Project: IEEE P802.15 Working Group for Wireless Personal Area Networks (WPANs)

Submission Title: [Samsung MAC proposal – Part 2: Co-existence, network management, security]
Date Submitted: [4 May 2009]

Source: [Eun Tae Won, Sridhar Rajagopal, Farooq Khan, Ranjeet Kumar Patro, Giriraj Goyal, Thenmozhi Arunan, Arun Naniyat, Kiran Bynam, Ashutosh Bhatia, Seung-Hoon Park, Noh-Gyoung Kang, Chihong Cho, Eui-Jik Kim, Jeongsik In, Yongsuk Park] **Company** [Samsung Electronics]

Contact: [etwon@samsung.com]

Re: [TG6 Call For Proposals, IEEE P802.15-08-0829-01-0006, 4th December, 2008]

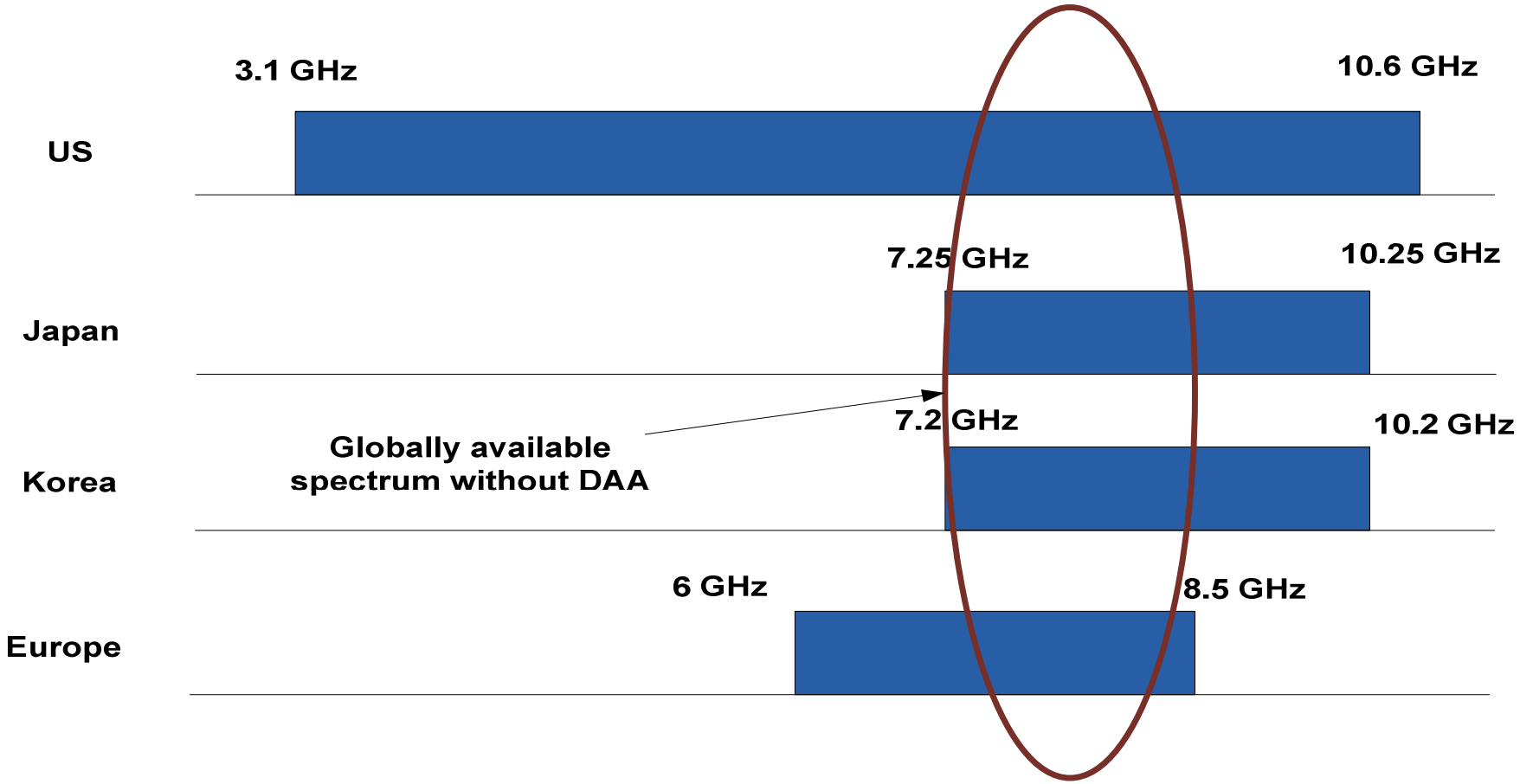
Abstract: [A complete MAC proposal addressing the functional requirements of implant and on-body communications. Part 2 covers co-existence, network management, security and wakeup]

