Lecture 11

Wireless Network Operations - I

Cell Search and Radio Resource Management

Some questions

- How does a MS know what BS is serving an area, what frequencies, time slots or codes it can use with this BS?
  - Cell search
- How does a MS know which BS, frequencies, time slots or codes are the "best" to use?
  - Radio resource management
- How does the network know where to route calls or packets for a MS?
  - Mobility (Location) Management
- How does a BS know whether it "can" provide service to a MS and what services are allowed? How do you authenticate an MS? How do you bill an MS?
  - Authentication, authorization, accounting
- So, should a MS be on all the time and monitor the channel all the time?

+ Wireless Network Operations

- Cell Search and Registration
  - How does a mobile station know "how to connect" to the network?
- Radio Resource Management – RRM
  - Deals with power control, channel assignment and handoff decisions
  - Includes Power Management – PM
    - Deals with protocols and management for allowing MSs to save power
- Mobility Management – MM
  - Deals with location management and handoff management
- Authentication, authorization, and accounting – AAA
  - Deals with security, billing and access control
- Location Services
  - Deals with E-911 and other positioning aspects

Cell Search and Registration

- **Cell Search**
  - When a MS is first powered on, it has to find base stations or access points
  - Procedures vary by the technology
- General idea
  - You have a "beacon" signal to help the MS
  - Beacon, *n*. "a fire or light set up in a high or prominent position as a warning, signal, or celebration"[1]
- Challenges
  - Frequency channels and quality
- **Registration**
  - MS needs to let the network know that it is "active" and can be now reached
  - Messaging between MS and network
- It is complex!
  - What if the MS is connecting at a place very different from the last time?
  - What if a MS cannot find its own service provider, but a different one?

[1]Mac OS X Dictionary

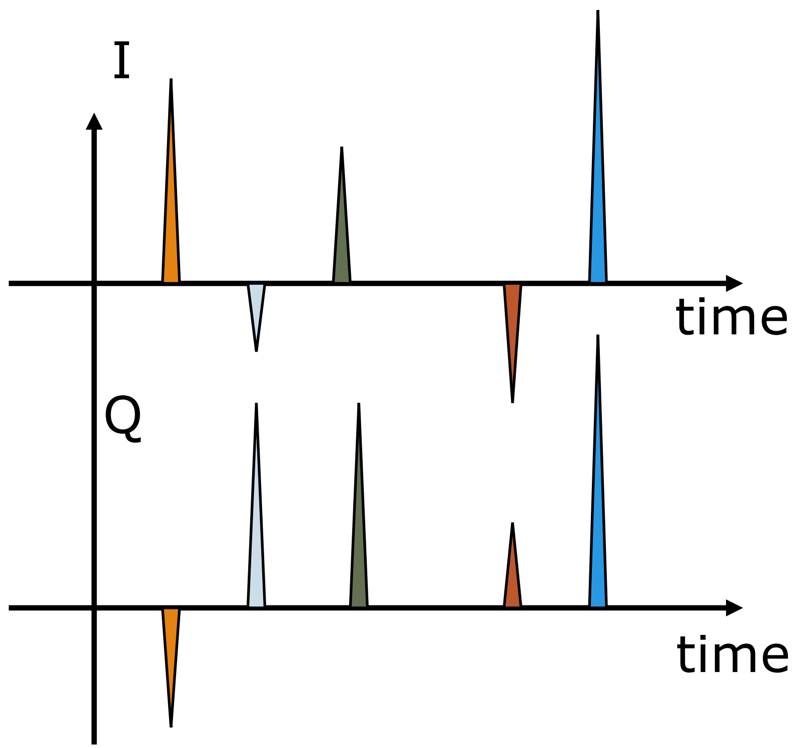
+ In Brief: Cell Search/Registration in AMPS

- AMPS has 30 kHz channels
  - 395 voice and 21 control channels
- MS looks for the “forward” control channels
  - Picks the strongest control channel
- Control channel
  - Broadcasts system ID and other types of information
  - MS needs to decode this information and see who it is connected to
  - If decoding fails, it is common to pick up the next strongest control channel
- MS transmits its ID and some other information on the reverse control channel to register with the network
  - Actual procedure is more complex than this

+ In Brief: Cell Search/Registration in GSM

- Cell search (Time multiplexed channels)
  - MS scans RF carriers and picks up the strongest it can sense
  - "Framing"
  - Uses an unmodulated carrier (all zeros) to synchronize the frequency (frequency correction channel – FCCH)
  - Use a synchronization channel (SCH) to get the timing for TDMA
- Beacon is the Broadcast Control Channel (BCCH)
  - Sends synchronization parameters, cell ID, etc.
  - It is decoded next to get information about the system/network
- A registration procedure follows
  - Many messages are exchanged to convey information about the mobile to the network and vice versa

+ In Brief: Cell Search in IS-95



Search correlator output:
5 strong signals have been detected

- Primary and Secondary Carriers – used in all cells
  - Remember – reuse = 1
- Pilot channel on primary carrier is tracked first
  - The MS processes the pilot channel to find the strongest signal
  - A search correlator sweeps through all possible pilot chip offsets to identify BSs in the area
- The MS picks the strongest pilot signal
  - This has a “PN-offset” that essentially identifies the cell
  - The MS uses the PN-offset of this pilot to track the synch channel and register

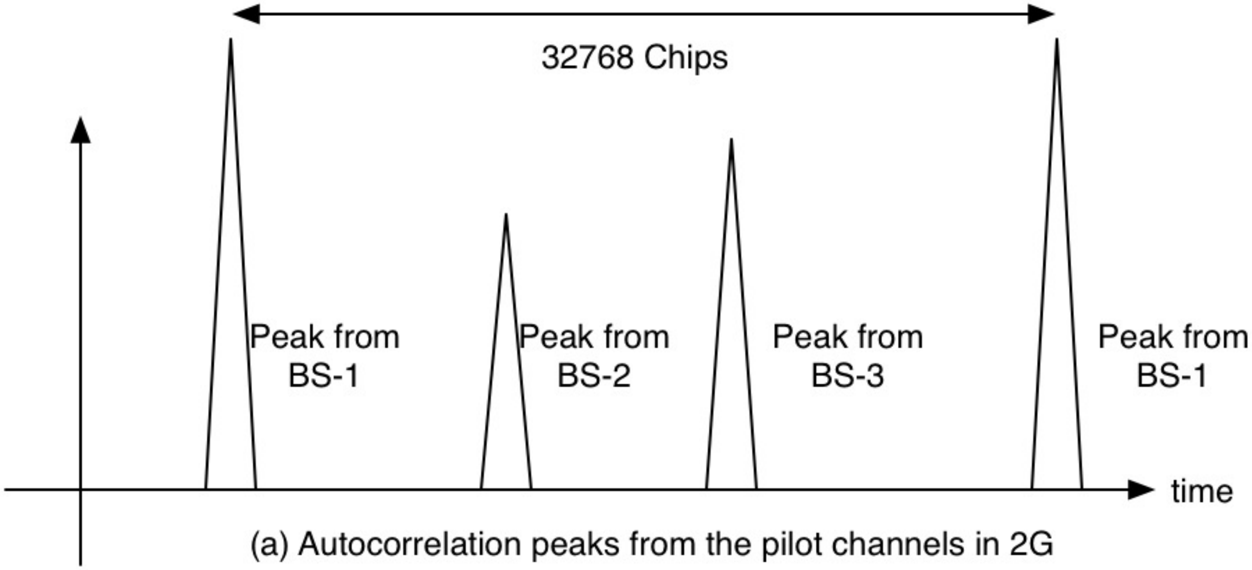
Cell Search Procedure in 3G UMTS

- In IS-95 how is the cell search procedure?
- In UTRA
  - No BS synchronization
  - Same PN code is NOT used in all cells
    - Different scrambling codes in different cells
    - Cannot search for 512 different codes of duration 10 ms each easily
    - Too many comparisons and correlations
  - It is a difficult problem
- The pilot channel is NOT used for cell search in UTRA
  - Instead the SCH is used in a different way

