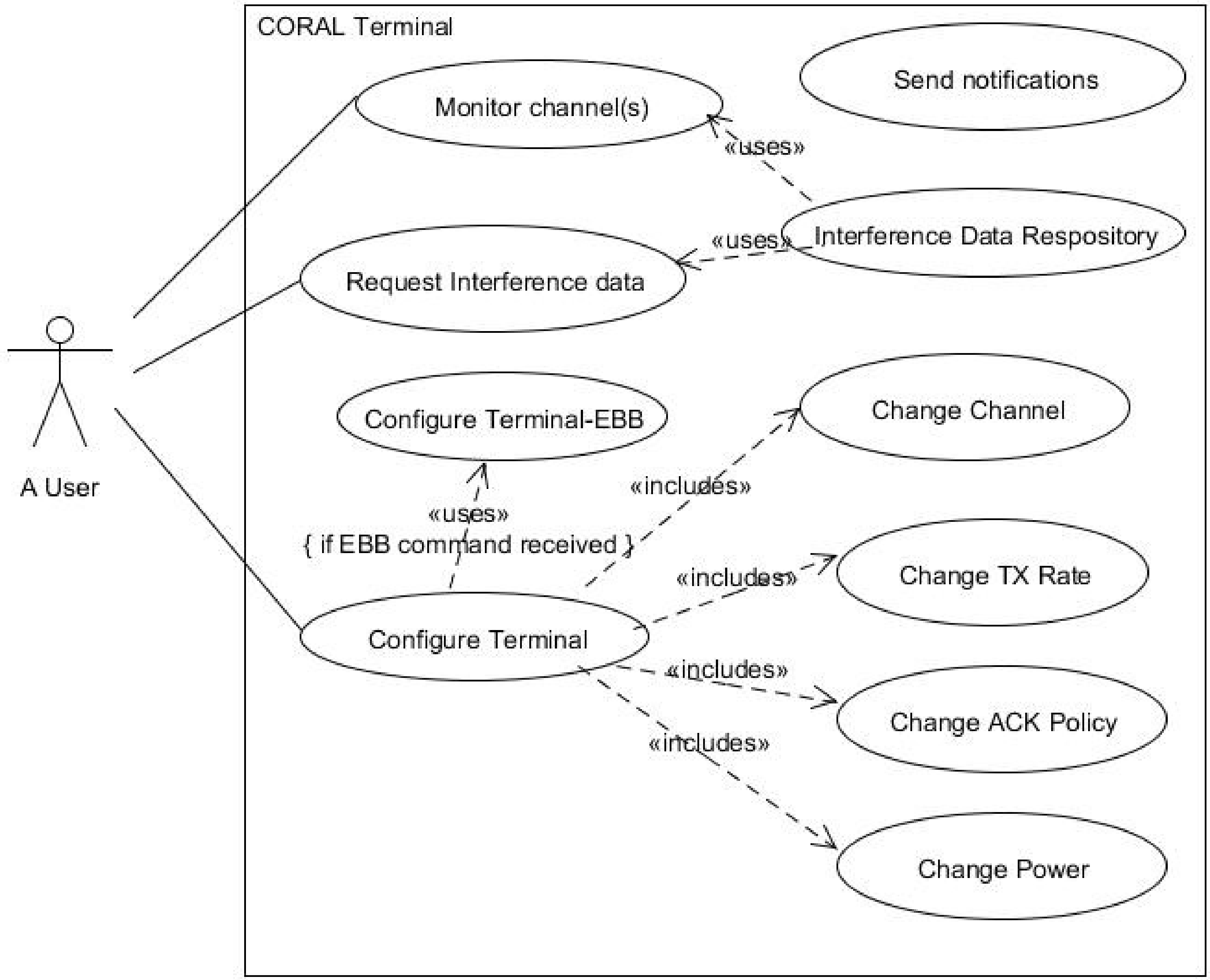
Madwifi Driver

- Core version r3314
- Latest patches by the development team
- Patches related to cross compilation

Modifications for CORAL

- Beacon notification
- Best effort Q for all type of traffic
- Number of retries
- Diversity enabled
- Deterministic transmission; CCA, backoff
- CTS/RTS Disabling
- Turn ON/OFF ACK policy

NetSNMP


CORAL Terminal
Monitor channel(s)
Send notifications
«uses»
Interference Data Respository
«uses»
Request Interference data
A User
Configure Terminal-EBB
Change Channel
«includes»
«uses»
{ if EBB command received }
«includes»
Change TX Rate
Configure Terminal
«includes»
Change ACK Policy
«includes»
Change Power

NetSNMP cont.

- Core version 5.1.2
- Version 2
- Latest patches by the development team
- Patches related to cross compilation

Modifications for CORAL

- 802.11 MIB agent implemented/modified
  - Handling all radio related configuration commands
  - Link related statistics collection
- A new sniffer agent implemented
  - Wireless sniffer
  - Handling part of EBB communication
  - Various CORAL system specific commands

Wireless Sniffer

- Kismet based, significantly modified for on-demand scanning
- Supports Canada and Europe bands
- Madwifi in monitor mode
- Captures raw 802.11 packets only
- Corrupted packets are accounted
- Controlled by SNMP
- Highly customizable

Wireless Sniffer – Interference capturing process

- 500 ms per channel
- Interference bins are created for each unique set of:
  - Source MAC
  - Destination MAC
  - BSSID
  - Channel
  - Packet Type
  - Packet Subtype
- When a packet is received, its bin is updated with:
  - timestamp
  - number of packets accumulated in the bin
  - average RSSI
  - packet utilization (packet length/packet transmitted rate)

Wireless Sniffer – Interference capturing process cont.

- Information captured from a packet
  - Captured time; local to system clock
  - GPS Location of the sniffer node
  - Packet type/subtype
  - Sniffer node ID
  - TX Duty cycle
  - TX Avg
  - Channel the packet is detected on
  - Channel the sniffer is on
  - Source MAC address
  - Destination MAC address
  - Total duration of packet(s)
  - SSID
  - RSSI or averaged RSSI
  - Number of packets
  - Transmit rate of the packet