Purpose: [To trigger discussion and initiate merger with other group members of TG6]

Agenda

- Co-existence
- Network Management
- Security

UWB spectrum allocation



Co-existence: Among top Issues for UWB BAN

BAN needs to support at least 10 piconets in 6x6x6 m area

There are only 2 UWB bands available globally without DAA

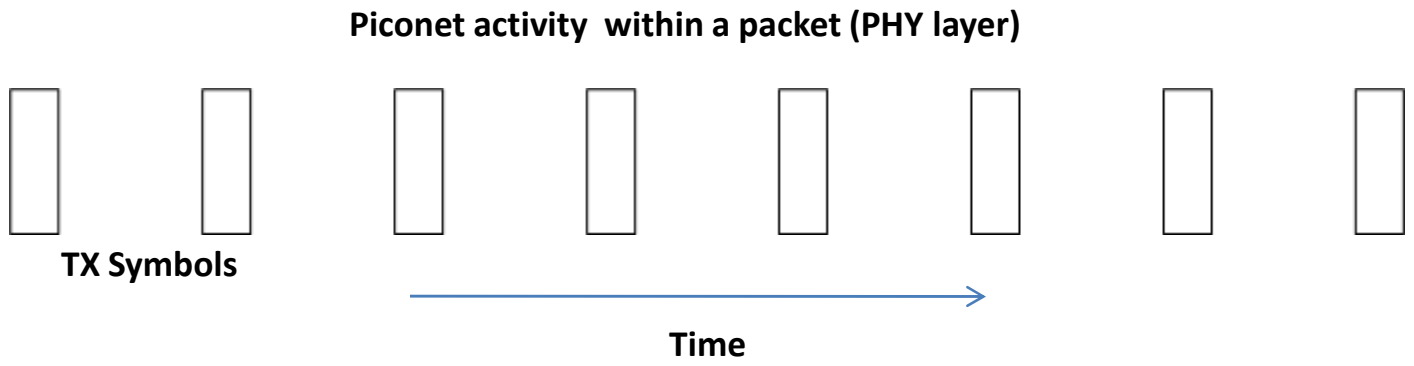
- At least 5 piconets may need to share a band in a fully loaded system

PHY has been designed to accommodate this with preamble design and duty cycle [see PHY proposal]

MAC can further help with channel selection to mitigate interference

Samsung PHY proposal (See PHY proposal for details)

- Low duty cycle waveforms for low power consumption.
- Duty cycle varies between 4% to 50%, depending on data rate
- Helps with co-existence



Samsung MAC proposal (See MAC proposal for details)

