Cognitive Radio Networking and Communication

AN OVERVIEW-PART II

University of Siena , 2014
VIPP Lab
Kassem M. Kallas

Outline

- User cooperative communication.
- IEEE 802.22 Standard
- Security Issues in Cognitive Radio

USER COOPERATIVE COMMUNICATION

- Users cooperate together to deliver data from source to sink through a relay in the middle.

- Benefits from cooperation:
    - -combat channel effects.
    - -increase link reliability.
    - -increase the throughput.
    - -save power.
    - -save spectrum resources.

USER COOPERATIVE COMMUNICATION

Relay Channels

- First introduced to increase the communication range and to solve the earth curvature problem(no LOS exists).

- Relaying can be of two modes:

  -**cooperative**: receiver combines relay and direct messages.

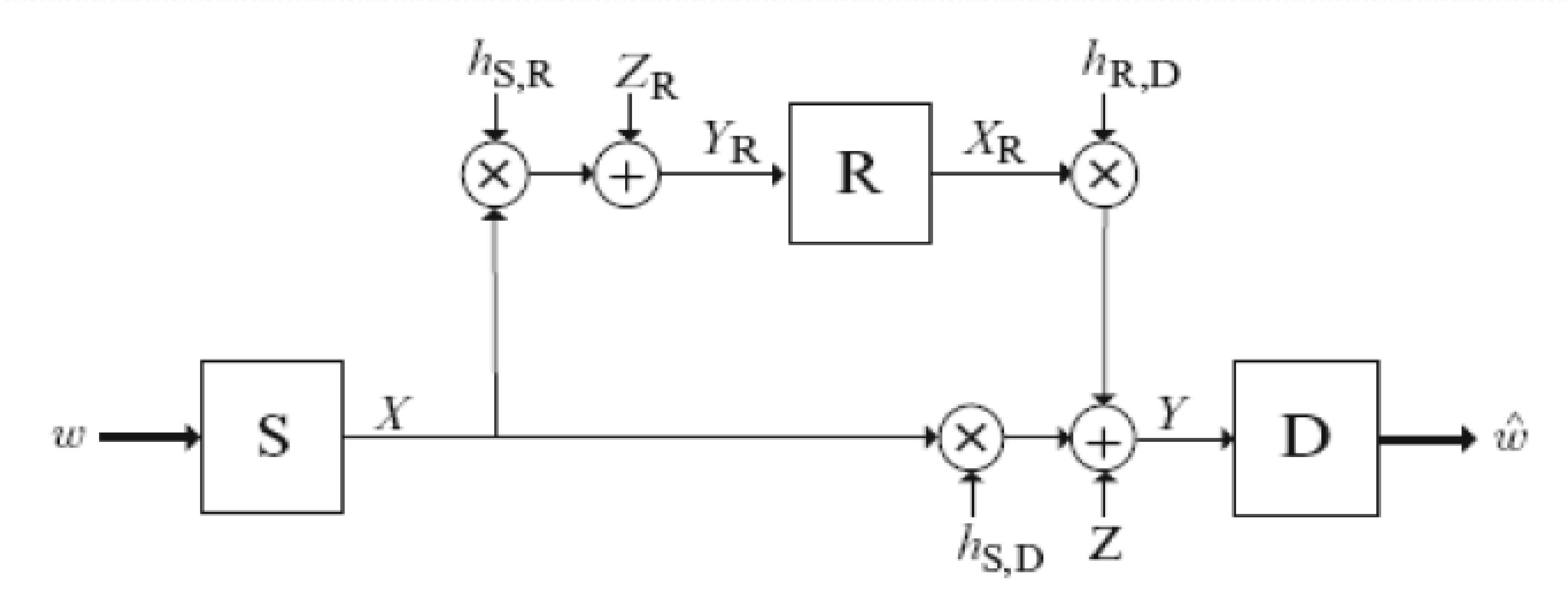
  -**non-cooperative**: receiver consider the direct link as noise or doesn't exist.

- Motivation:

  -Pr{deep fade at both relay and direct links at same time} << Pr{direct link only}.

USER COOPERATIVE COMMUNICATION

Relay Channels-**Three node model**



•Strategies for relaying:

-Amplify and Forward (noise will be amplified).

-Decode and Forward (more complex).

•The communication period will be divided to two parts: one for transmission and another for relaying of data.

USER COOPERATIVE COMMUNICATION

Relay Channels- **optimal relaying time**

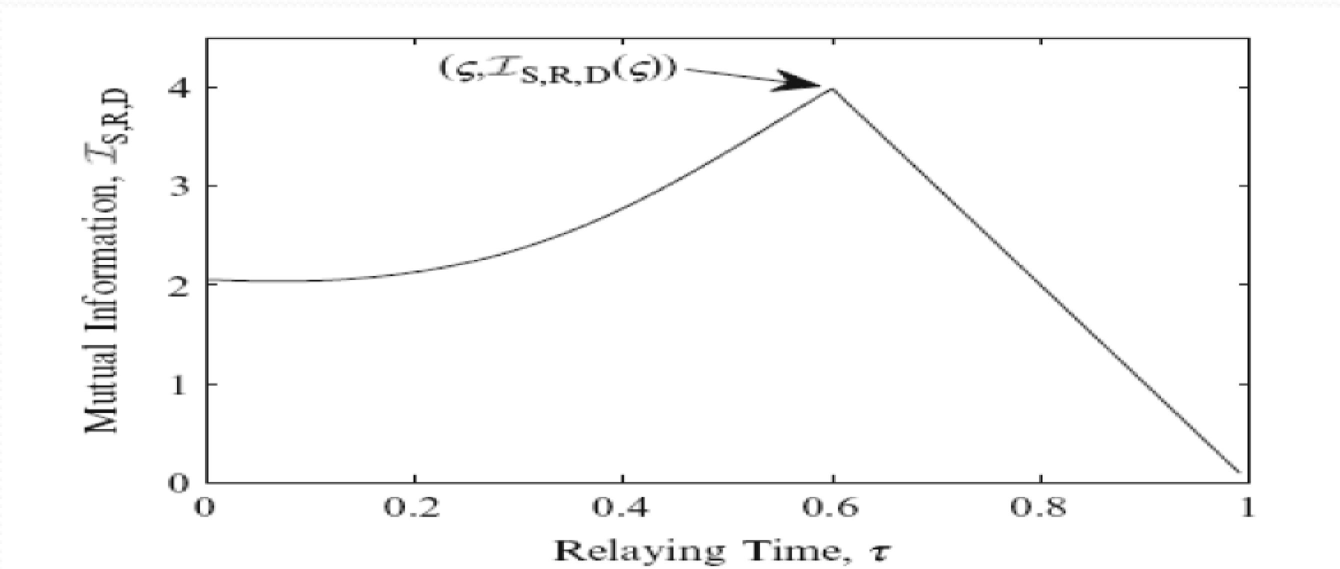
•**τ** is important: it affects the achievable rate and degree of cooperation between nodes.

-if **τ** =0 , no relaying.