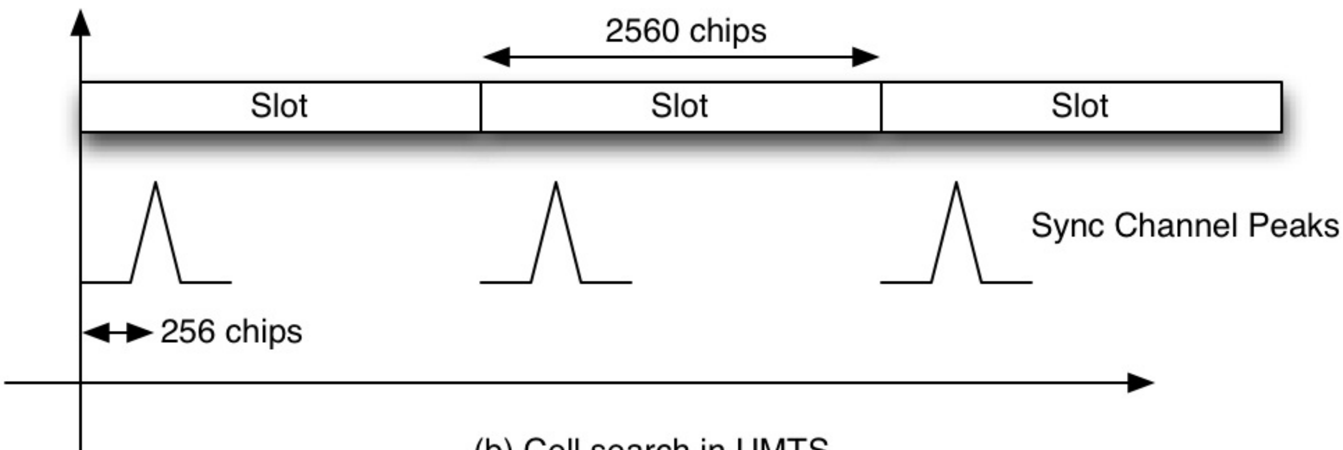
Cell search procedure – II

- Step 1: The primary SCH code is the same for all cells
  - It is the same in each slot
  - Detection of a peak can be used to determine the slot boundary
- Step 2: Detection of secondary SCH code
  - The MS seeks the largest peak among 64 secondary SCH codes also of length 256 chips
    - Scrambling codes are divided into 64 code groups
  - It needs to check this in each of the 15 slots that make up a frame
  - Once the secondary SCH code is picked up
    - The code group is known
    - There is frame synchronization as well
- Step 3: Each code group has 8 primary scrambling codes
  - The MS tests each of these codes over the duration of the frame to determine the correct code
  - For this, it employs the CPICH

Cell search in UMTS Vs IS-95



(a) Autocorrelation peaks from the pilot channels in 2G

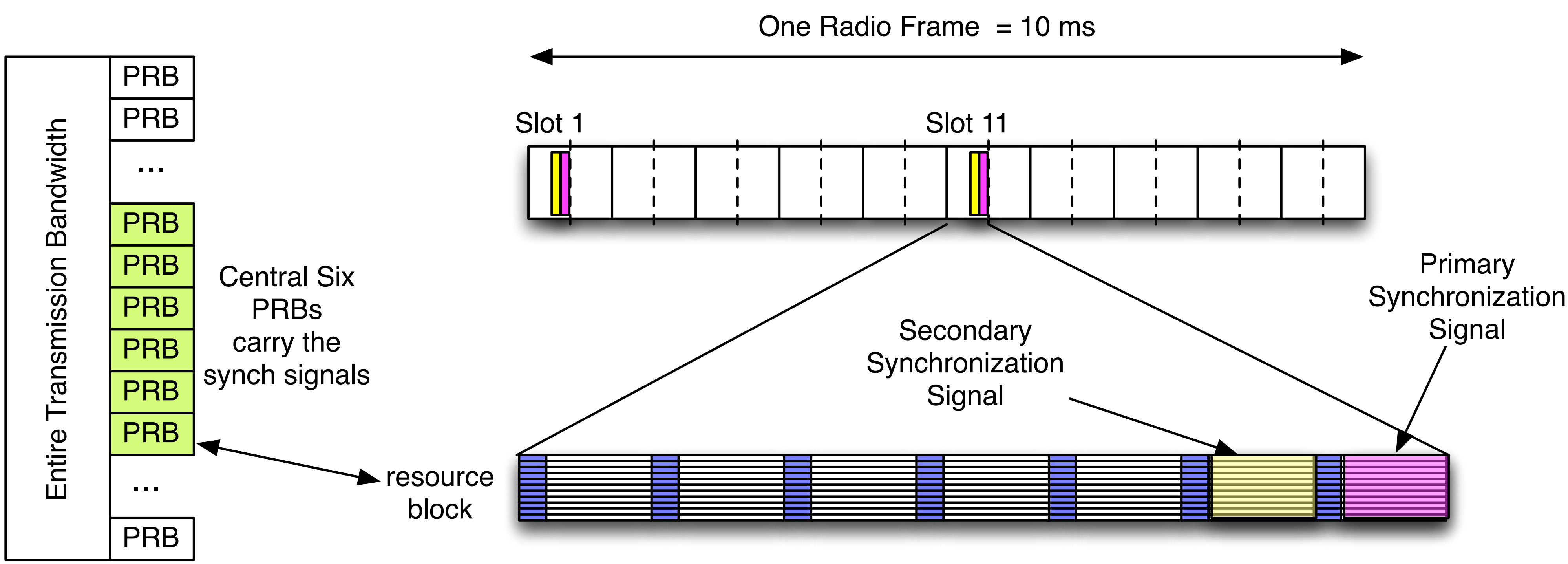


(b) Cell search in UMTS

In Brief: Cell Search in LTE

- OFDMA and time/frequency resource blocks (RBs)
- Problems
  - Different bandwidths supported in LTE (1.25, 2.5, 5, 10, 20 MHz)
  - Need smaller delay for cell search
- Sync Channel
  - Uses "central" 1.25 MHz bandwidth
  - Comprises of 76 sub-carriers with a spacing of 15 kHz
  - Within these, a primary (P-SCH) and secondary (S-SCH) synchronization channel is transmitted
    - Each carries part of the Cell-ID
- Reference Signal (RS)
  - Used for downlink channel estimation

Cell Search in LTE

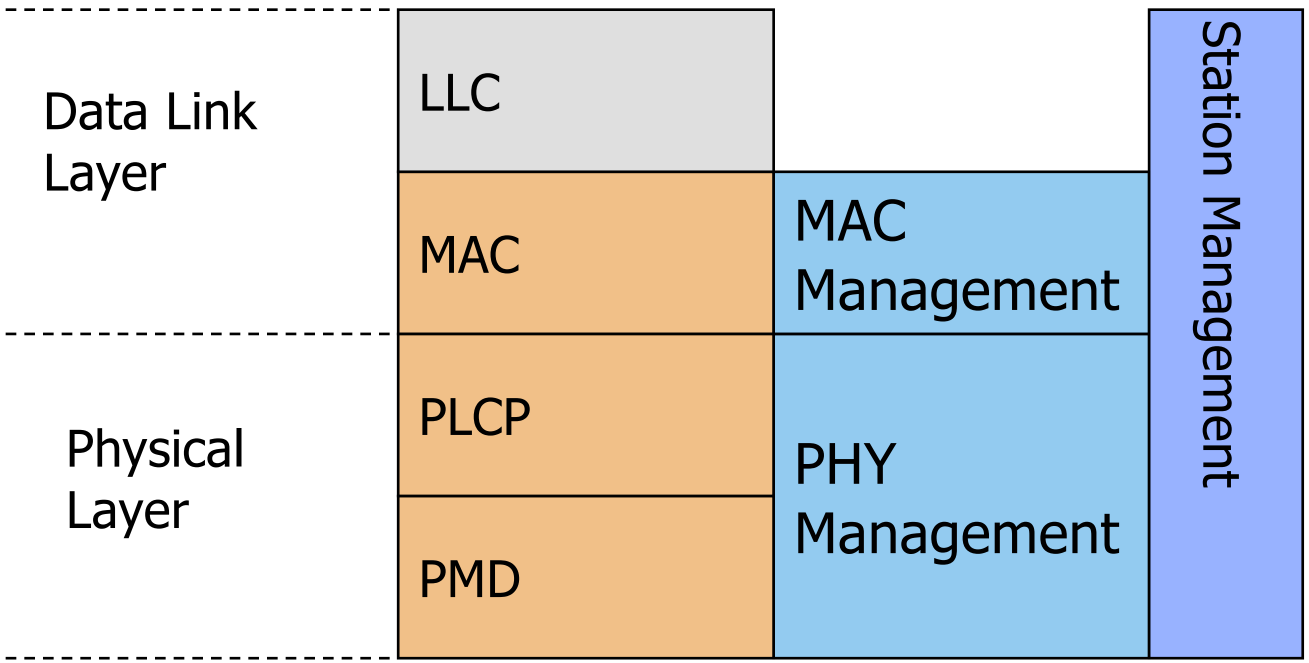


"Cell Search" in IEEE 802.11

- There is no real "cell search" in 802.11
- MS scans the air for the various channels specified in IEEE 802.11
  - Recall the 5 MHz separation and 25 MHz bandwidth
- MS uses the "beacon" message to pick the strongest signal
  - Beacon is decoded
  - If network (B/E SSID) is known, it "associates" with the AP
  - If it is unknown, user may be prompted (or not – it may simply associate itself)

IEEE 802.11 Protocol Architecture

MAC layer independent of Physical Layer (mostly)
Physical varies with standard (802.11, 802.11a, etc.)
PLCP: Physical Layer Convergence Protocol
PMD: Physical Medium Dependent