Single MAC

- Implant, on-body communications

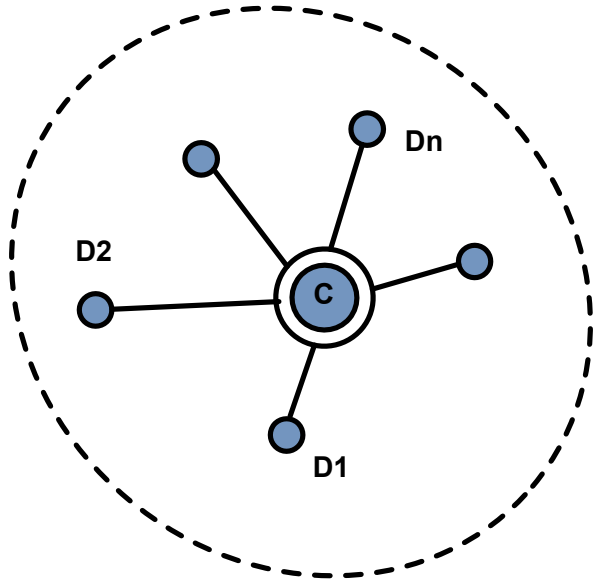
Star topology

Polling based MAC

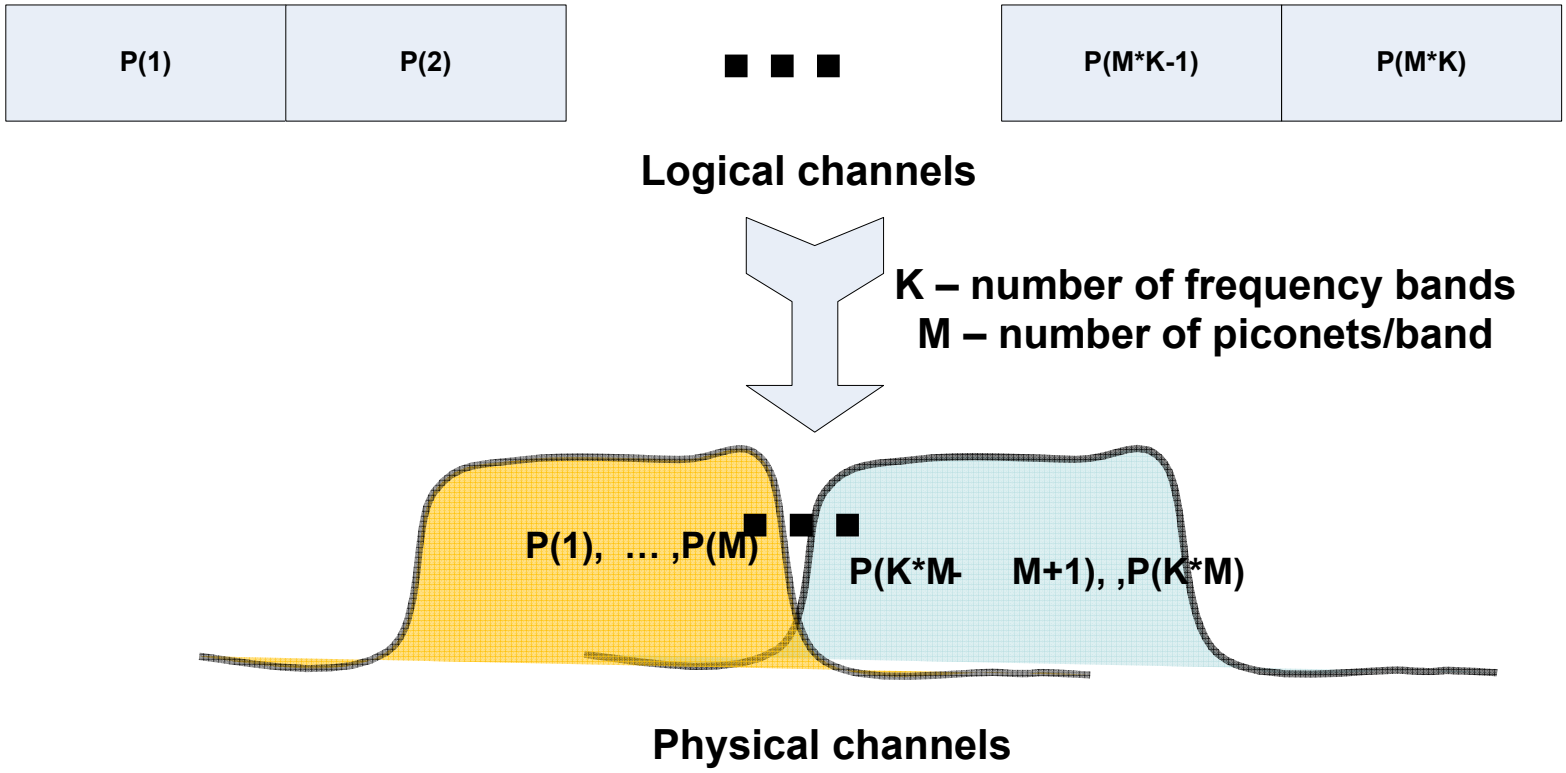
- Device cannot initiate communication except to the response from a coordinator (MICS rule)