Wireless Sniffer – customization

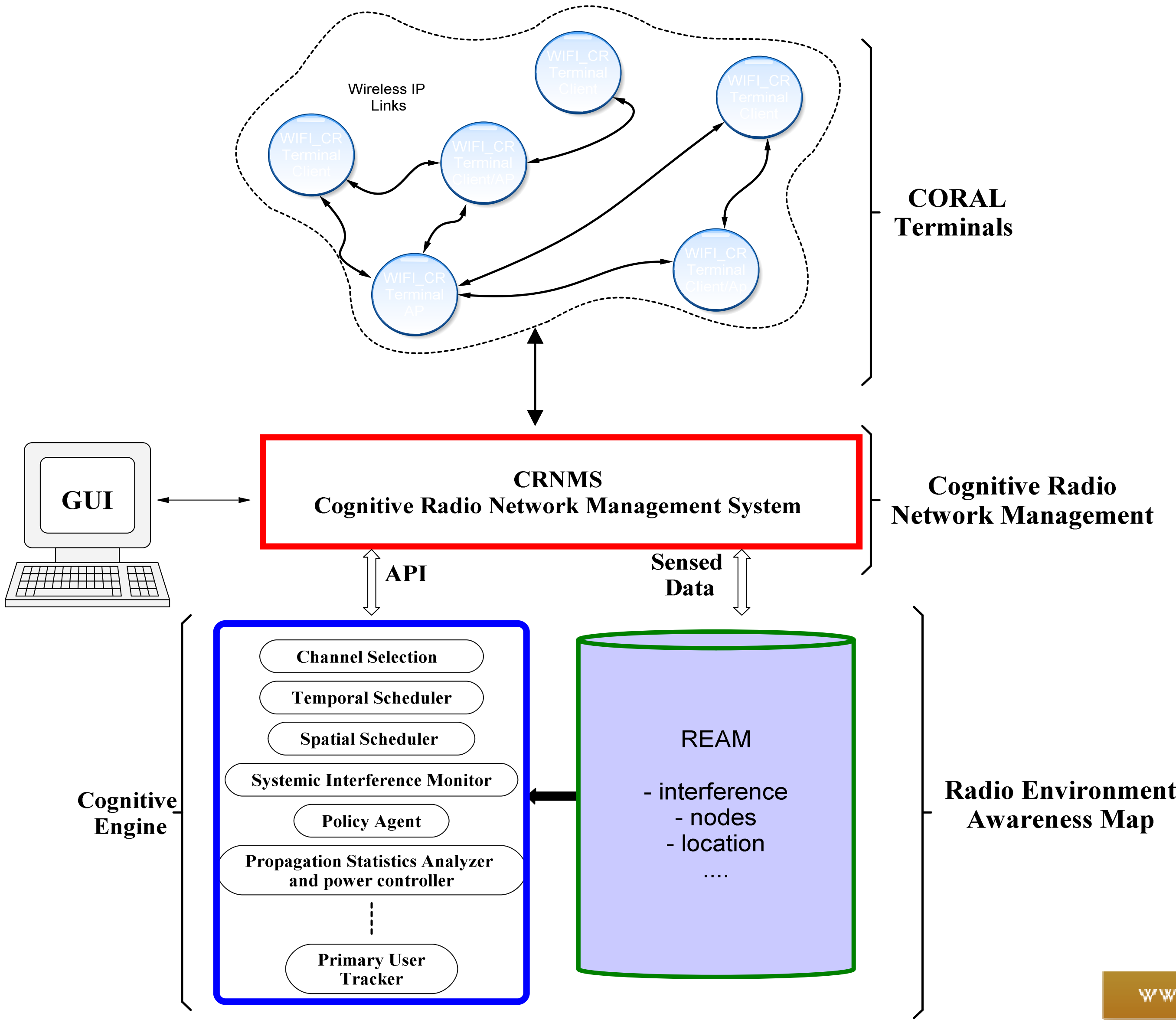
- Sniffer software can be customized for:
  - Packets only from a specific node
  - Management, controls or data packets only
  - Complete decoded-preamble
  - Channel utilization
  - Statistics collection: Number of corrupted packets, Retransmission packets, etc

Wireless Sniffer cont.

- High CPU usage
- All packets reaching monitor interface are accounted
- Fields extraction
- Utilization calculation
- RAM usage

```
Mem: 12676K used, 114708K free, 0K shrd, 0K buff, 4936K cached
CPU:  27% usr  62% sys   0% nice   9% idle   0% io   0% irq   0% softirq
Load average: 0.08 0.02 0.01
  PID  PPID USER     STAT   VSZ %MEM %CPU COMMAND
  828     1 root     S     5032   4%  90% /usr/bin/kismet_drone
  795     1 root     S     4248   3%   0% /usr/sbin/snmpd -Lf /dev/null -p /var
  928   789 root     S     1992   2%   0% /usr/sbin/dropbear -p 35
  936   789 root     S     1992   2%   0% /usr/sbin/dropbear -p 35
  937   936 root     S     1972   2%   0% -ash
  237     1 root     S     1972   2%   0% syslogd -C16
  929   928 root     S     1968   2%   0% -ash
    1     0 root     S     1960   2%   0% init
  935   929 root     R     1960   2%   0% top
  228     1 root     S     1960   2%   0% logger -s -p 6 -t
  230     1 root     S     1960   2%   0% init
  239     1 root     S     1956   2%   0% klogd
  834     1 root     S     1952   2%   0% watchdog -t 5 /dev/watchdog
  789     1 root     S     1936   2%   0% /usr/sbin/dropbear -p 35
  622     1 root     S     1404   1%   0% hostapd -P /var/run/wifi-ath0.pid -B
  819     1 root     S     1388   1%   0% /usr/sbin/ntpclient -i 60 -s -l -D -p
  251     1 root     S     1136   1%   0% /sbin/hotplug2 --override --persisten
    5     2 root     SW<      0   0%   0% [khelper]
   83     2 root     SW<      0   0%   0% [mtdblockd]
```

CRNMS


Wireless IP Links
WIFI_CR Terminal Client
WIFI_CR Terminal Client/AP
WIFI_CR Terminal AP
CORAL Terminals
GUI
CRNMS
Cognitive Radio Network Management System
Cognitive Radio Network Management
API
Sensed Data
Channel Selection
Temporal Scheduler
Spatial Scheduler
Systemic Interference Monitor
Policy Agent
Propagation Statistics Analyzer and power controller
Primary User Tracker
Cognitive Engine
REAM
- interference
- nodes
- location
....
Radio Environment Awareness Map

CRNMS API

- Interface provided by the CRNMS to control / interrogate CORAL terminals
- Interface provided to access the REAM data collected by the CRNMS
- API Available for the following programming languages:
    - C, MATLAB, Python
- APIs specified/generated from the WSDL (Web Service Description Language) specification

CRNMS API

- Interface used for
    - scheduling, monitoring, configuration,…
    - setting direction, data rate, EIRP, channel, scheduling
    - soliciting interference, position, occupancy

CRNMS API

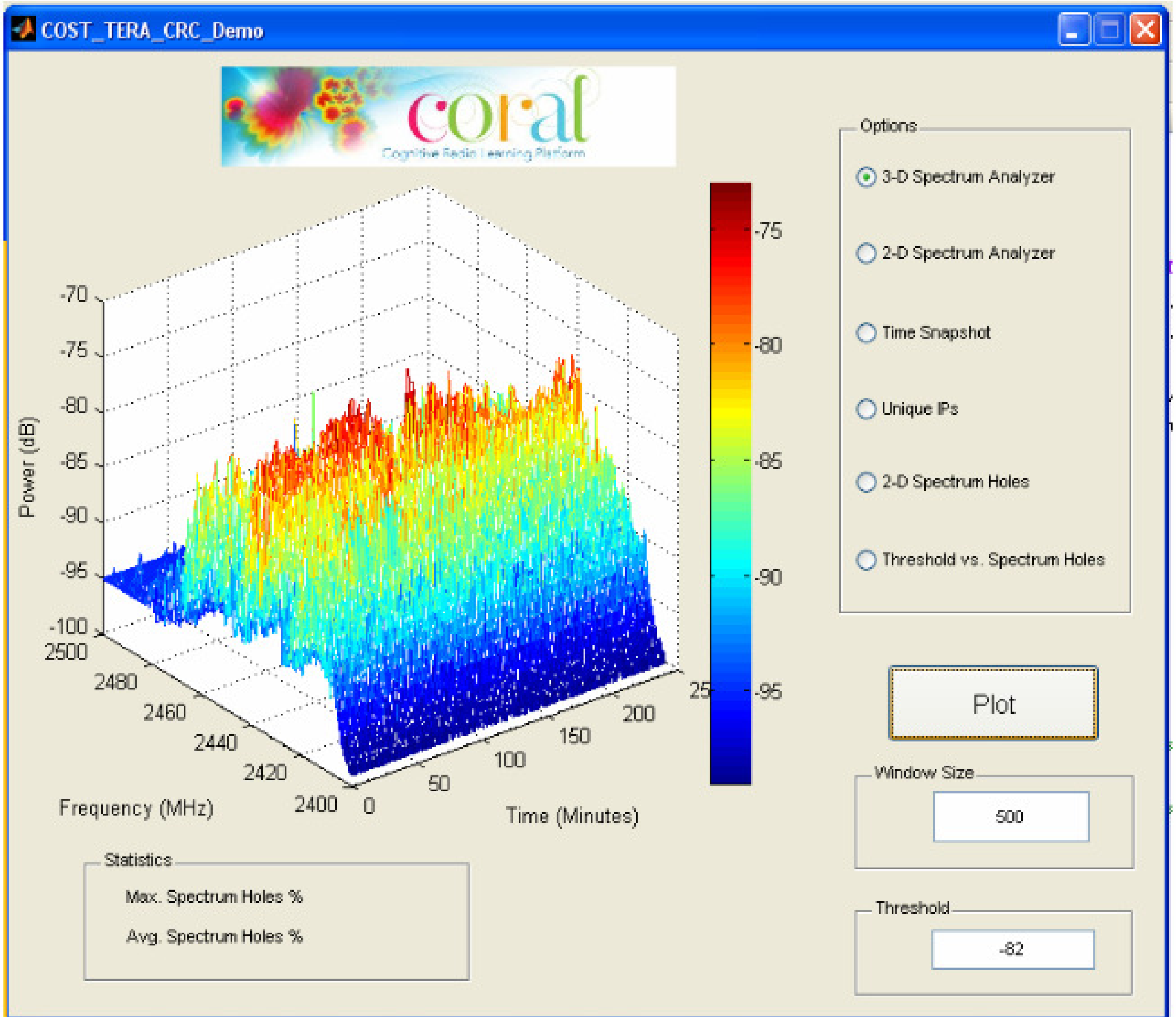
- getVersionSynch
- getNodeInfoSynch
- getGpsInfo
- getStatusInfo