-If **τ** =1 , no direct link.

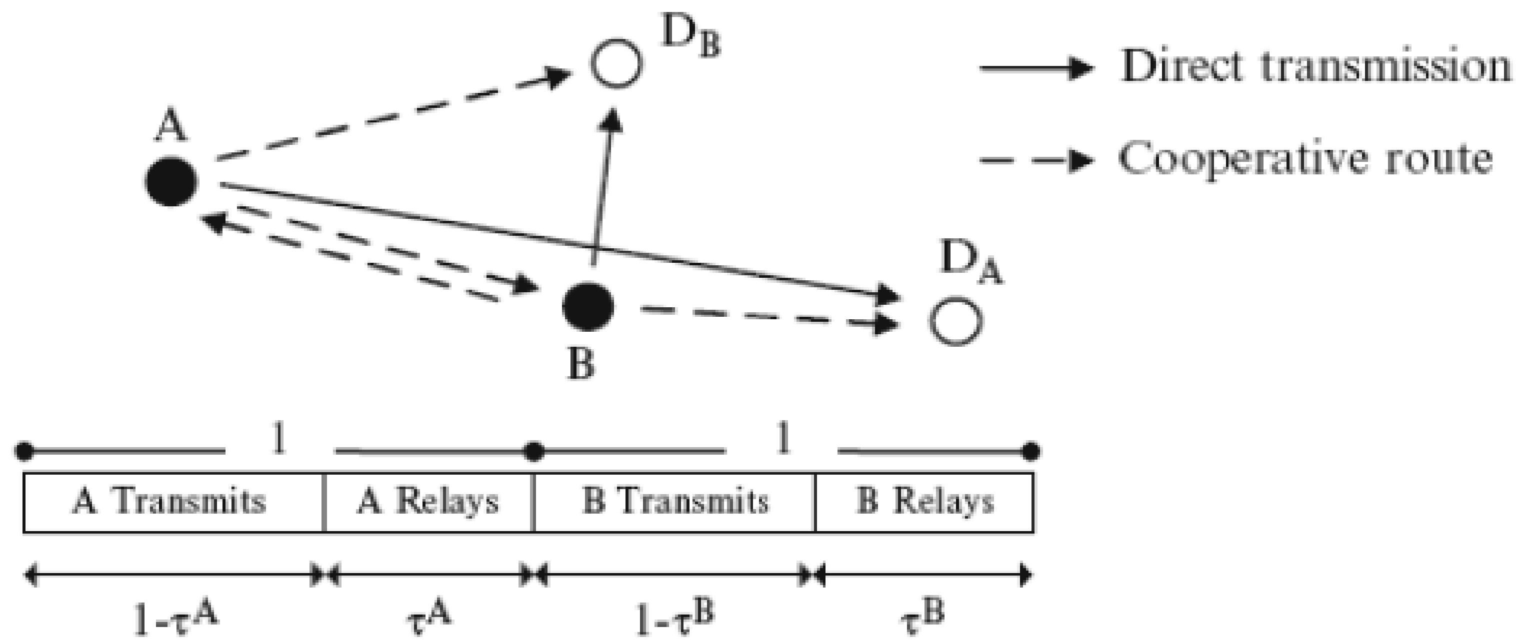
•To maximize the throughput, we need to choose optimal relaying time **τ**.

•The optimization problem is: $\mathbb{P}: \max_{0 \le \tau < 1} \mathcal{I}_{S,R,D}(\tau).$



USER COOPERATIVE COMMUNICATION

User cooperation in wireless networks-**two users model**



Network can have many sources, many destinations and all want to cooperate.

Ex:

•Two channels: (A,B, DA) and (B,A,DB).

USER COOPERATIVE COMMUNICATION

User cooperation in wireless networks, **partner selection**

<u>How nodes select a partner to cooperate?</u>

Suppose node A searches for partner B then(all these are done through message passing),

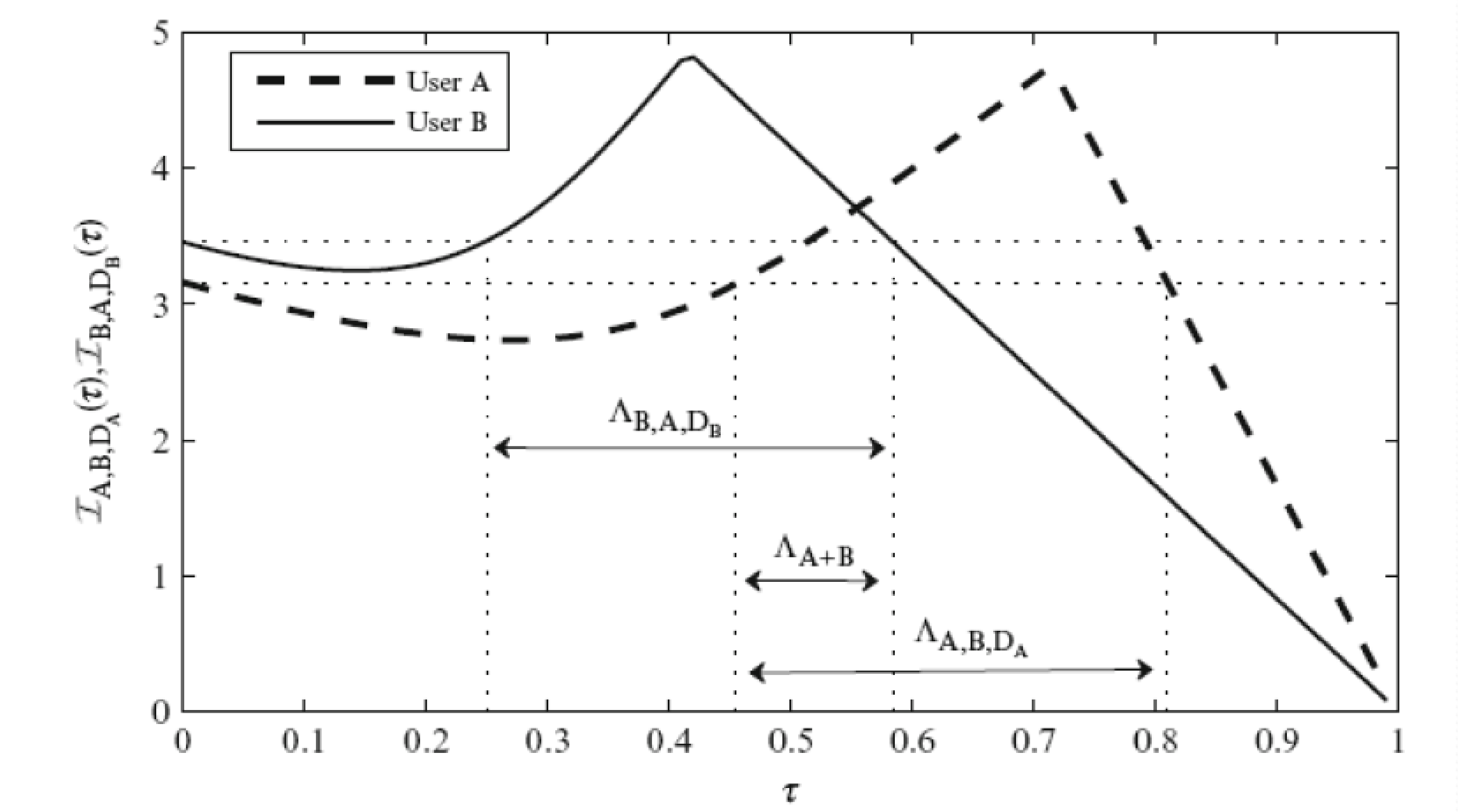
-A look for node B that gives a higher rate, means higher SNR than direct link(i.e. after A request message).