Star Piconet Topology

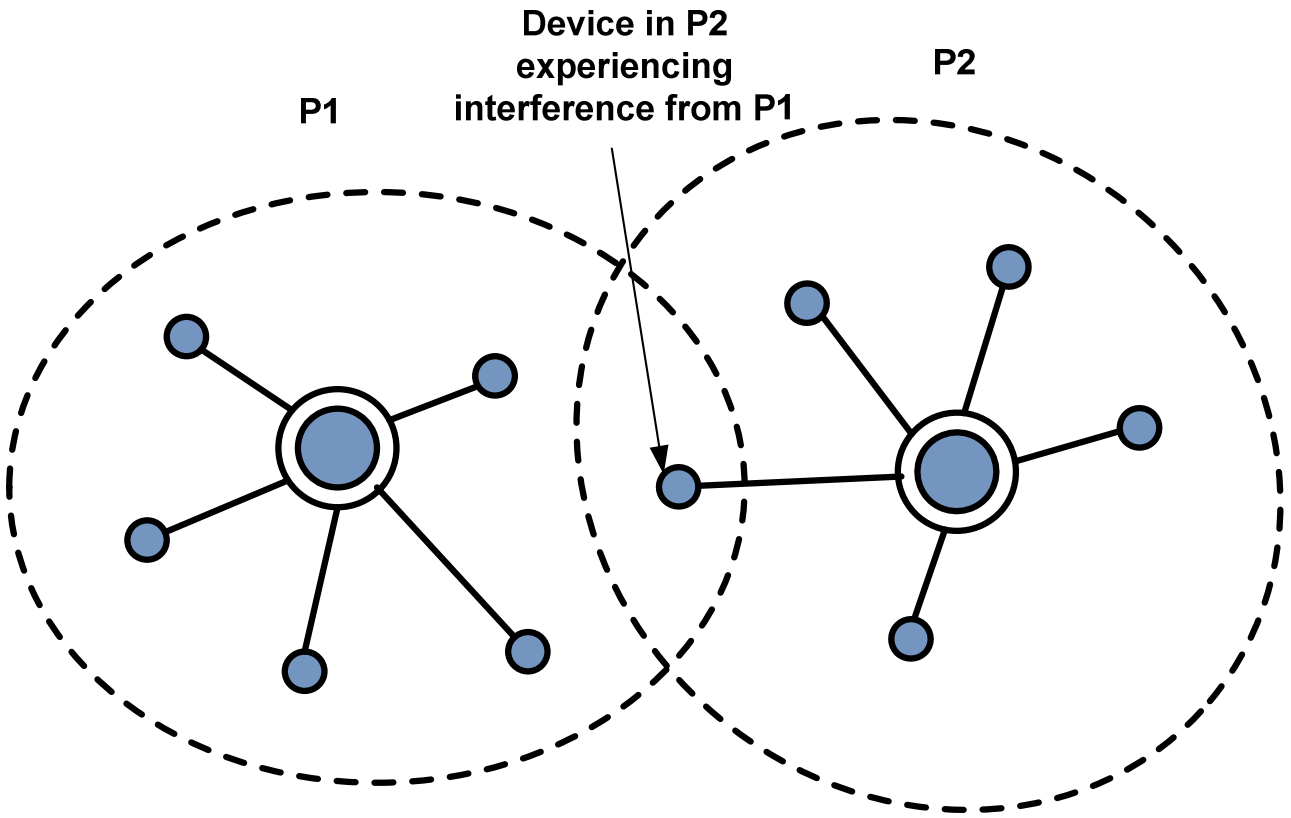
- Single controller (PAN co-ordinator)
- Devices cannot talk to each other
- Devices cannot talk unless told by controller
- Controller makes all decisions
- Device scans in all channels for association request from controller and connects on receiving request and association grant