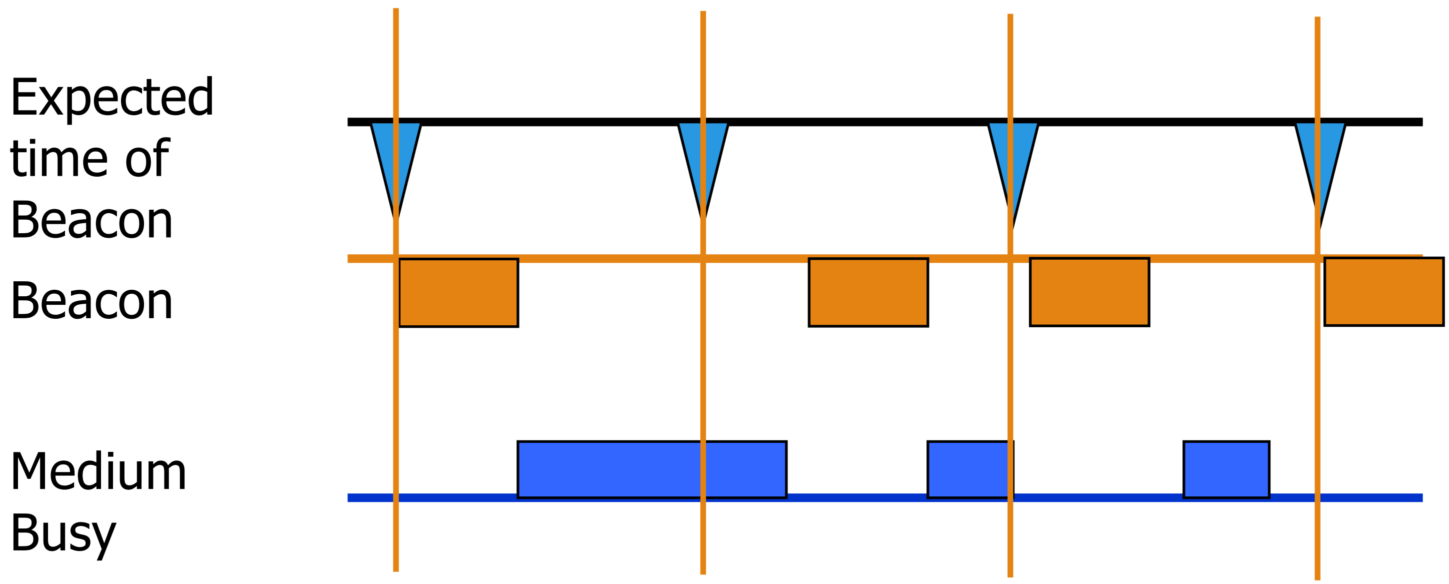
More on the Protocol Stack

- IEEE 802.11 data link layer has two sublayers
  - Logical Link Layer
    - Determined by wired network interface
  - Media Access Control (MAC) layer :
    - Security, reliable data delivery, access control
    - Provides coordination among MSs sharing radio channel

MAC Management Frames in 802.11

- Beacon
  - timestamp, beacon interval, capabilities, ESSID, traffic indication map (TIM)
- Probe
  - ESSID, Capabilities, Supported Rates
- Probe Response
  - same as beacon except for TIM
- Re-association Request
  - Capability, listen interval, ESSID, supported rates, old AP address
- Re-association Response
  - Capability, status code, station ID, supported rates

Beacon in IEEE 802.11



- Beacon is a message that is transmitted quasi-periodically by the access point
- It contains information such as the BSS-ID, timestamp (for synchronization), traffic indication map (for sleep mode), power management, and roaming
- Beacons are always transmitted at the expected beacon interval unless the medium is busy
- RSS measurements are made on the beacon message

Association

- In order to deliver a frame to a MS, the distribution system must know which AP is serving the MS
- Association is a procedure by which a MS “registers” with an AP
- Only after association can a MS send packets through an AP
- How the association information is maintained in the distribution system is NOT specified by the standard

Re-association and Dissociation

- The ***re-association*** service is used when a MS moves from one BSS to another within the same ESS
- It is always initiated by the MS
- It enables the distribution system to recognize the fact that the MS has moved its association from one AP to another

- The ***dissociation*** service is used to terminate an association
- It may be invoked by either party to an association (the AP or the MS)
- It is a notification and not a request. It cannot be refused
- MSs leaving a BSS will send a dissociation message to the AP which need not be always received

What is Radio Resource Management?

- RRM should
  - Continuously provide the “best” possible RF channel between the MS and the fixed network
- Questions
  - What is “best”?
  - What parameters are part of the provision of the RF channel?
  - How does this change over time?
- In general, RRM needs a reference channel that is known, stable and can be used for comparison
  - Beacon in 802.11, BCCH in GSM/GPRS, pilot channels in CDMA etc.

Why Radio Resource Management?

- **Problem: Interference**
  - Types of interference
    - Uplink interference and downlink interference
    - Intra-cell and inter-cell interference
- **Solution: Power Control**
  - Control the power transmitted by MSs and BSs
    - The smaller the transmitted power, lower the interference
  - By-product
    - Saves on the battery consumption at the MS

- **Problem: Cellular topology requires handoff**
  - Issue
    - At some point of time the MS must make a decision to handoff
    - Handoffs have penalties – loss of quality, increasing interference, increasing signaling load etc.
  - **Required Solution: Handoff Decision**
    - Exactly one handoff must be made at the right time at the right place

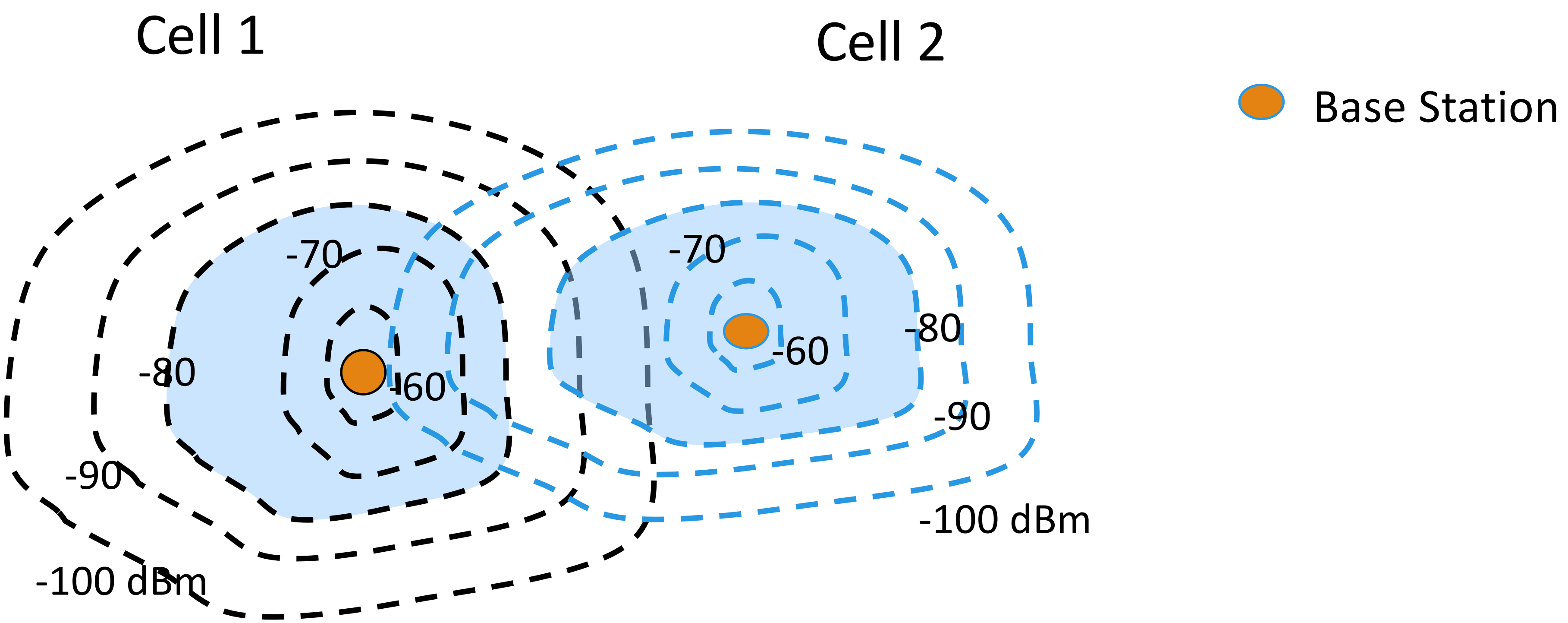
A more formal definition of RRM

- To each active MS, assign
    - A base station
    - A waveform (or channel)
        - Frequency, time slot, group of time slots, or codes, or group of codes, modulation scheme, coding scheme
    - A transmit power
  - When we do this at a cell boundary it is “handoff decision”
  - Is it fixed for the rest of the time within the cell? How does it change for voice? For data?
- Constraints
  - Link quality should be acceptable for all MSs
  - Constraints are satisfied for as many MSs as possible
- Objective function
  - Maximize revenue with QoS constraints – what does this mean?