- setPollingInterval
- collectData

- resetEbb

- **setBestChannel**
- **setCodeWord**
- **setTxPower**
- **setLinkSpeed**
- **setAntennaDstTable**
- **setAck**
- **setEbbMode**

MATLAB Toolbox



Examples of how the API can be used

- filter data in REAM to store specific network characteristics
- data mining
- interference signature versus time
- study of network activity
- tune network to maximize throughput dynamically / autonomously
- sense interference, adjust timeslots, beam angles, channel to avoid interference (spatial, temporal, spectrum tuning)
- find whitespace and use it opportunistically

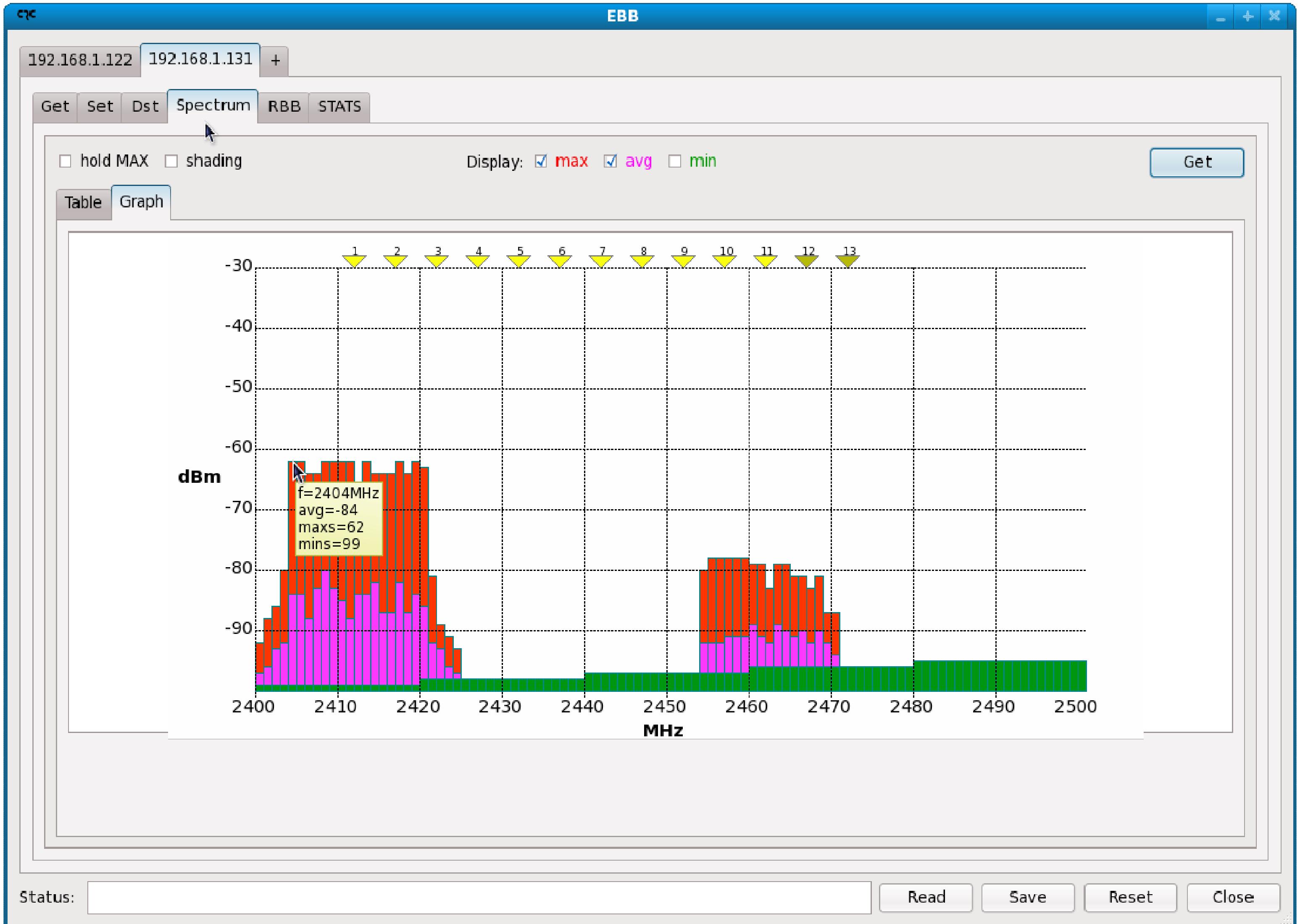
REAM Database

- Interference Table
  - WIFI interference collected by the CORAL terminals (SA, DA, SSID, RSSI, Packet type, Packet Subtype, ...)
- Spectrum Data Table
  - Spectrum Analyzer data collected by the CORAL terminals (101 measurements from 2.4 to 2.5Ghz)
- Nodes Table
  - Information about the nodes currently part of the Cognitive Radio Network (including location if available)
- Alerts Table
  - Log of primary users detection