Logical to physical channel mapping



Inter-piconet interference



Piconet co-existence

Shared Non-interference (NI) mode

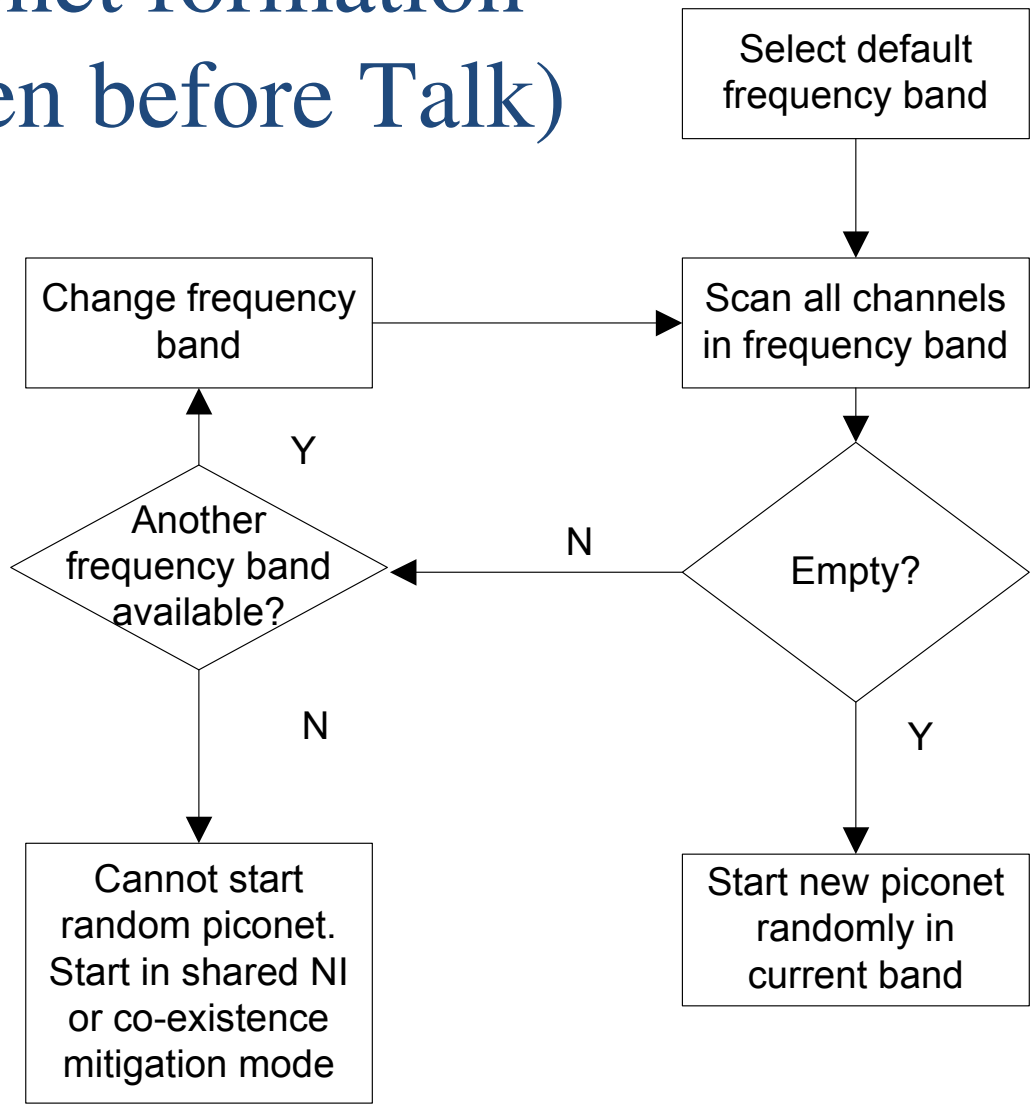
- Piconet controllers can talk to each other
- Option 1: time resource sharing
- Option 2: Offset piconet synchronization