RRM Functions

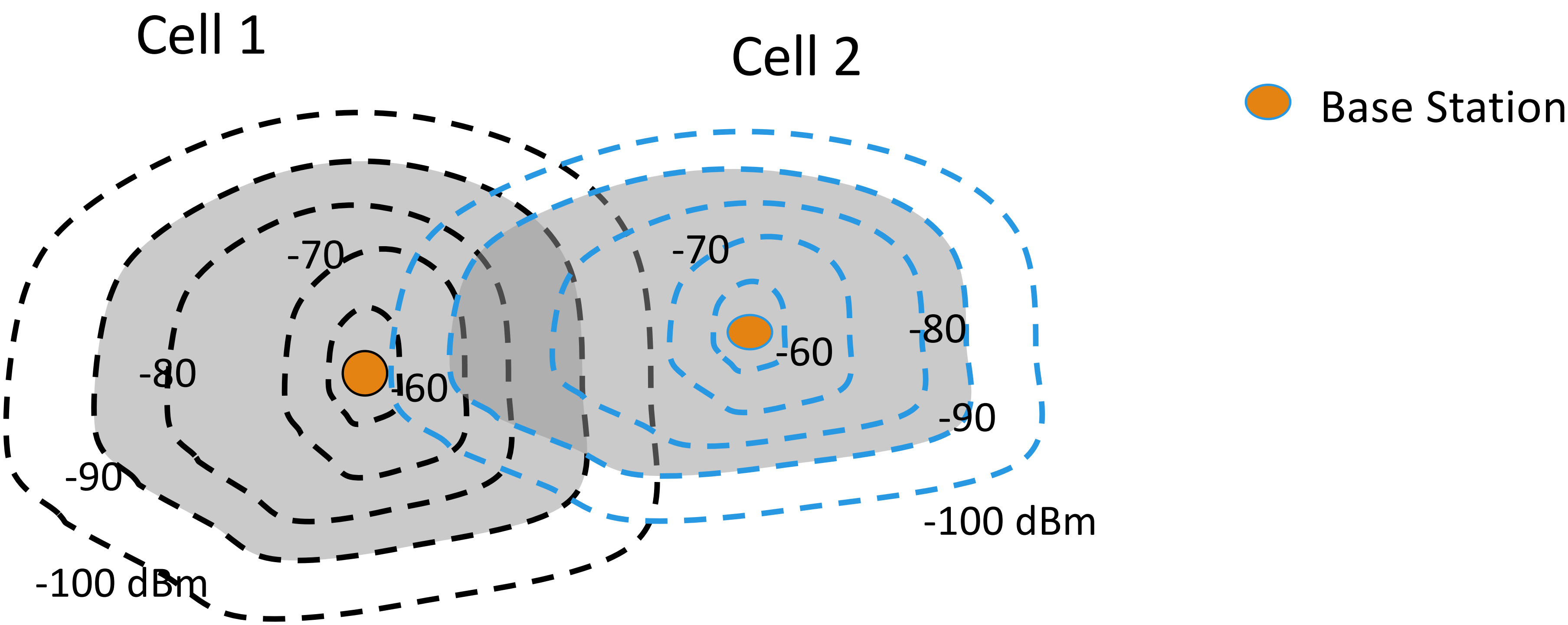
- Base station and rate/channel assignment
  - Link adaptation
- Transmit power assignment
  - Power control
- Handoff decision
  - Intra-cell handoff
  - Inter-cell handoff
  - Soft handoff
- Technology specific issues
  - Dynamic Frequency Selection
    - How to select the frequency of operation in a BSS of HIPERLAN/2 or IEEE 802.11a
  - Channel hopping in CDPD

BS Selection: How to select the best channel?



-80 dBm threshold leaves “holes”

BS Selection: How to select the best channel?



-90 dBm threshold makes transmission to another cell deep inside a cell

Solution?

- No “single variable” algorithm such as RSS will satisfy all variations
- Use many parameters to make a decision
  - Use those most appropriate for the propagation characteristics
  - A channel with adequate signal level should not be selected
  - In general the channel with the STRONGEST RSS is always selected to start since it is most likely a local channel (physically closest)
  - (Compare using the largest SIR instead)

Link Adaptation and Adaptive Multi-rate Transmissions

- RRM typically handles the messages that are transmitted in support of link adaptation
- Measurements of RSS, power levels, etc. are exchanged between the RRM layers in the mobile and BSC/RNC/Node-B/e-Node B as needed
- You can think of this as being related to the "channel assignment" problem

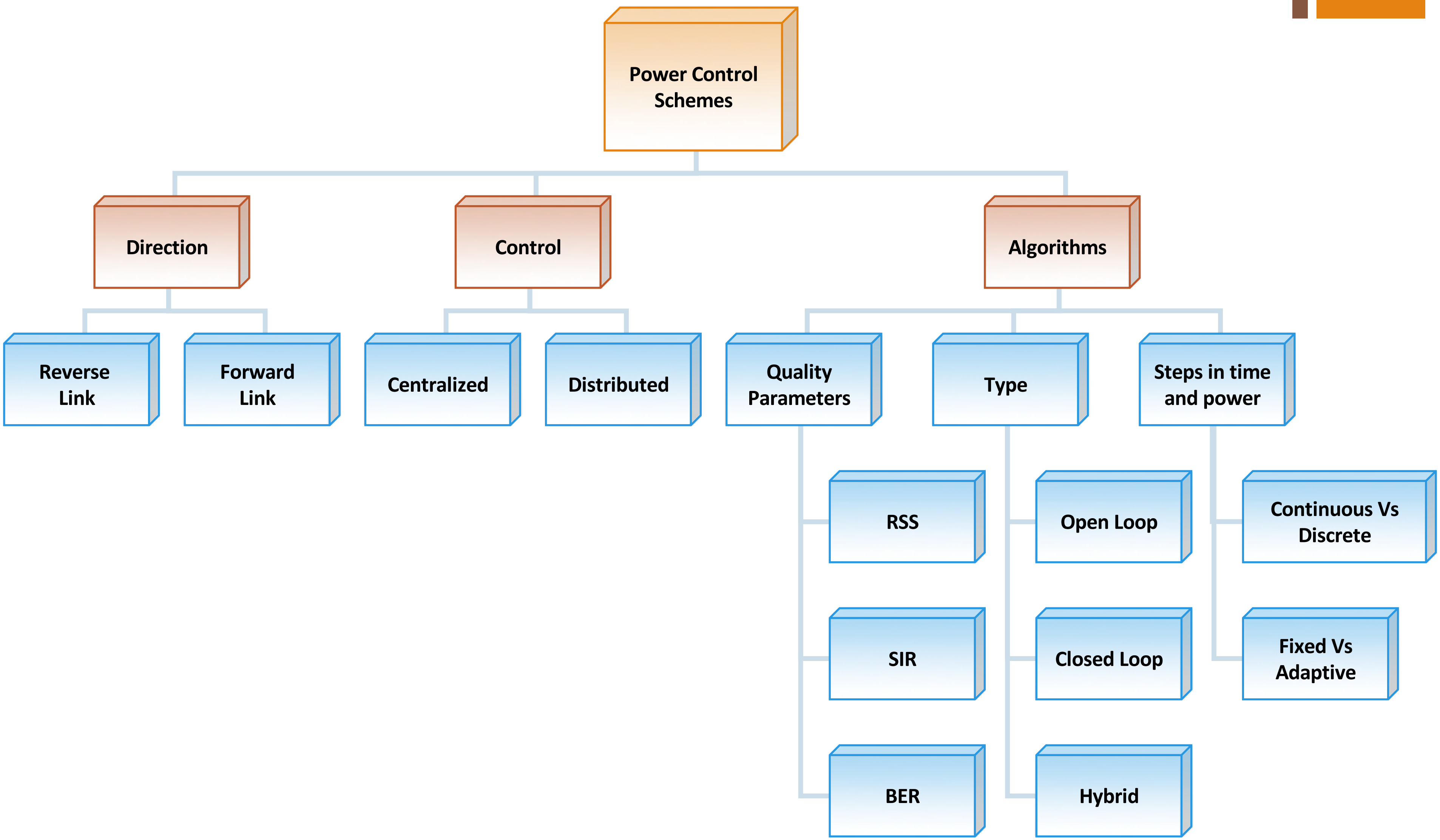
Power Control

- Co-channel interference management
  - Excessive transmit power in a cell at a frequency can effectively lock the channel up preventing it’s use in co-channel cells
- CDMA systems
  - Very very important to prevent the near-far effect
- Affects capacity of the system
- Affects the life of the battery in a MS