-A has a set of candidates but if B "good" for A, it doesn't mean A "good" for B(i.e. after A collecting the replies).

-solution: find all possible time allocations for both and see if common region exists.

USER COOPERATIVE COMMUNICATION

User cooperation in wireless networks, **partner selection**



IEEE 802.22 STANDARD

•FCC: allow the use of fallows in licensed TV band 54-862 MHz(UHF/VHF) by unlicensed users providing no harmful interference on PUs. It is a WRAN(Wireless Regional Area Network) standard that uses CR.

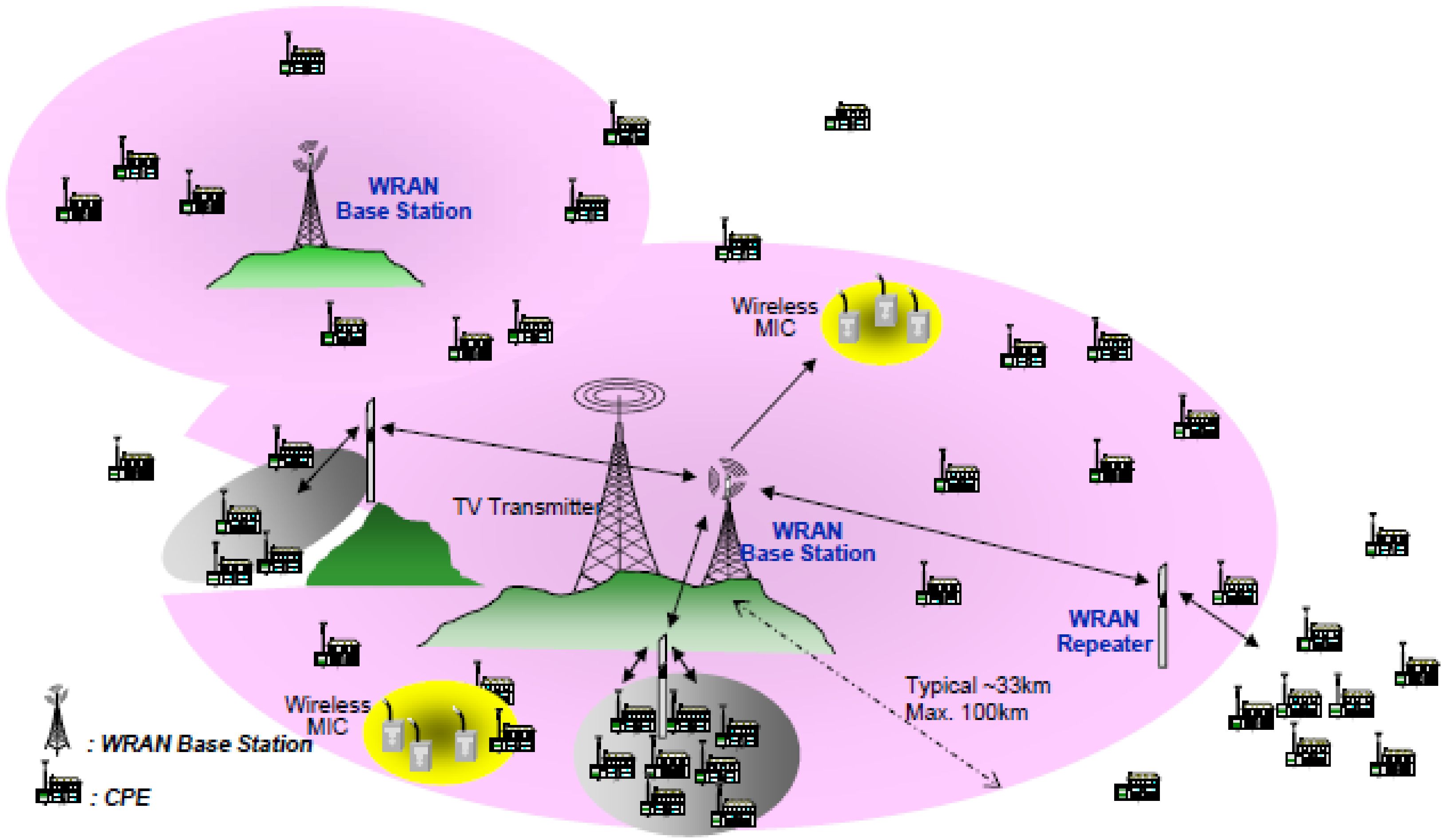
•Employing CR-based promising technology in WRANs , IEEE started the formation in November 2004.

•WRAN operates in rural areas (lower population density) and covers between 33 and 100 km.

•Entities in WRAN: Customer Premise Equipment(CPE) and Base Station(BS).