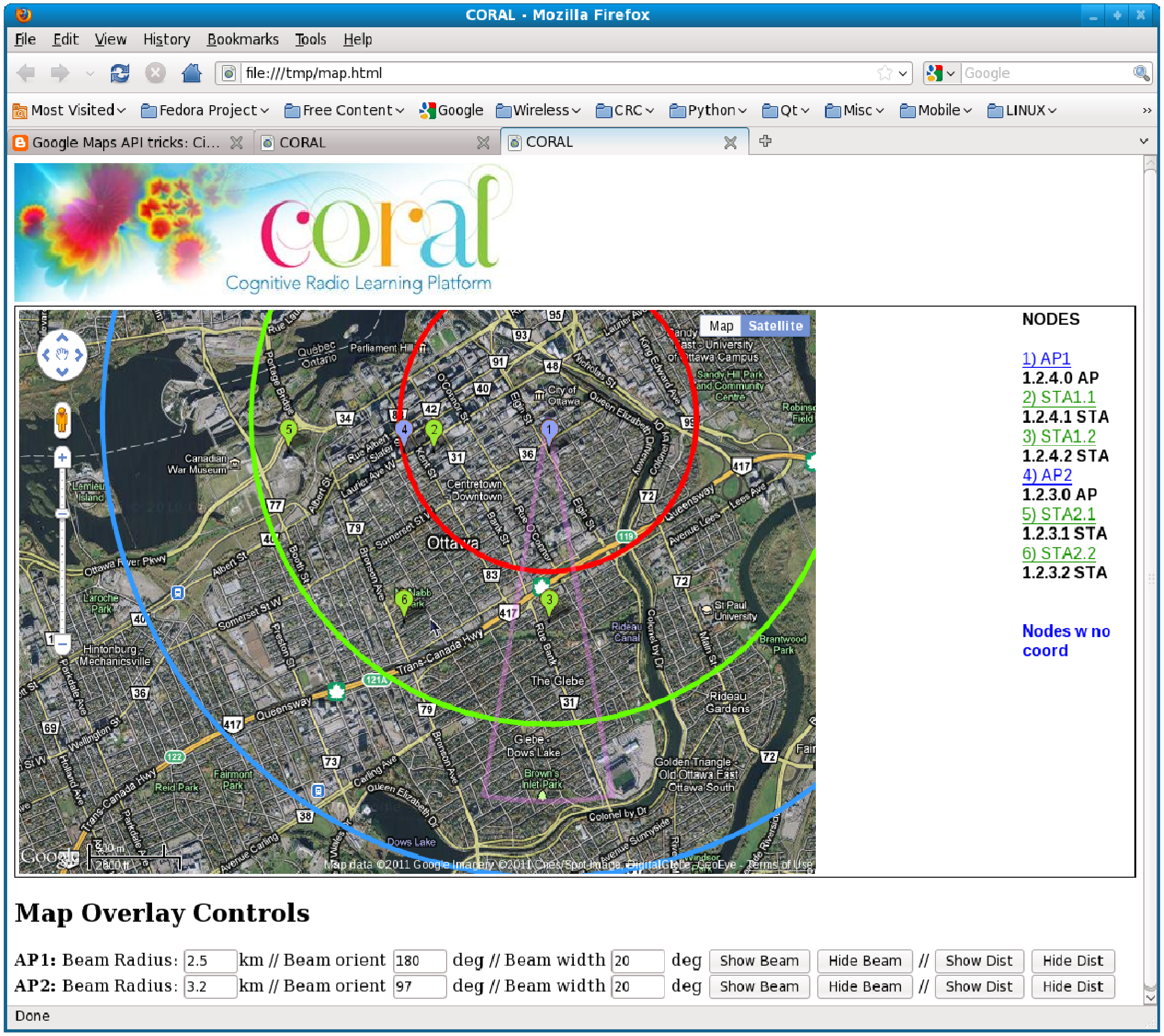
SQL

- REAM database can be queried using the SQL language; examples:
  - SELECT * FROM interference WHERE channel = 11 ;
  - SELECT * FROM interference WHERE channel = 11 and rssi > -65 ;
  - SELECT key,bssid,sa,da,ssid,rssi FROM interference where mode = 'AP';
  - SELECT DISTINCT sa FROM interference WHERE rssi > -65 ;
  - SELECT DISTINCT node from nodes WHERE parent = '12:34:56:78:90:02' ORDER by node;
  - SELECT sa,da,rssi FROM interference WHERE rssi > -60 AND sa IN (SELECT DISTINCT node from nodes WHERE parent = '12:34:56:78:90:00') ORDER by sa ;
  - SELECT * from interference WHERE time > (now() - INTERVAL '1 minute')   ;