Co-existence interference mitigation (CM) mode

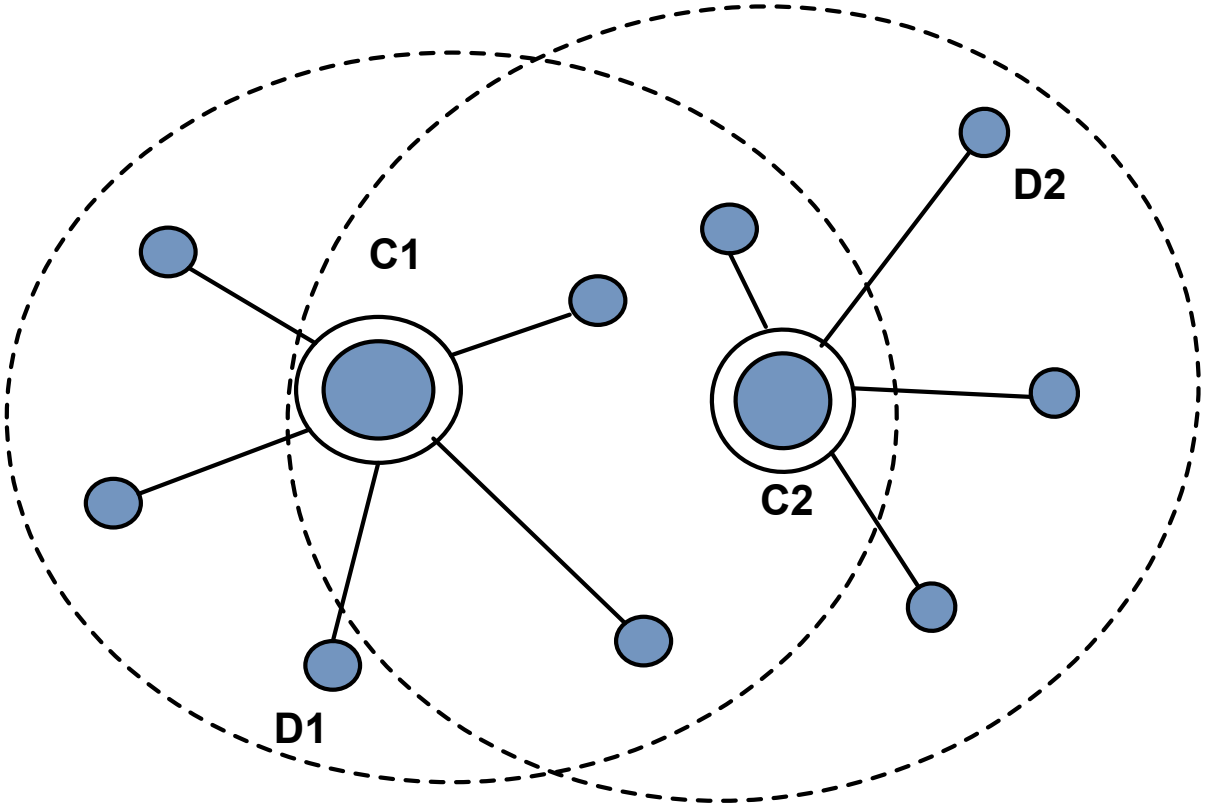
- Piconet controllers cannot talk to each other
- Do not have enough bandwidth to accommodate
- Best effort piconet selection

Piconet formation (Listen before Talk)