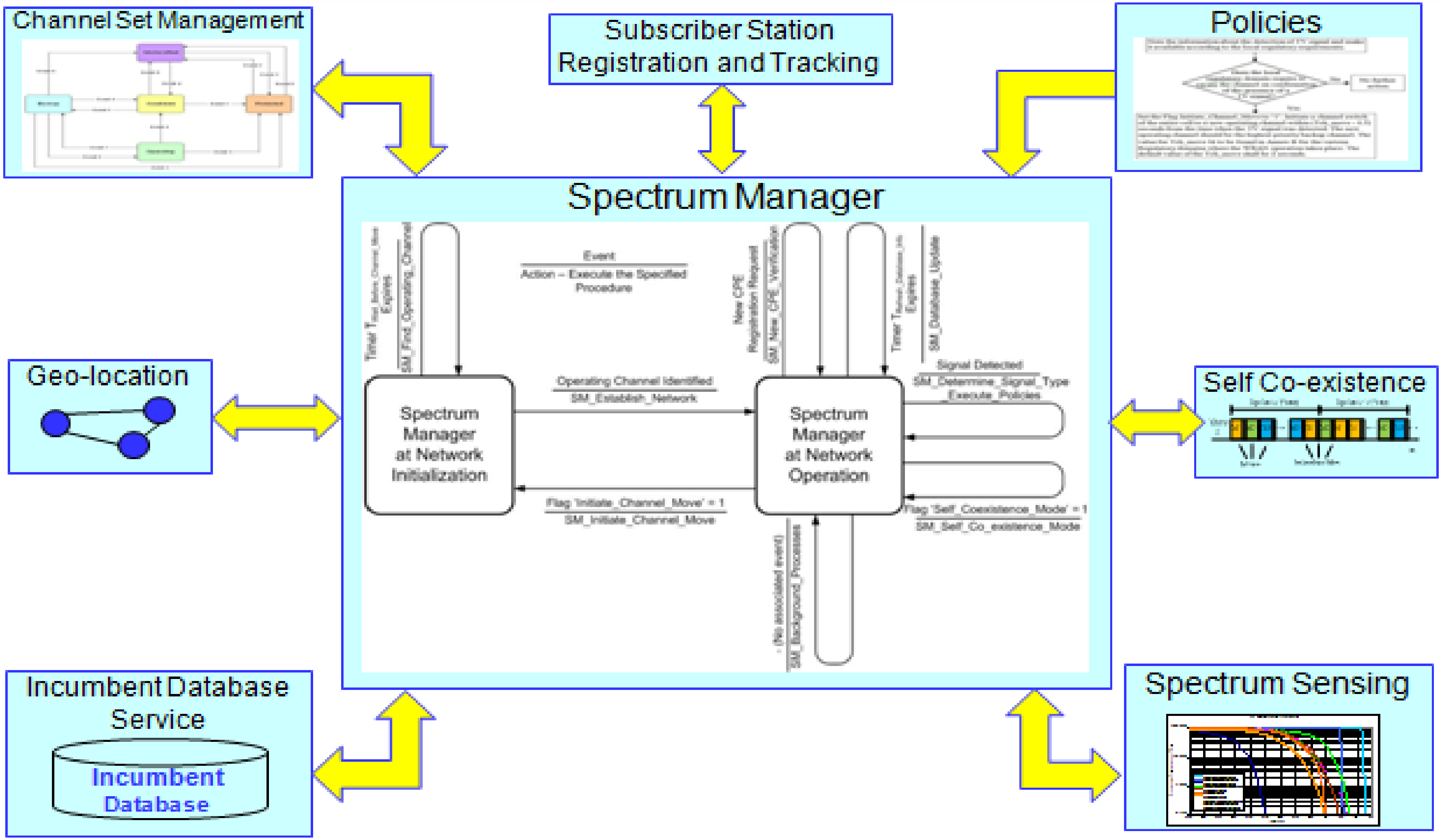
IEEE 802.22 STANDARD

Deployment Example



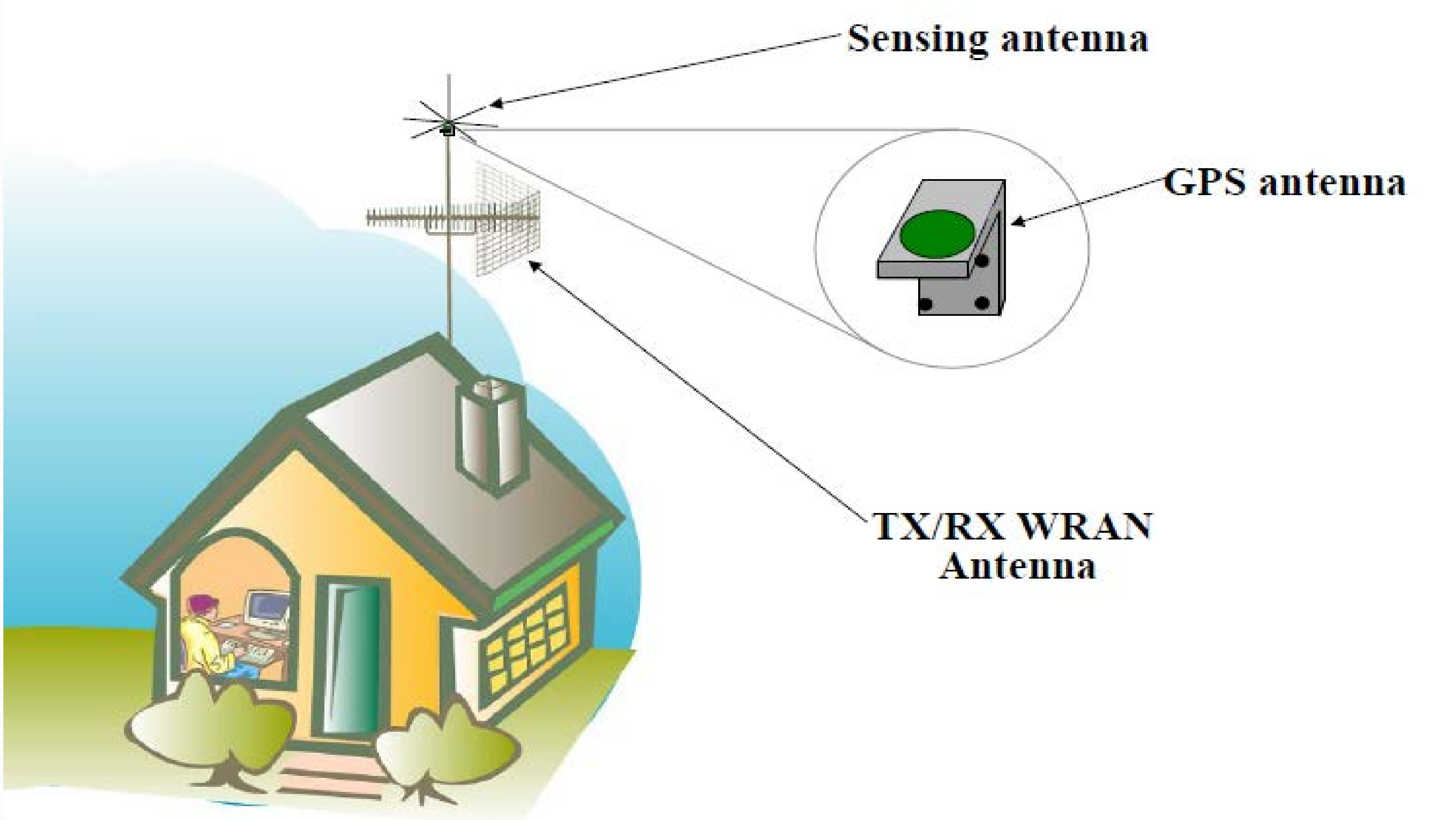
IEEE 802.22 STANDARD

CR capability



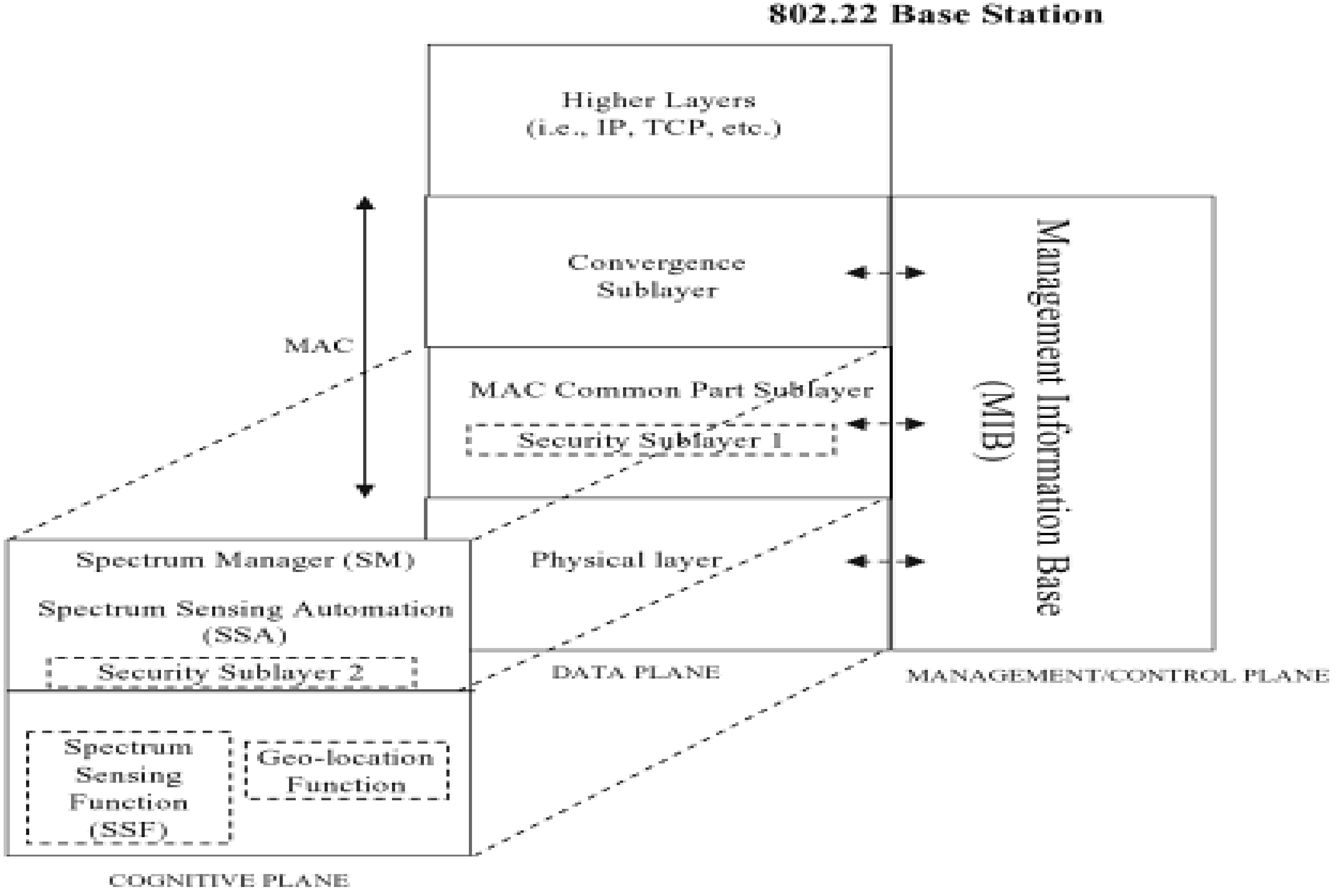
IEEE 802.22 STANDARD

CPE installation



IEEE 802.22 STANDARD

Reference architecture



IEEE 802.22 STANDARD

Physical layer

•Primary functions: main data communication, spectrum sensing, and geo-location.

•Multiple Access: OFDMA.

•Modulation: QPSK, 16-QAM, 64-QAM.

•MIMO can be used to enhance the throughput.