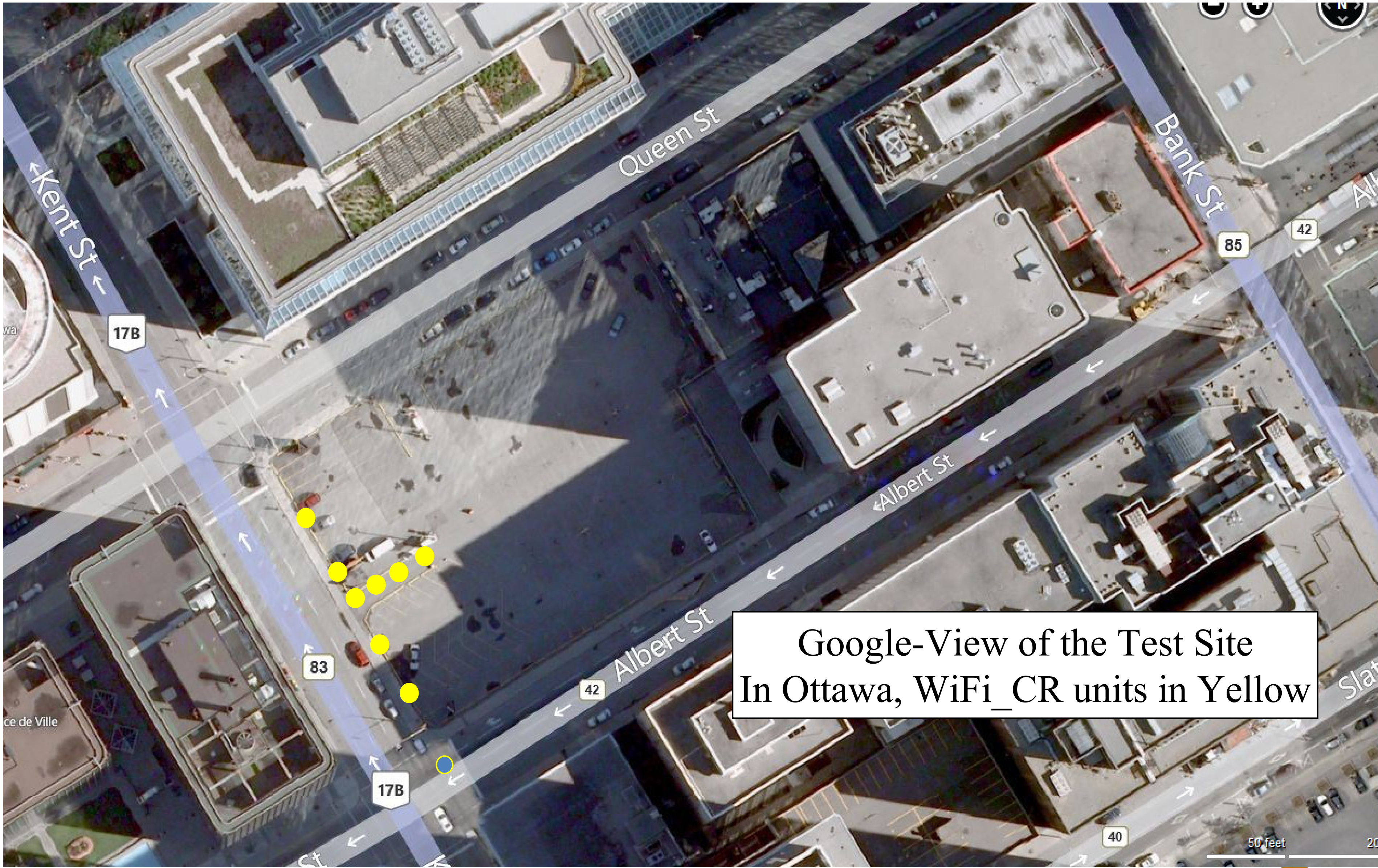
GUI – Spectrum Analyzer Data



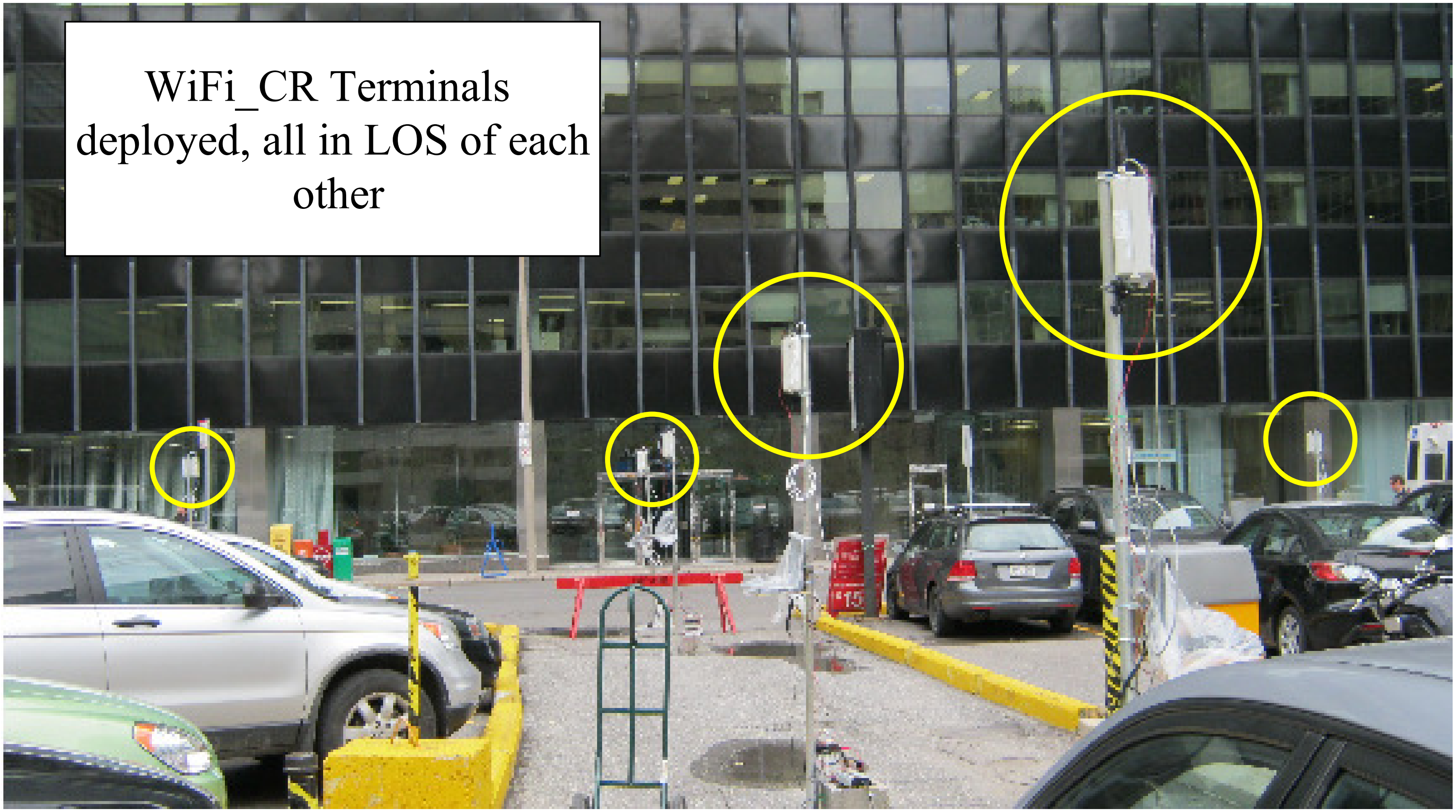
GUI – Mapping Capabilities



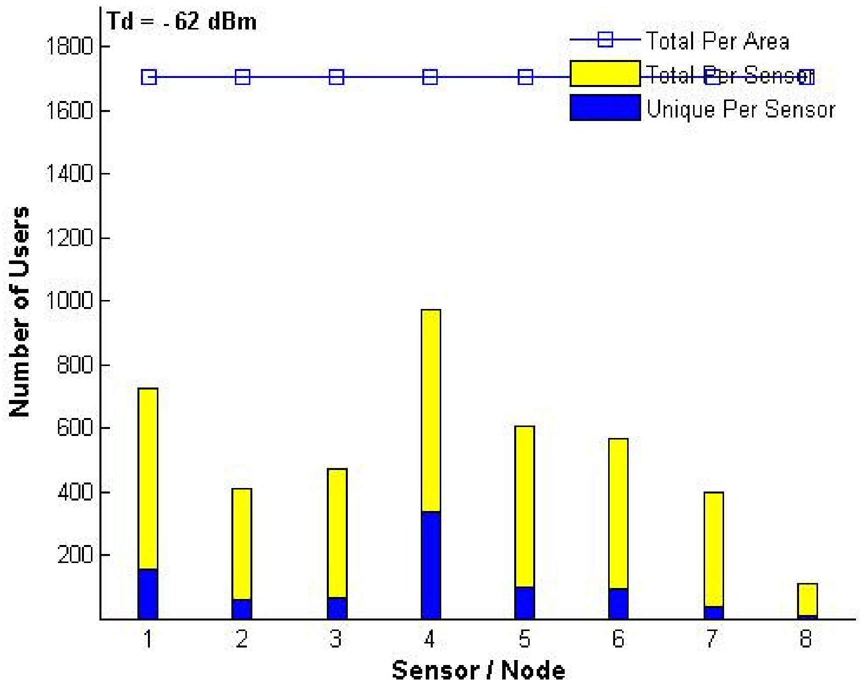
Application Example: Investigation of the Outdoor Urban Interference environment by mining The REAM data base….urban target area for the experiment



Application Example: Investigation of the Outdoor Urban Interference environment by mining the REAM data base…experiment set up.

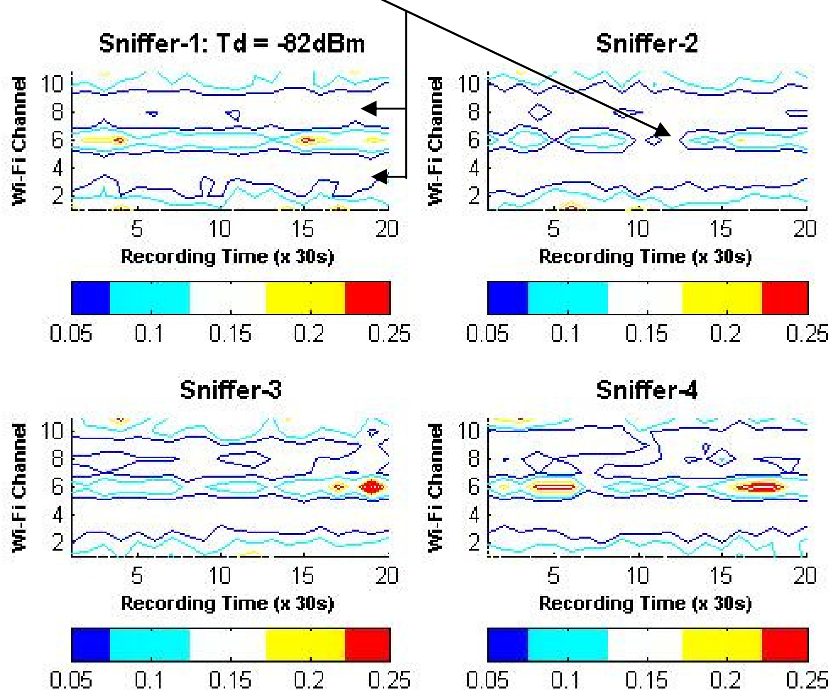


Application Example: Investigation of the Outdoor Urban Interference environment by mining the REAM data base: Extracted Results…Occupancy by interference



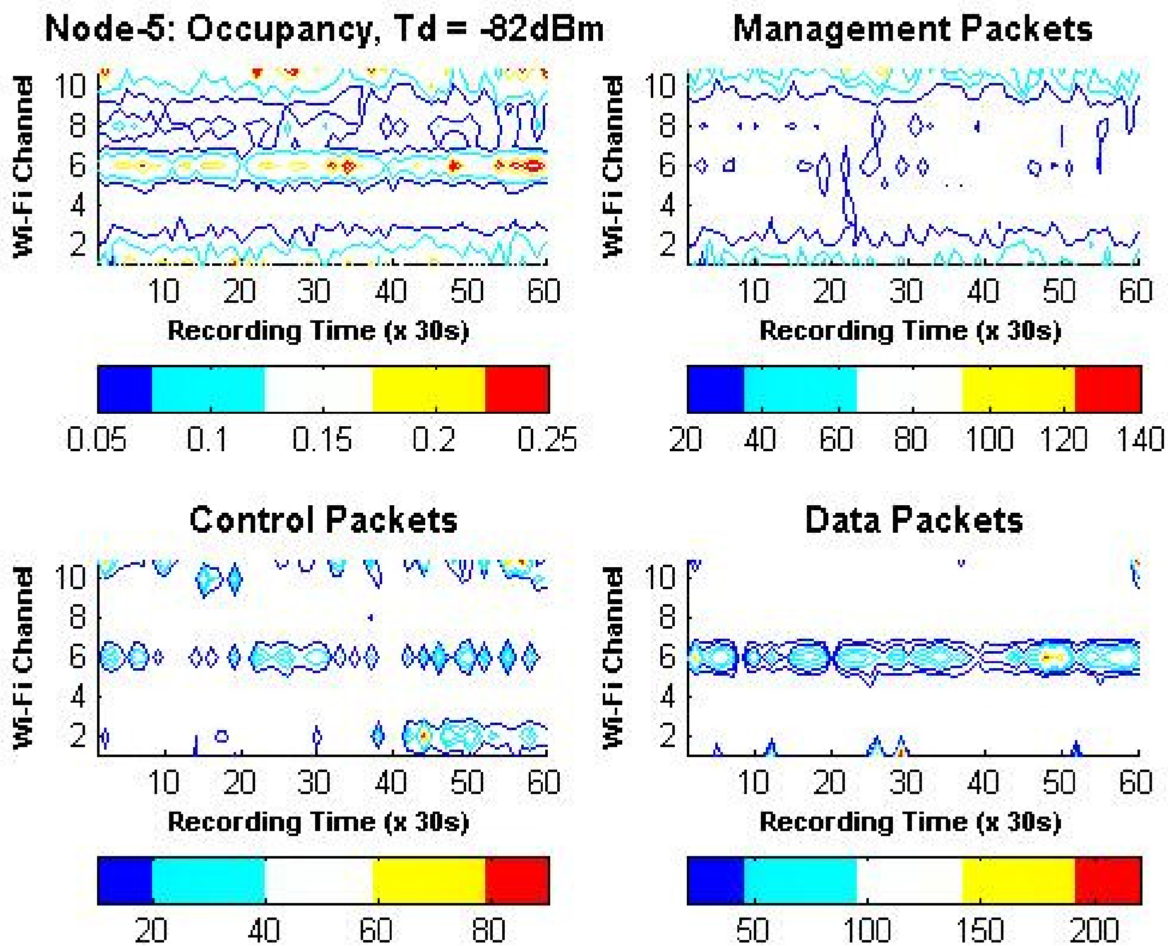
Interferers detected per 10 minute interval
With packet powers>-62 dBm, for all sniffers