Power Control (2)

- What is the ideal solution?
  - Early systems tried to maintain a constancy of RSS at the receiver
    - Eliminates the need for receivers to have a large dynamic range
  - Today: A MS should transmit at the *minimum* power that results in an “acceptable SIR” for voice
    - Transmitting above this power wastes the battery power and causes interference
    - Transmitting below this power increases the error rates

Classification of Power Control Schemes



Parameters of power control schemes

- Quality measure
  - RSS
  - SIR and BER
    - If the SIR is constant, so is the BER
    - If the SIR is fluctuating, the average SIR $\neq$ average BER
  - Available measurements
    - Measurements reports of RSSI – received signal strength indicator or CQI – channel quality indicator
- Constraints
  - What the maximum and minimum transmit powers allowed by the hardware, the system regulations, etc.
- Time delays
  - Measuring RSS or BER and signaling this information requires time
- Step size
  - Usually power control has to be performed in discrete steps (1 dB to 5 dB)
  - The step size could be fixed or adaptive depending on how dynamic the channel is

Open Loop Power Control

- Usually implemented on the reverse link
  - The MS measures the quality of the **reference** channel and decides what transmit power to use
    - If the RSS is above a threshold or the BER is small, the MS may reduce its transmit power
    - If the frame error rate is large, the MS may increase its transmit power
- Advantages
  - Simple to implement
- Disadvantages
  - The forward channel is much different from the reverse channel – they are usually NOT correlated
  - Delay in implementing this, especially in TDMA systems

Example of Open Loop Power Control: IS-95 Systems

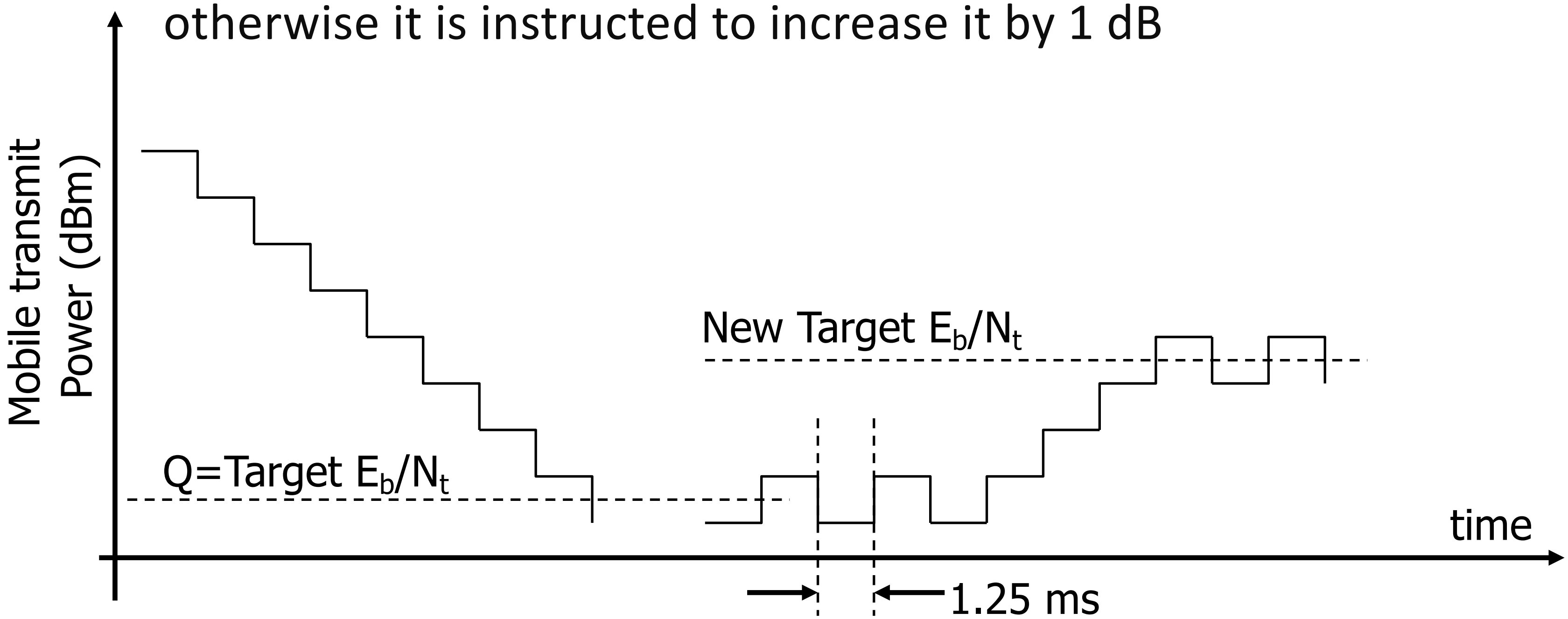
- Reverse Link
- Upon powering up, a MS listens to the pilot channel (the reference channel in IS-95)
- The MS transmits signals such that its transmit power is inversely proportional to the total RSS on the pilot channels from all BSs
  - The signal is called an “access probe”
  - If there is no ACK for the access probe, it is retransmitted with a higher power
  - The process is repeated till an ACK is received or the transmit power becomes the maximum allowed
- If no ACK is received, the MS backs off and repeats the process again (up to 15 times)

Closed Loop Power Control

- There is a feedback mechanism between the BS and the MS
  - On the forward control channel, the BS indicates what steps the MS has to take to change its transmit power
- Example: GSM/GPRS
  - The MS reports the RSS from up to six neighbouring BTSs to the serving BS
  - The serving BTS measures the RSS from the MS and its distance (crude) and computes the minimum required transmit power
  - Afterwards, power control is performed in steps of 2 dB

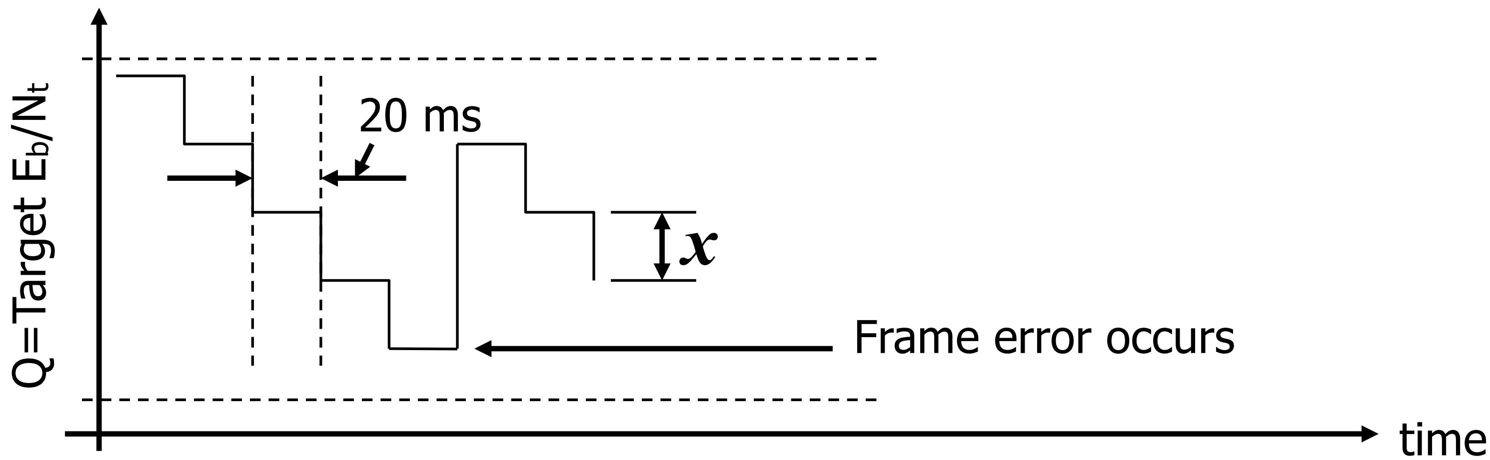
Closed Loop Power Control in IS-95

- Inner loop
  - Suppose the target E_b/N_t is Q dB
  - Every 1.25 ms, the BS computes whether the E_b/N_t value is greater than Q or not by sampling it 16 times
  - If it is greater, the MS is instructed to decrease its power by 1 dB, otherwise it is instructed to increase it by 1 dB