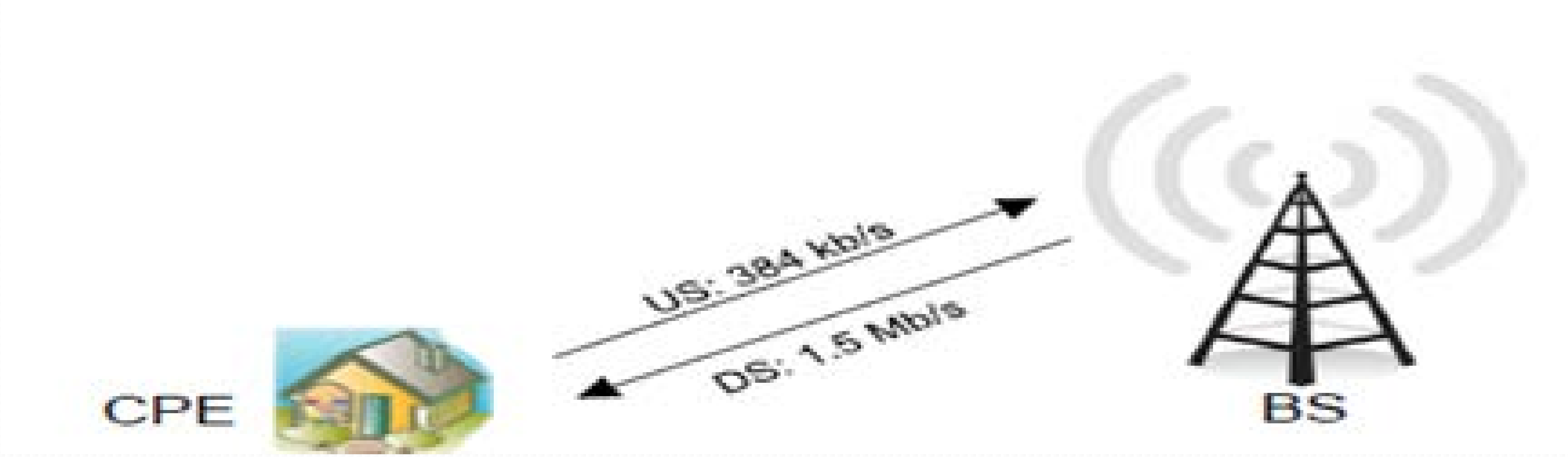
•Coding: convolutional code first, other options: LDPC, and Turbo with coding rates of 1/2 , 2/3, 3/4 and 5/6.

•Net. Spectral efficiency: from 0.624 bits/sec/Hz to 3.12 bits/sec/Hz.

•Preambles: for detection, synchronization, and channel estimation.

•Generation of preamble with low correlation to decrease the PAPR.

IEEE 802.22 STANDARD
Physical layer (cont.)



•Channel of 6 MHz to serve 255 devices/BS.

•Power control:

--regulatory specific.