Spectrum 'Holes'



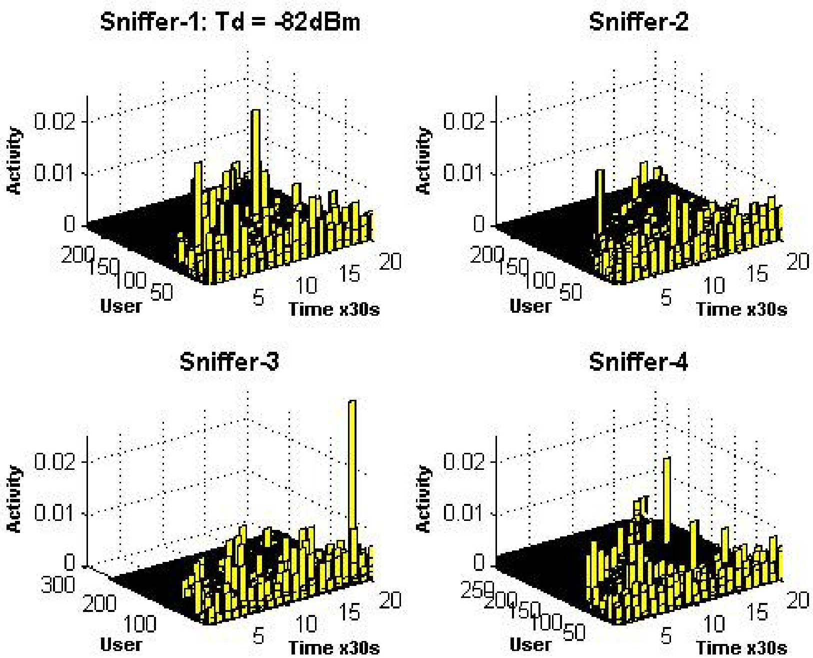
Packet Occupancy, all interfering packets
With power >-82 dBm, as seen at each sniffer

Application Example: Investigation of the Outdoor Urban Interference environment by mining the REAM data base: Extracted Results…Occupancy variations

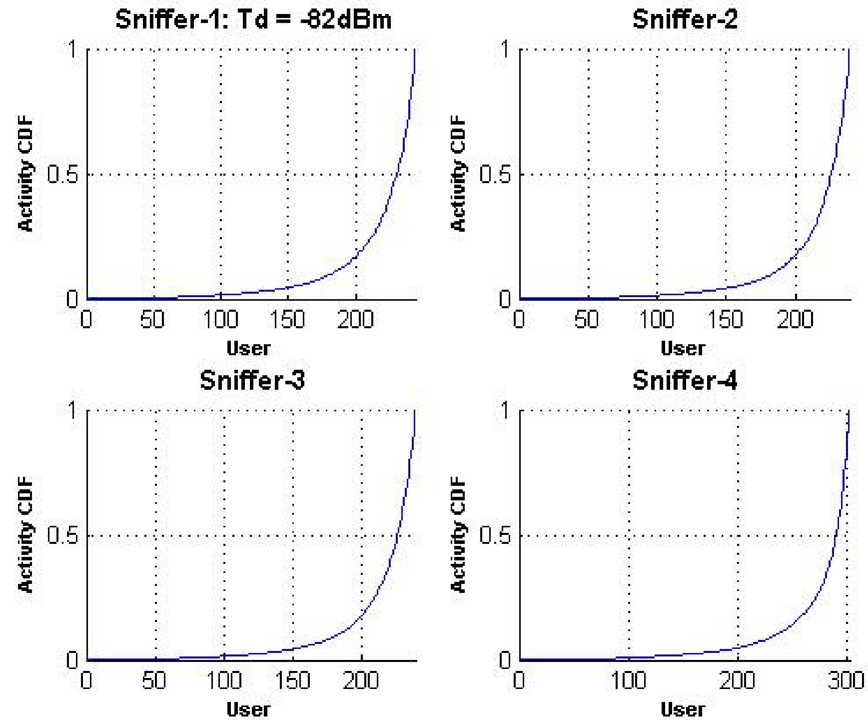


Total Occupancy and Occupancy by different types of WiFi Packets
as seen on Sniffer 5, for powers > -82 dBm

Application Example: Investigation of the Outdoor Urban Interference environment by mining the REAM data base: Extracted Results…degrees of occupancy by users

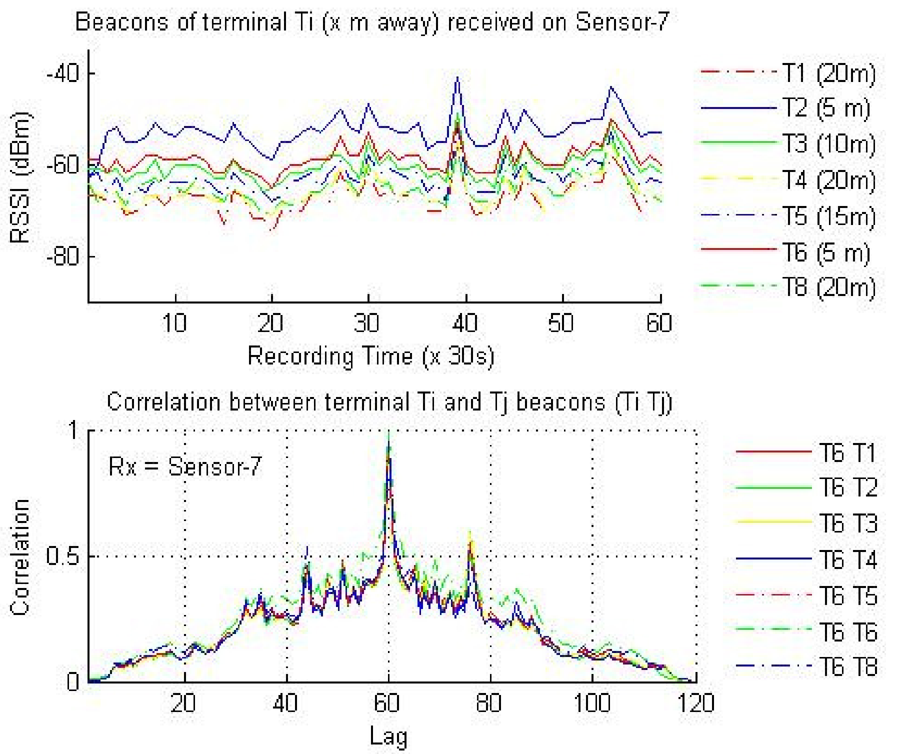


User activity per sniffer over a 10 minutes sample.
Users are unique source addresses; ~ same time,
But at different sniffers