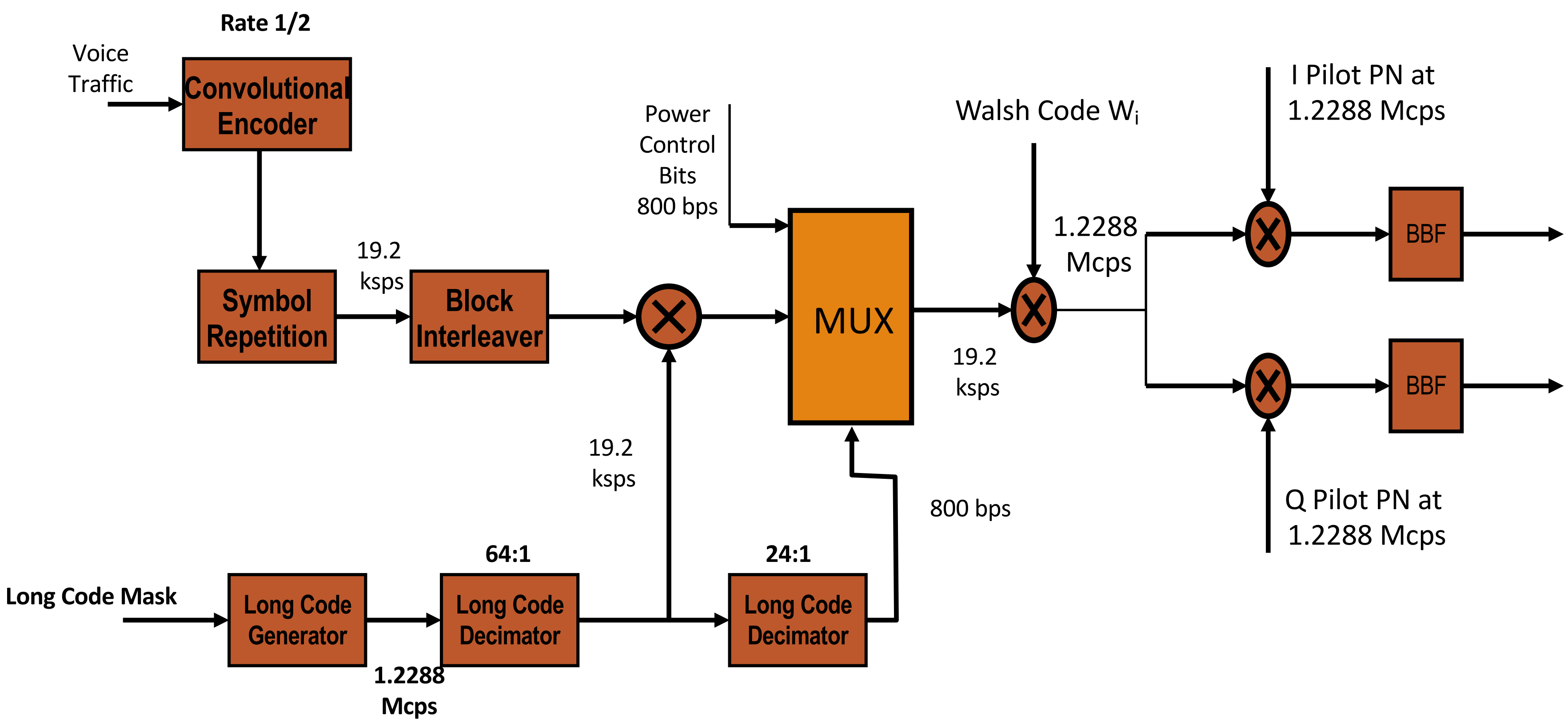


Closed Loop Power Control in IS-95 (2)

- Outer Loop Power Control
  - The target E_b/N_t value is varied over time to reflect changes in the environment like velocity of the MS, fading etc. to obtain the same frame error rate
  - It is reduced by X dB every 20 ms, where $100X$ = 3 dB
  - It is increased when a frame error occurs



Operation of the Forward Traffic Channel (Rate Set 1)



Operation of the FTCH (RS-1)

- Speech data is sent through a rate ½ convolutional encoder
  - Output rates will be 19.2, 9.6, 4.8 or 2.4 kbps
  - Same convolutional encoder as synch/paging channel
  - Difference: The encoder is reset to all zero state after 20 ms
- Depending on the output of the convolutional encoder, the symbols are repeated
  - 19.2 kbps – no repetition
  - 9.6 kbps – 1 repetition, 4.8 kbps – 3 repetitions and 2.4 kbps – 7 repetitions
- Final output is ALWAYS 19.2 kbps for 20 ms => a total of 384 bits

Further steps in FTCH operation

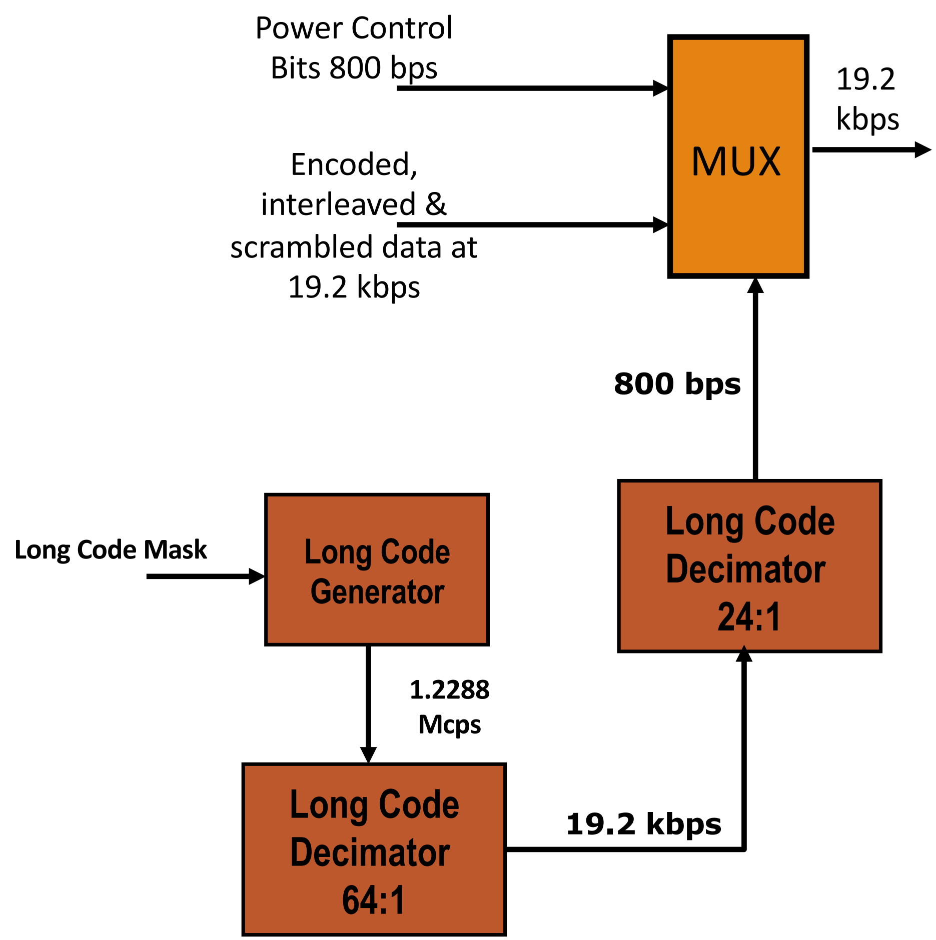
- The 384 bits are interleaved over 20 ms
- The bits are scrambled using the long code
  - The long code mask is either public or private
  - The private long code mask is NOT specified
  - Used to provide privacy of voice
- The data is then multiplexed with a *power control* subchannel
  - This contains 1 bit every 1.25 ms (800 bps)
    - If the bit is 1 the MS reduces its transmit power by 1 dB
    - If the bit is 0 the MS increases its transmit power by 1 dB

1100011000	Permuted ESN

Public long code mask for traffic channel

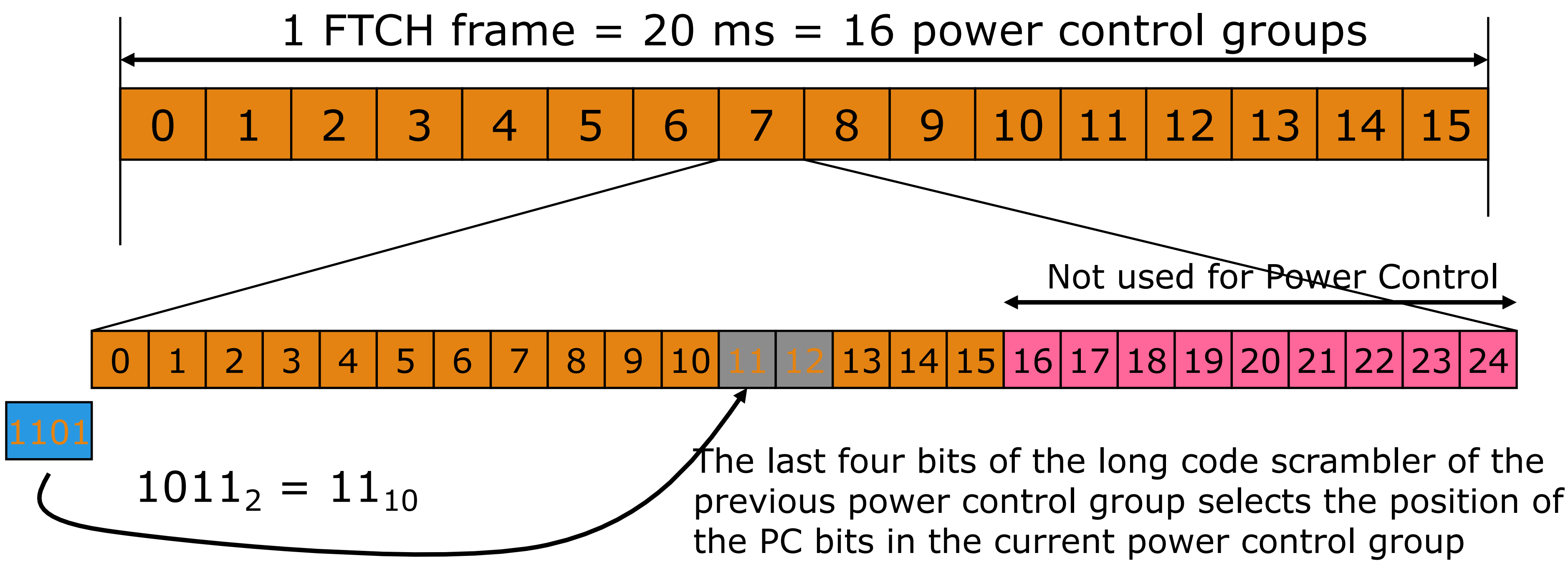
Multiplexing with the power control subchannel