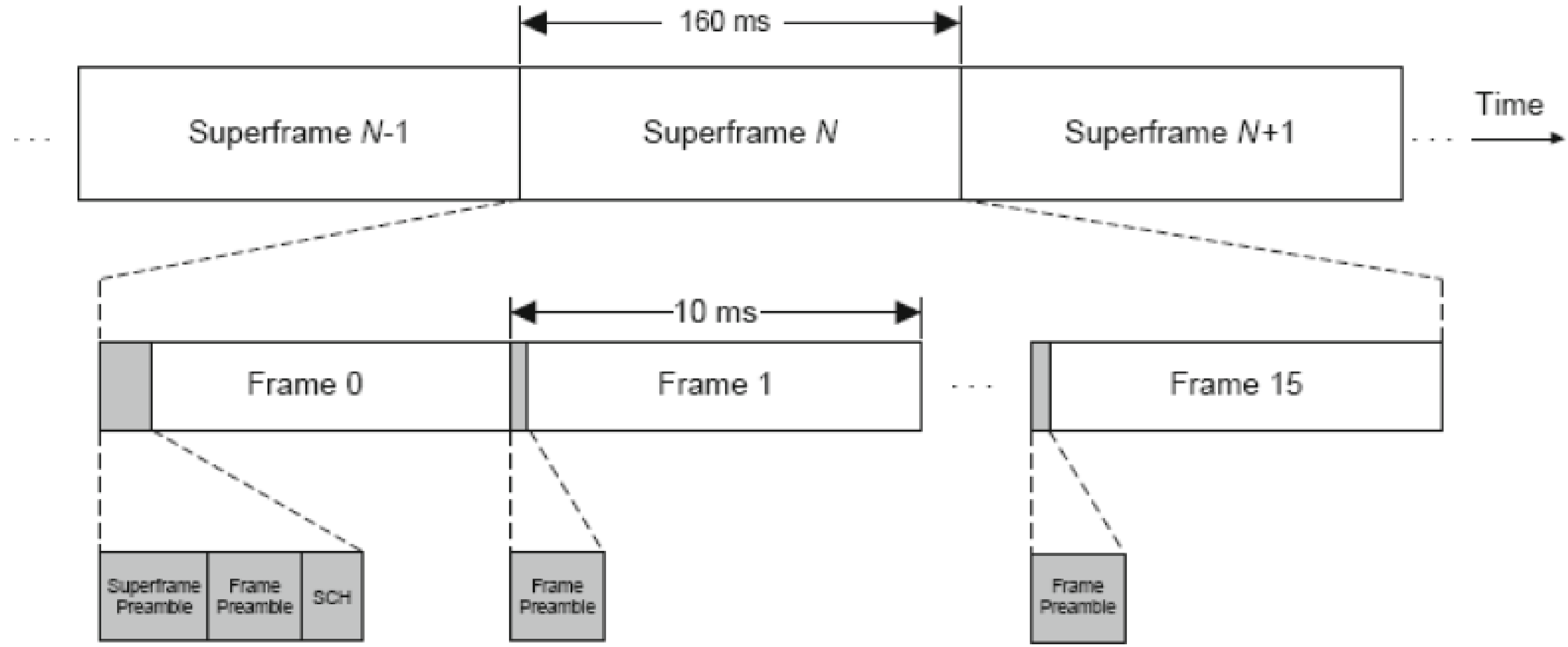
--CPEs obtain their transmission power level from BS.

-- 1 dB step power control with 0.5 dB resolution.

IEEE 802.22 STANDARD

MAC layer

•Inherited from 802.16 standard.



•Two structures: superframe and frame.

•TDD frame structure.

•Superframe preamble for synchronization, frame preamble for channel estimation, and SCH is the superframce control header.

IEEE 802.22 STANDARD
MAC layer-(cont.)

- Various QoS levels for flows at MAC:

QoS	Application
UGS (unsolicited grant service)	VoIP
rtPS (real-time polling service)	MPEG video Streaming
nrTPS(non-real-time polling service)	FTP
BE(best effort)	E-mail
Contention	BW request

IEEE 802.22 STANDARD

MAC layer-(cont.)

•Cognitive functionalities:

-Dynamic and adaptive scheduling of Quite Periods (QPs) used as sensing periods for Incumbent detection.

-Two sensing durations: fast(1 ms/channel) and fine(25 ms/channel),depends on the fast the BS decide if the fine sensing is needed or not.

-CPE can alert BS about Incumbent existence(detecting PU signal): using UCS(urgent coexistence) notification or low priority MAC messages.

-FCH(frame control header) messages used by BS when it wants one or more subscribers to move their channels.

- SCH(superframe control header) carries information about BS MAC address, silent periods(QPs), and channels can be used by CEPs when turned on.

IEEE 802.22 STANDARD

Incumbent detection

Different techniques:

1. Quite Periods (QPs).

2. Channel measurement management(to report incumbent detection):
   -even out of QPs.

3. Synchronization between CPEs and BS:
   -avoid interference in the sensing and detection phase.
   - No transmission during QPs.

4. Geo-location:
   -Geo-location of BS and CPE has to be known.
   -Incumbent DB are maintained by regulatory bodies to keep the information of licensed TV operation in any given geographical location.

IEEE 802.22 STANDARD

Coexistence

•Two types:

-incumbent coexistence: between PU and SU.

-self-coexistence: co-existence of similar networks(WRANs).

•Self-coexistence problem is addressed by:

1. Network discovery and coordination: at the setup phase, using SCH sent by BS and CPE reports to BS(to know the CPEs inside the cell controlled by such BS).

2. Coexistence Beacon Protocol (CBP): BS sends packets that contain information about cell, backup channels. Coexisting BSs generate random numbers and the one with highest win the channel.

IEEE 802.22 STANDARD

Channel Classification

- Available: not occupied by TV transmitter.
  - -Disallowed: Due to local regulation(i.e. used by police).
  - -Operating: Currently used by the BS.
  - -Backup: In the Backup list of the BS(if PU return on operating channel).
  - -Candidate: For backup.
  - -Occupied: used by other WRANs.
  - -Unclassified.