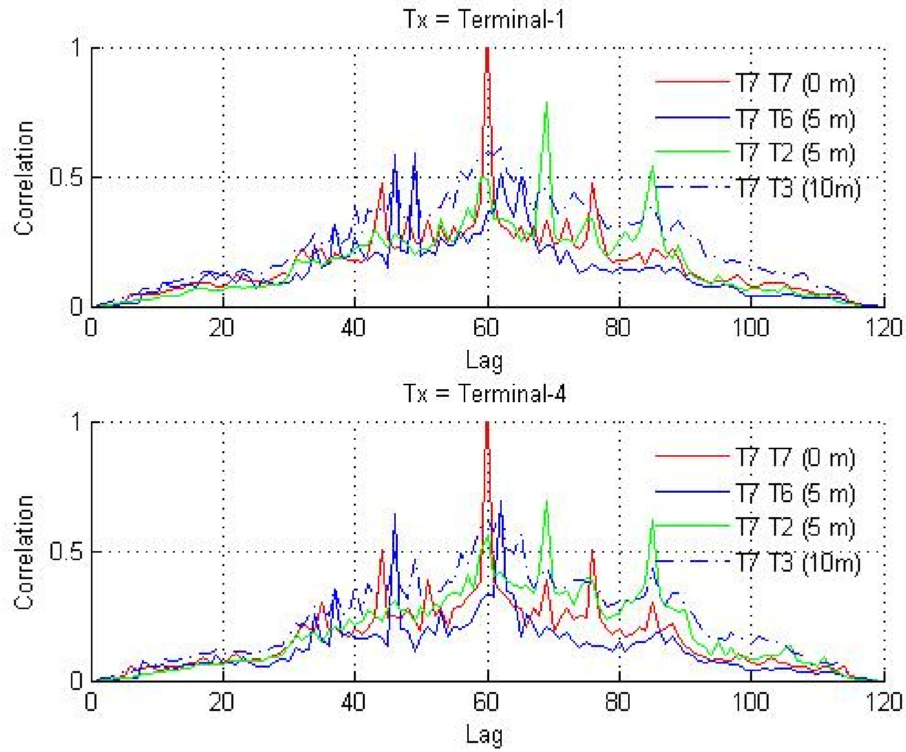


CDF of user activity over a 10 minutes sample.
At different sniffers, power >-82 dBm

Application Example: Investigation of the Outdoor Urban Interference environment by mining the REAM data base: Extracted Results…correlation of interferenc



Top Graph: RSSI of received beacons emanating from terminals 1-6,8 as measured on terminal 7
Bottom Graph: Correlation between beacons' RSSI emanating from terminal 6 and Terminals (1-7,8) as measured on Terminal 7

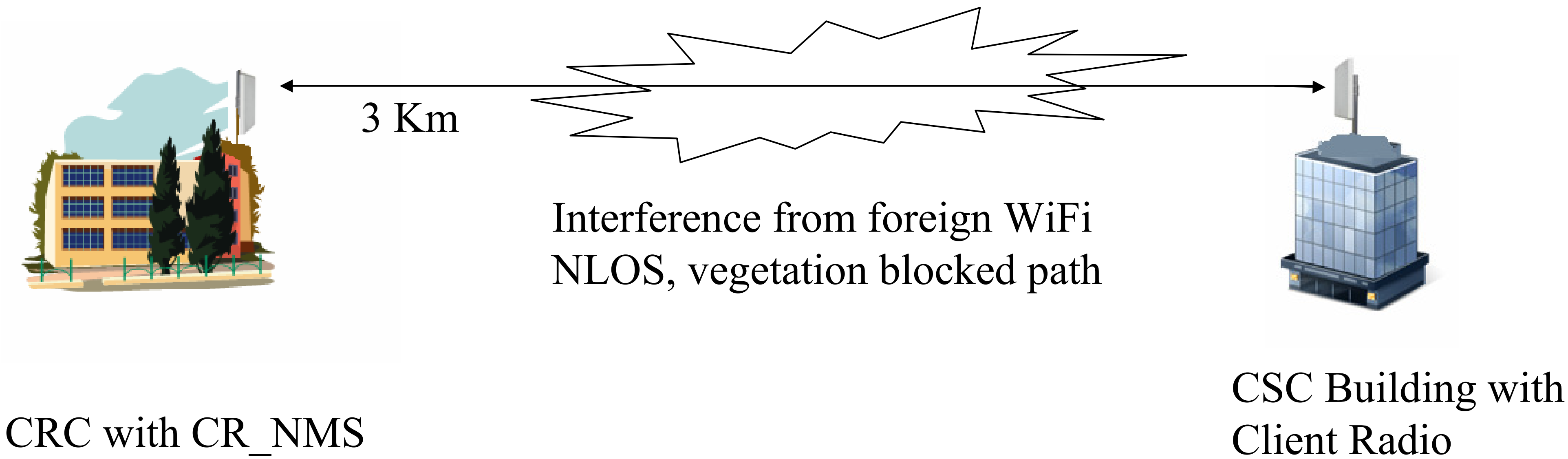


Top Graph: Correlation of beacons emanating from Terminal 1 as received at Terminals pairs {7,7},{7,6},{7,2},{7,3}
Bottom Graph: Correlation of beacons emanating from Terminal 4 as received at Terminals {7,7},{7,6},{7,2},{7,3}
60 Minute duration, distances between terminal pairs shown

Dynamic Spectrum Access

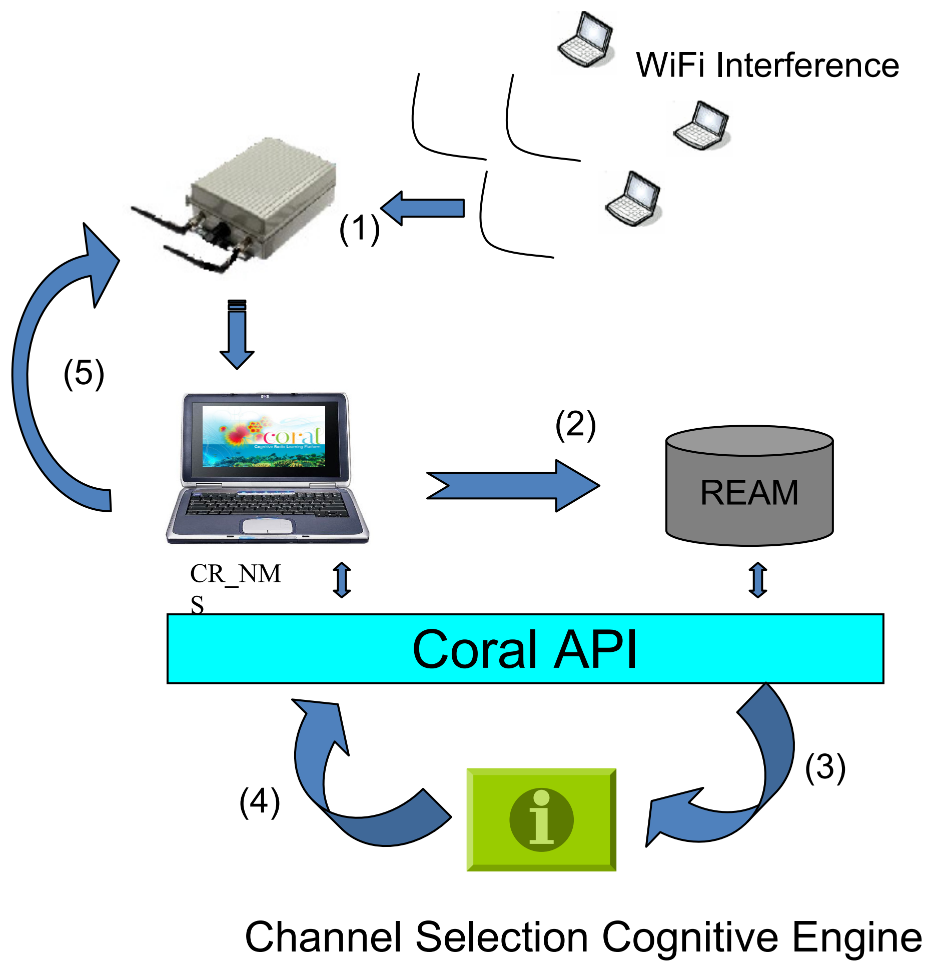
- Objective: Implement an algorithm that chooses the WiFi channel providing the best throughput in a long

  range point to point WiFi link.
- Approach: This DSA algorithm is to be based on the per channel interference energy and occupancy.