- The power control bits steal bit positions from encoded data
  - The power control information occupies two symbols in the traffic stream
    - The traffic stream has been at least doubled because of the convolutional coding
- The convolutional code is used to correct the introduced errors



More on the power control subchannel

- A 20 ms frame is divided into 16 *power control groups*
  - One power control group = 20/16 = 1.25 ms
  - 1.25 ms has 19.2 x 1.25 = 24 bits



More on power control (2)

- If the last four long code scrambling bits are a_{20} a_{21} a_{22} a_{23}, the position is determined by a_{23} a_{22} a_{21} a_{20}
- Why is the position of the power control bit not fixed?
  - If the MS is asked to raise or lower power in the same way over several PC groups and the bit position is fixed, a spectral line can be created because of the periodicity
  - By using the long code bits, the position is randomized
- Power control bits are always transmitted at 100% power
- The power control bit in a PCG is determined based on the measured power two PCGs prior to it
- How does the MS know where the PC bits are located?

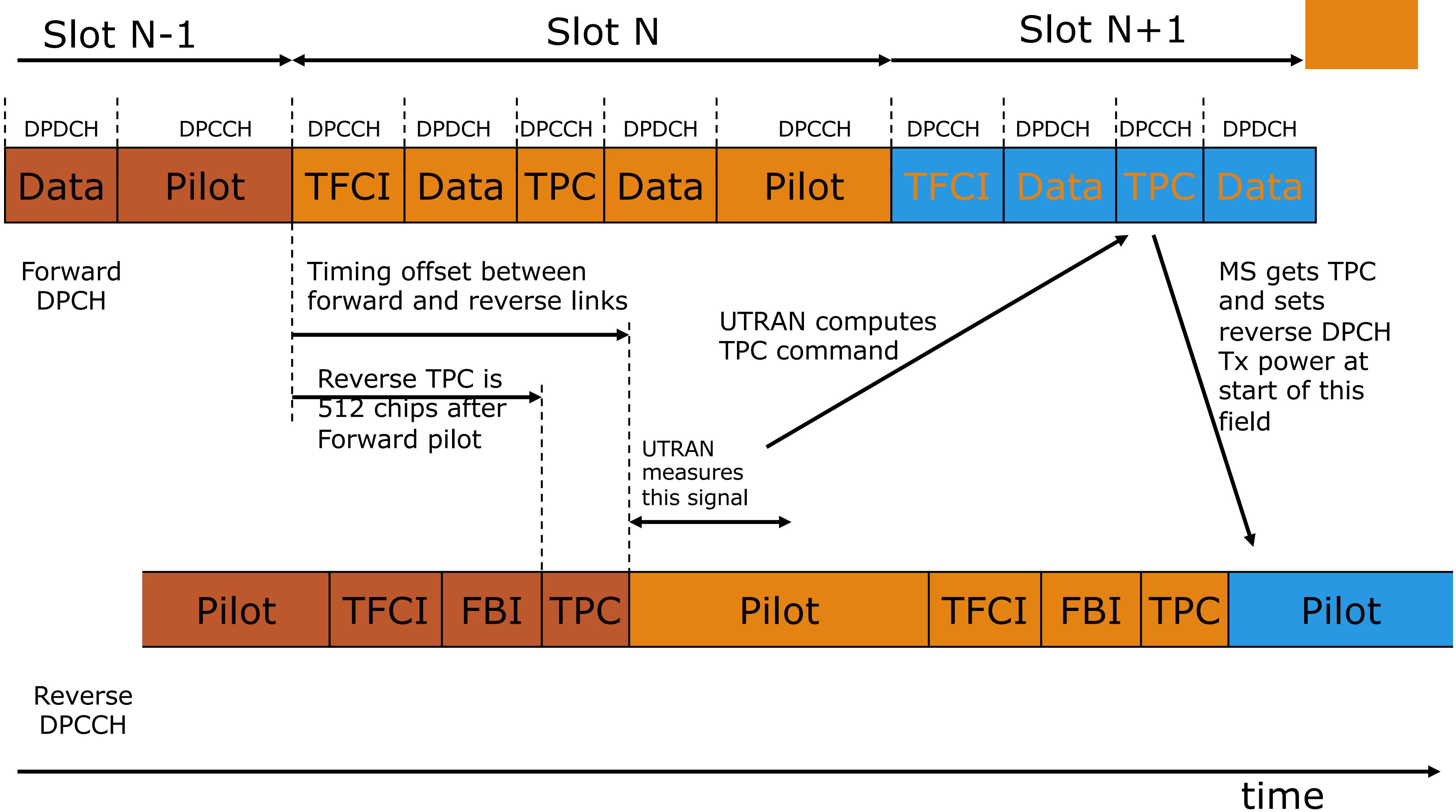
Power Control Procedures in UMTS

- Open Loop Power Control
  - MS sets transmit power to some specific level
  - Tolerance is $\pm$ 9 dB (normal) and $\pm$ 12 dB (extreme)
- Closed Loop Power Control
  - Inner Loop – Forward Link
    - Enables BS to adjust its transmit power in steps of 0.5 or 1 dB
    - The MS sends a TPC command to the BS
    - Goal – to maintain a satisfactory SIR at the MS
  - Inner Loop – Reverse Link
    - The MS adjusts its transmit power in response to a TPC command from the BS
    - Step size is 1,2, or 3 dB
  - Outer Loop Power Control
    - Sets the target SIR to satisfy a given frame error rate