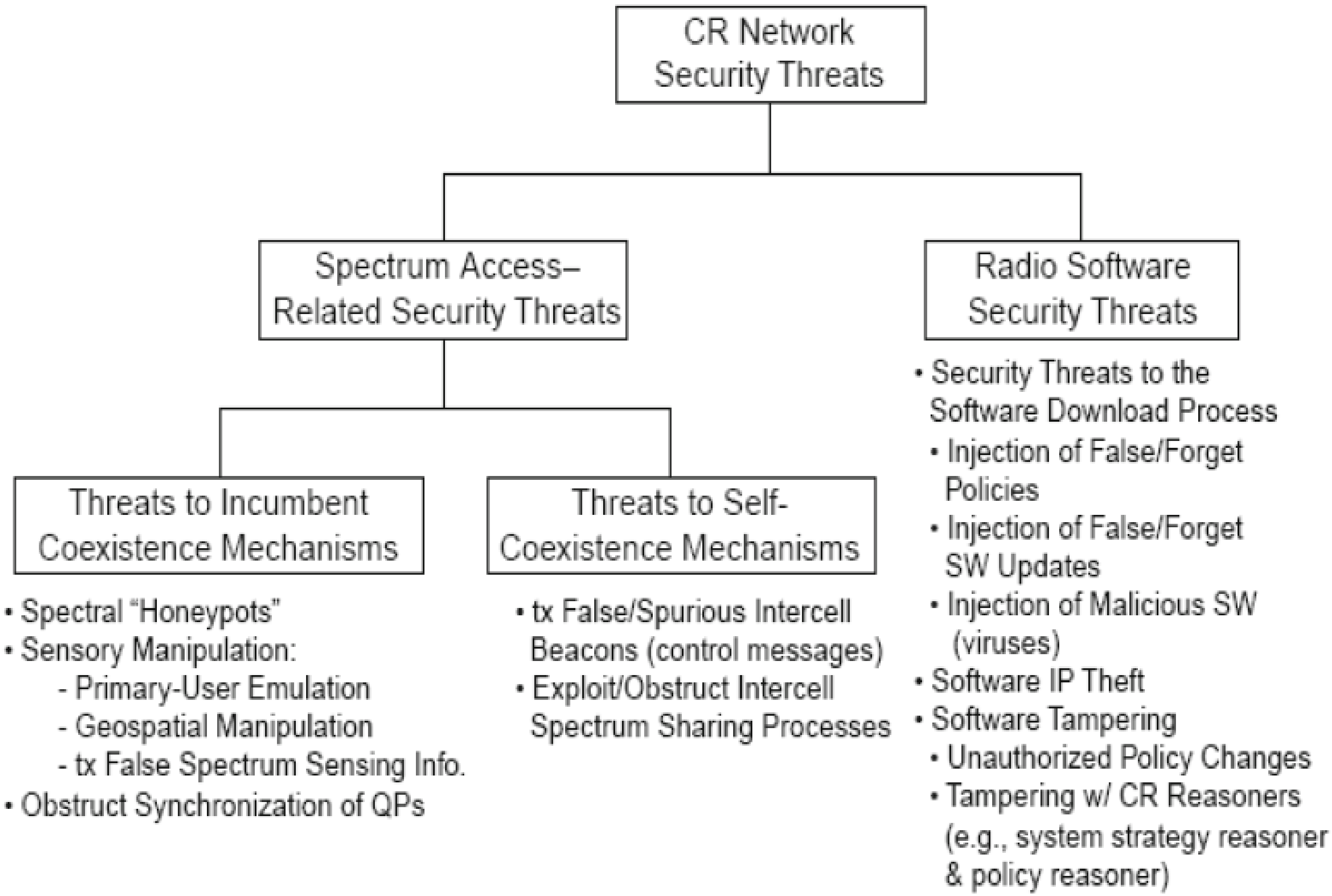
- Not available: currently occupied by TV transmitter.

- Channel termination, switch, add, and QP is done between BS and CEPs on request/response basis.

The complete documentation for the standard is found at:

[1]:http://www.ieee802.org/22/

SECURITY ISSUES IN COGNITIVE RADIO



SECURITY ISSUES IN COGNITIVE RADIO

Security Threats in Self-coexistence

•In IEEE 802.22, coverage areas of WRANs may overlap and may decrease the network throughput.

•Problem addressed by Inter-cell synchronization using beacons and by Inter-BS dynamic resource sharing at MAC level by random number selection .

-the attacker can involve and choose very high number each time and win the channel and BS loose.

•If inter-cell communication is not feasible, BS gather control info. about the other cell from CPEs in the overlapping area using CPE beacons.

•Beacons are not protected in IEEE 802.22 SSL.

-vulnerable to forgery (beacon falsification attack), replay, modification.

SECURITY ISSUES IN COGNITIVE RADIO

Security Threats in Incumbent coexistence

•Spectrum sensing is essential and must be trustworthiness as it is the primary functionality of cognitive device.

•Two types of attacks:

1. Primary user emulation attack (PUE).

2. Spectrum Sensing Data Falsification attack (SSDF).

SECURITY ISSUES IN COGNITIVE RADIO

PUE attack, Incumbent Coexistence

•FCC states that: no modification is allowed to PU signal to accommodates SU unlicensed spectrum usage.

•The attacker tries to emulates the characteristics of the primary user signal.

•Classification of PUE attacks depends on the motivation of the attacker:

-Selfish PUE attack: The attacker wants to maximize its own spectrum occupancy.
-Malicious PUE attacks: It is a DoS attack to prevent legitimate users from detecting the existence of spectrum holes.

SECURITY ISSUES IN COGNITIVE RADIO

PUE attack, **solutions**

Reference	Contribution
Ref.[2]	For IEEE 802.22 standard specifications: -Detection of attacker is based on testing the signal characteristics, the location of PU, and the power level. -Then, trying to obtain the attacker location if detected.
Ref.[3]	Derives analytical model for power received from attacker: -Two PDFs: for attacker and for real PU signals. -Two hypothesis(H0 and H1) on the PDFs and decide using a threshold.

[2]: *Alexander M. Wyglinski, Ph.D., Maziar Nekovee, Ph.D., and Y. Thomas Hou, Ph.D*, "Cognitive radio network security," Cognitive Radio Communications and Networks. Elsevier Inc, 2010, ch. 15, sec. 15.2, pp. 437-441

[3]: Z. Jin and K. Subbalakshmi, "Detecting Primary User Emulation Attacks in Dynamic Spectrum Access Networks," in *Proc. ICC, 2009,* pp. 1–5.

SECURITY ISSUES IN COGNITIVE RADIO

PUE attack, **solutions**

Reference	Contribution
Ref.[4]	Using channel impulse response as "**link signature**" : -Obtain the PU link signature from a **helper node** very close to PU. -Helper node has to check: it calculates the ratio between 1st and 2nd components of multipath signal and if above threshold → PU real signal. -SU compare the distance in link signature between the signal under test and the signal from helper node and set a threshold, if the distance is below→ PU real.

[4]:Y. Liu, P. Ning, and H. Dai, "Authenticating Primary Users' Signals in Cognitive Radio Networks via Integrated Cryptographic and Wireless Link Signatures," in *Proc. 2010 IEEE Symposium on Security and Privacy, 2010,pp. 286–301.*