Dynamic Spectrum Access

- DSA Process
  1. CR NMS collects WiFi interference data from Coral terminals periodically
  2. Collected data are stored in database (REAM database)
  3. Channel selection application selects a best channel periodically according to the WiFi interference environment
  4. Application sends switch channel command to CR NMS when a better channel is selected other than current channel
  5. CR NMS sends command to AP to switch Channel



Dynamic Spectrum Access

▪ Algorithm

Selected Channel : $$\overset{*}{J} = \underset{j}{\text{argmax}} \{ \; IS_j(Ap)/2 + \sum_{k=1}^{N} (IS_j(Sta_k)/(2*N)) \}$$

The raw data representing the interference environment of CRN.

CRNMS Interference DB

Time	Channel	Node	RSSI (dbm)	Duration (us)	....
12:00	1	Ap	-70	2220	....
12:00	2	Sta_1	-81	4002	....
12:01	2	Sta_2	-75	12604	....
....	....	....	....	....	....

Step 1

Utilization for channel *j* is calculated as percentage of the total duration of WiFi interference packets over the total scanned time.

$$U_j = \left(\sum_{j=1,\, t=DT-DI}^{M,\, DT} (D_{j,t}) \right) \Big/ (STR * DI)$$

Energy for channel *j* is calculated as total energy that the WiFi interference packets have.

$$E_j = \sum_{j=1,\, t=DT-DI}^{M,\, DT} (D_{j,t} * 10^{(RSSI_{j,t}/10)})$$

Ap 12:00~12:05

Channel (j)	Utilization (U_j) (%)	Energy (E_j)
1	20	3.07
2	9	1.2
3	10	0.4
....	....	....

Sta_1 12:00~12:05

Channel (j)	Utilization (U_j) (%)	Energy (E_j)
1	10	2.028
2	6	0.34
3	3	0.205
....	....	....

Sta_2 12:00~12:05

Channel (j)	Utilization (U_j) (%)	Energy (E_j)
1	30	0.928
2	8	0. 49
3	11	1.705
....	....	....

...

Step 2

Interference Score (IS) for Channel *j*

$$IS_j = f(U_j) - g(E_j)$$

12:00~12:05 Interference Score Table

Channel	AP	Sta_1	Sta_2	....	Sta_k
1	70	80	50	....	....
2	84	88	70	....	....
3	80	90	60	....	....
4	87	95	90	....	....
5	90	93	88	....	....
6	83	85	79	....	....
7	91	87	87	....	....
8	98	91	92	....	....
9	89	95	94	....	....
10	77	82	90	....	....
11	60	77	87	....	....

Step 3

f and g are channel condition evaluation functions

Dynamic Spectrum Access

- Algorithm
  - The interference index is calculated as a weighted sum of each node's IS. The AP takes half the weight and each station shares equally for the other half

Step 3

Interference Index
12:00~12:05

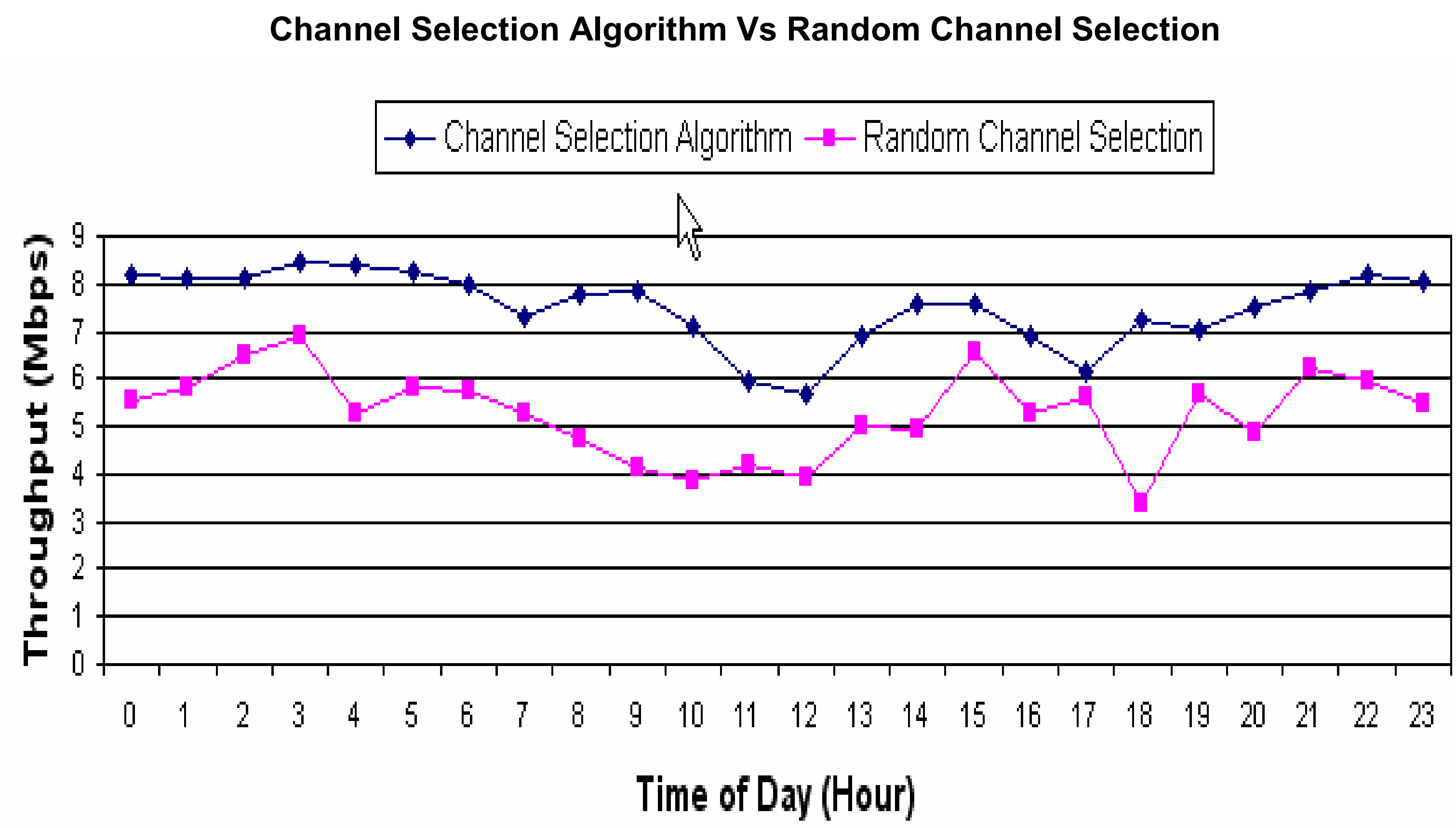
Channel (j)	Interference Index
1	71
2	85
3	83
4	87
5	90
6	79
7	88
8	95
9	94
10	89
11	68

$$\text{Interference Index}_j = IS_j(Ap)/2 + \sum_{k=1}^{N} \left(IS_j(Sta_k) / (2*N) \right)$$

$$\text{Selected Channel : } J^* = \underset{j}{\operatorname{argmax}} \left\{ IS_j(Ap)/2 + \sum_{k=1}^{N} \left(IS_j(Sta_k) / (2*N) \right) \right\}$$

  - The above weight scheme is designed for fairness. It can be changed for other special requirements, such as QoS; In this case, each station may have different weight according to its request for service

Dynamic Spectrum Access



Experiment was executed between CRC building 2and CSC building in August 11th, 2011

Future Work

- An improved multi-radio, multi-band WiFi_CR is in the works.
- Cognitive Femtocells
- Sub-700 MHz WiFi_CR for TVWS applications.
- Increasing collaborations: the more, the merrier…putting a practical spin on CR in the ISM environment.
- Moving into IEEE 802.11n; LTE, and beyond.

- Thank you….Questions?