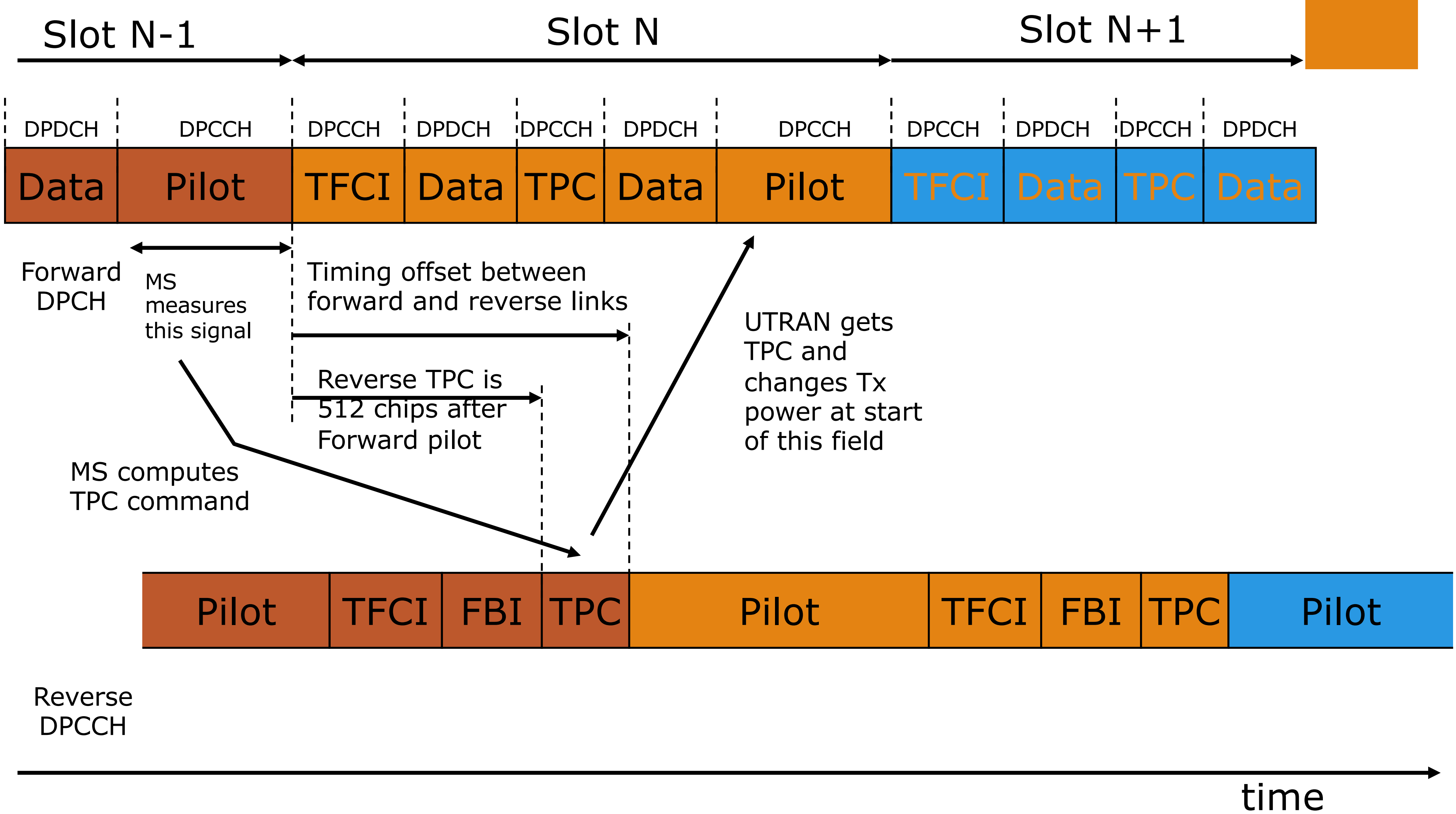
Reverse Link Power Control – I

- The MS starts transmitting on the reverse DPCCH using a power set by the higher layers
- The serving cell measures the received SIR
  - The SIR is compared with a threshold
  - If the received SIR > threshold, a TPC command of 0 is transmitted
    - The MS reduces its power by 1 or 2 dB as dictated by higher layers
  - If the received SIR < threshold, a TPC command of 1 is transmitted
    - The MS increases its power level
  - If both a DPDCH and a DPCCH are present, both powers are increased or decreased simultaneously
    - The reverse DPCCH should immediately adjust the pilot transmit power

Reverse Link Power Control - II



Forward Link Power Control



+ Control of the Power Control Mechanism

- Distributed power control
  - The open and closed loop power control mechanisms discussed previously
  - They deal with the powers of each MS individually
  - This is a distributed mechanism although the control is with a central authority – the BS or BSC
  - The MSs should reach ideal transmit power and SIR levels iteratively

- Centralized power control
  - The BS or BSC has knowledge of all radio links in the system
    - RSS, SIR, BER for all MS-BS combinations are known
  - An optimal power allocation can be derived
  - Practically impossible to keep track of all links in the system

Power Control in Wireless LANs

- As they exist today, there is NO power control in WLANs
  - Potential problems
    - Carrier sensing, hidden and exposed terminals
- In Europe, power control is mandated for operation in the 5 GHz bands
  - HIPERLAN/2 specifies transmitter power control
- In the USA, the IEEE 802.11h group looked at power control issues

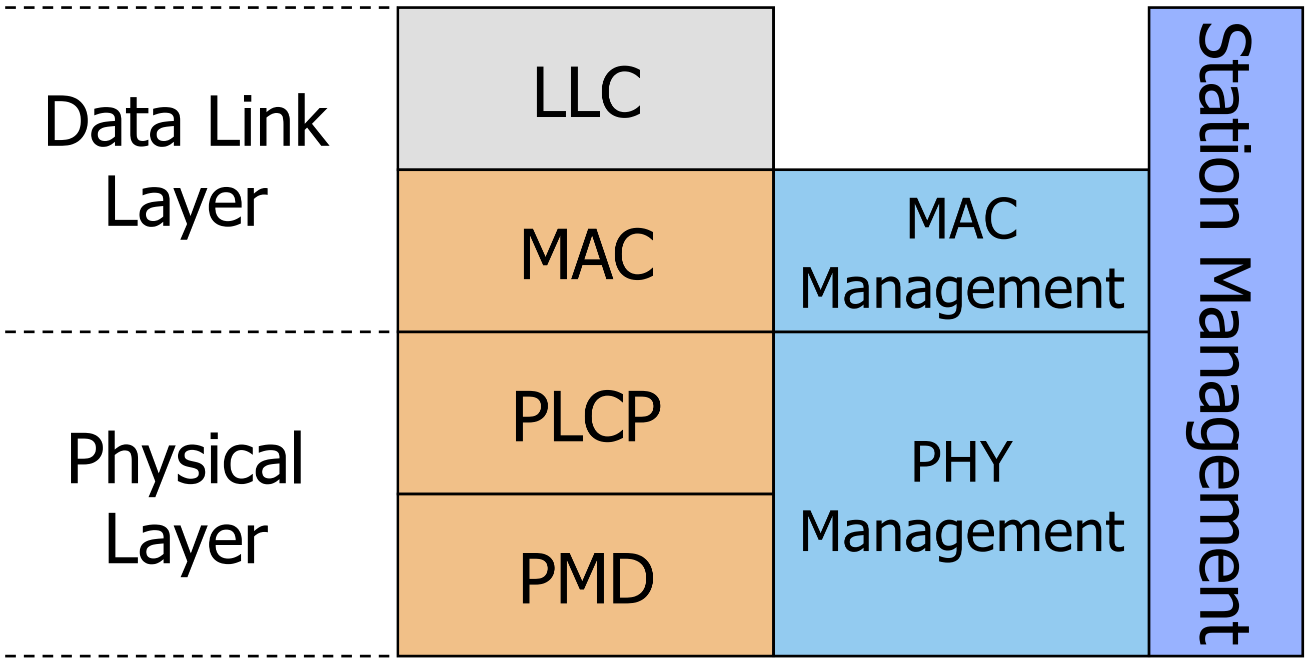
IEEE 802.11h proposal

- Defines only the PHY and MAC changes necessary to implement power control
- Actual algorithms are implementation dependent
- Suggested absolute TX Power Settings for all MSs
  - -15 dBm to +30 dBm, 3 dB steps
  - 16 settings – use a 4 bit representation
  - Closely follows HIPERLAN/2

Other details of the proposal

- Power levels can be controlled in both a centralized and a distributed fashion
  - AP can use global TX power limit within BSS
  - MSs can request power level changes from other MSs
  - AP (and MSs) can individually set power level for each destination MS/AP

IEEE 802.11 Protocol Architecture



PLCP: Physical Layer Convergence Protocol
PMD: Physical Medium Dependent

MAC Management Frames in 802.11

- Beacon
  - timestamp, beacon interval, capabilities, ESSID, traffic indication map (TIM)
- Probe
  - ESSID, Capabilities, Supported Rates
- Probe Response
  - Same as beacon except for TIM
- Re-association Request
  - Capability, listen interval, ESSID, supported rates, old AP address
- Re-association Response
  - Capability, status code, station ID, supported rates

MAC changes in IEEE 802.11

- Power control information is exchanged with "Probe Request" and "Probe Response" frames
- Use a "command" bit
  - A "zero" requests the current transmit power level information
  - A "one" instructs setting the transmit power level to a given value
- Global power levels are communicated in the beacon – e.g. maximum transmit power in a BSS or IBSS

Why Power Management?

- Limited battery power at the MS
  - Reasons for power consumption
    - Transmissions
    - Channel monitoring
    - Device operation
      - Backlight
      - Accessing disk space
      - CPU
  - Solution approaches
    - Power saving mechanisms
      - Suspended modes of operation
    - Energy efficient protocol design
      - Minimize unnecessary transmissions
    - Energy efficient software/device designs

Power saving mechanisms

- Transmissions and receptions consume a lot of power
  - Measurements of the old Lucent Wavelan cards indicated that a 15 dBm card consumes
    - 1.83 W in transmit mode
    - 1.8 W in receive mode
    - 0.18 W in standby mode
- A MS must spend as much time in standby mode as possible to conserve power
  - Voice terminals – discontinuous transmission using the voice activity factor & standby modes
  - Data terminals – sleep modes when there is no data to transmit or receive
    - There must be provisions in the network to handle calls or packets that arrive for a MS that is sleeping

Power Saving in 802.11

- All MSs switch off the radio part when unnecessary
- They have to be synchronized to wake up at a particular time when a sender will transmit buffered frames for them
- All unicast messages are announced in the TIM (traffic indication map) of the beacon
- MSs request delivery if they wake up on time (usually) and discover the existence of buffered packets for them
- DTIMs (Delivery TIMs) are used for multicast/broadcast messages less periodically
- ATIMs (Ad Hoc TIMs) are used by MSs in an ad hoc configuration in special time windows