SECURITY ISSUES IN COGNITIVE RADIO

PUE attack, **solutions**

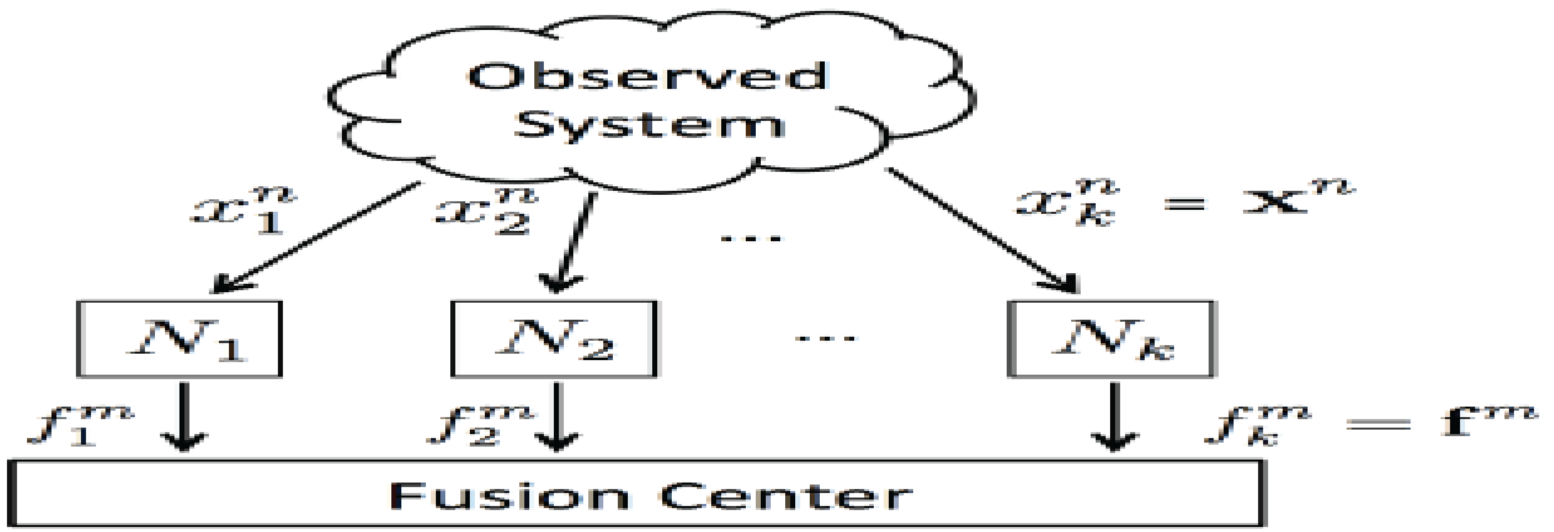
Reference	Contribution
Ref.[5]	Using public key cryptographic approach (breaks the FCC rule): -digital signatures using public key cryptography within PU signal. In turn, SU verifies the signature using secondary BS. -secondary BS with the aid of certification authority verify the signature. -it is weak to DoS attack during QPs.

[5]:C. Mathur and P. Subbalakshmi, "Digital signatures for centralized DSA networks," in *Proc. 1st IEEE Workshop on Cognitive Radio Networks, 2007, pp. 1037–1041.*

SECURITY ISSUES IN COGNITIVE RADIO

SSDF attack, Incumbent Coexistence

•Failure in context of data fusion(attacker or misbehaving nodes).
•Two modes: **centralized and distributed**.
•Fusion rule: AND, OR, and Majority…
•FC may take inappropriate decisions, and then resulting in:
 -underutilization of spectrum.
 -increasing interference to incumbent users.
•Attacker types: Malicious, Greedy, and Unintentionally.
•DSS model in **centralized** mode:



SECURITY ISSUES IN COGNITIVE RADIO

SSDF attack – **solutions, Binary type reports**

Reference	Contribution
Ref.[6]	Based on a reputation metric: -if the node report mismatch with FC result, the metric increases. -smaller the metric, more reliable the node. -if the node exceeds a threshold, it will be isolated.
Ref.[7]	**Improvement over**[7]: restoring the metric for temporary misbehaving nodes to be more fair with honest nodes.

[6]: A. Rawat, P. Anand, H. Chen, and P. Varshney, "Countering byzantine attacks in cognitive radio networks," in *Proc. ICASSP, 2010, pp. 3098*–3101.

[7]: W. Wang, H. Li, Y. Sun, and Z. Han, "Attack-proof collaborative spectrum sensing in cognitive radio networks," in *Proc. CISS, 2009,* pp. 130–134.

SECURITY ISSUES IN COGNITIVE RADIO

SSDF attack – **solutions, Binary type reports**

Reference	Contribution
Ref.[8]	Considers "**hit and run**" intelligent attacker: -attacker knows the fusion technique of the FC. -deviates between honest and lying modes. -it has its own suspicious level(if below a threshold ***h:*** malicious mode). -**detection method**: assign a point to the node each time exceeds ***h.*** -when the number of points exceeds a threshold, node removed permanently.

[8]: E. Noon and H. Li, "Defending against hit-and-run attackers incollaborative spectrum sensing of cognitive radio networks: A pointsystem," in *VTC, 2010, pp. 1–5*.

SECURITY ISSUES IN COGNITIVE RADIO

SSDF attack – **solutions, Continuous type reports**

Reference	**Contribution**
Ref.[9]	Proposes to divide the grid of sensors into clusters: -nodes in different clusters sends their RSS along with their locations to the FC. -two phases: 1. pre-filtering: examining similarities in the conditional probability density function(CPDF) of the power for nodes belong to same cluster . If the node lies between two defined thresholds → considered as legitimate . 2. weighted gain combining: assign a weight to each node based on its CPDF and then FC accumulates the reports to announce about the spectrum occupancy.

[9]: A. Min, K. Shin, and X. Hu, "Attack-tolerant distributed sensing for dynamic spectrum access networks," in *Proc. ICNP, 2009, pp. 294–303*.

SECURITY ISSUES IN COGNITIVE RADIO

SSDF attack – **solutions, Continuous type reports**

Reference	Contribution
Ref.[10]	Ad-hoc approach(decentralized mode): -The SU decision depends on its own measurements as well as the others. -Its own observations are more trusted than any other node. -the **detection** based on deviation from a mean value of the reports. -Users with max. deviation are assumed attacker and their input ignored in the decision.

state of art found at:[11].

[10]: F. Yu, M. Huang, Z. Li, and P. Mason, "Defense against spectrum sensing data falsification attacks in mobile ad hoc networks with cognitive radios," in *Proc. Milcom, 2009, pp. 1–7.*

[11]: A. G. Fragkiadakis, E. Z. Tragos, I. G. Askoxylakis, "A Survey on Security Threats and Detection Techniques in Cognitive Radio Networks," IEEE COMMUNICATIONS SURVEYS & TUTORIALS, vol. 15, no. 1, First quarter 2013.

SECURITY ISSUES IN COGNITIVE RADIO

Radio Software Threats

•The software suffers from attacks due to its high re-configurability.

•Three classes of attacks on the radio software:

-illegal software cloning(illegal copying).

-unauthorized software tampering(editing the software).

-threats related to software download.

•The tampering is dangerous because the attacker can play with the radio parameters. For example generate high interference on PU by increasing the transmission power.

•"obfuscation"(create noisy vision) can **resist** the tampering: It is a reverse engineering that transform the software code to a code less understandable.

•Tamper resistance techniques can be used to **detect/prevent** violation (non-authorized editing) of the original software.

•Obfuscation and tamper resistance can be used together.

SECURITY ISSUES IN COGNITIVE RADIO

Radio hardware security

•The isolation between hardware and software is the most important for hardware security to check software commands before hardware responding.

Reference	Contribution
Ref.[12]	Secure Radio Middleware(SRM): -a software resides between hardware and software sides and using policies, it checks all the software request that wants to change the radio parameters.

[12]: C. Li, A. Raghunathan, and N. Jha, "An architecture for secure software defined radio," in *Proc. Date '09, 2009, pp. 448–453.*