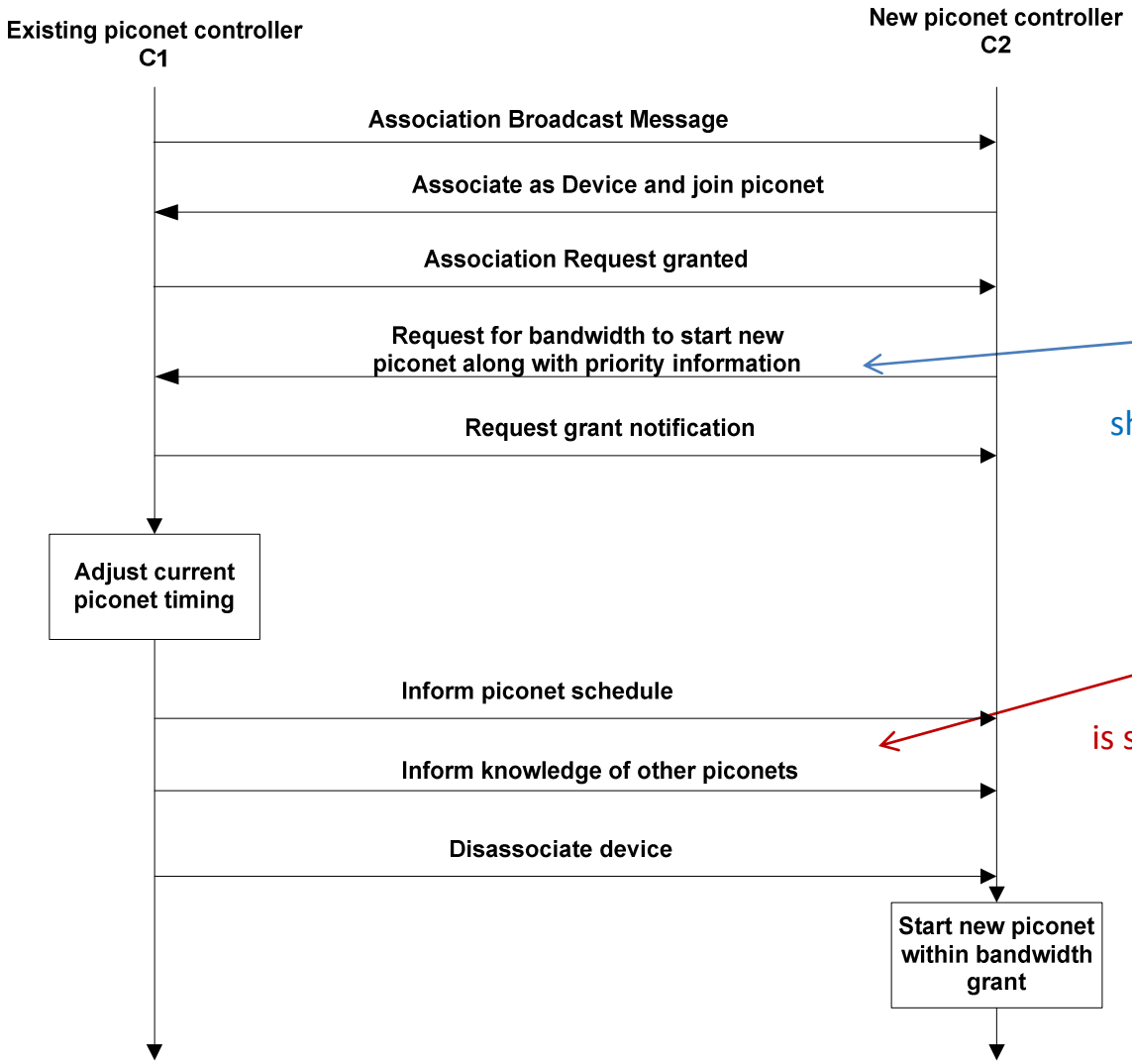
Note:
It is assumed ok to take a long time (seconds) for piconet formation since it is a one-time process at start-up.
Hence, it might be acceptable to spend time searching for other piconets and getting information to make the best decision for logical channel selection



C1 – C2 can talk to each other



Time resource sharing (NI)

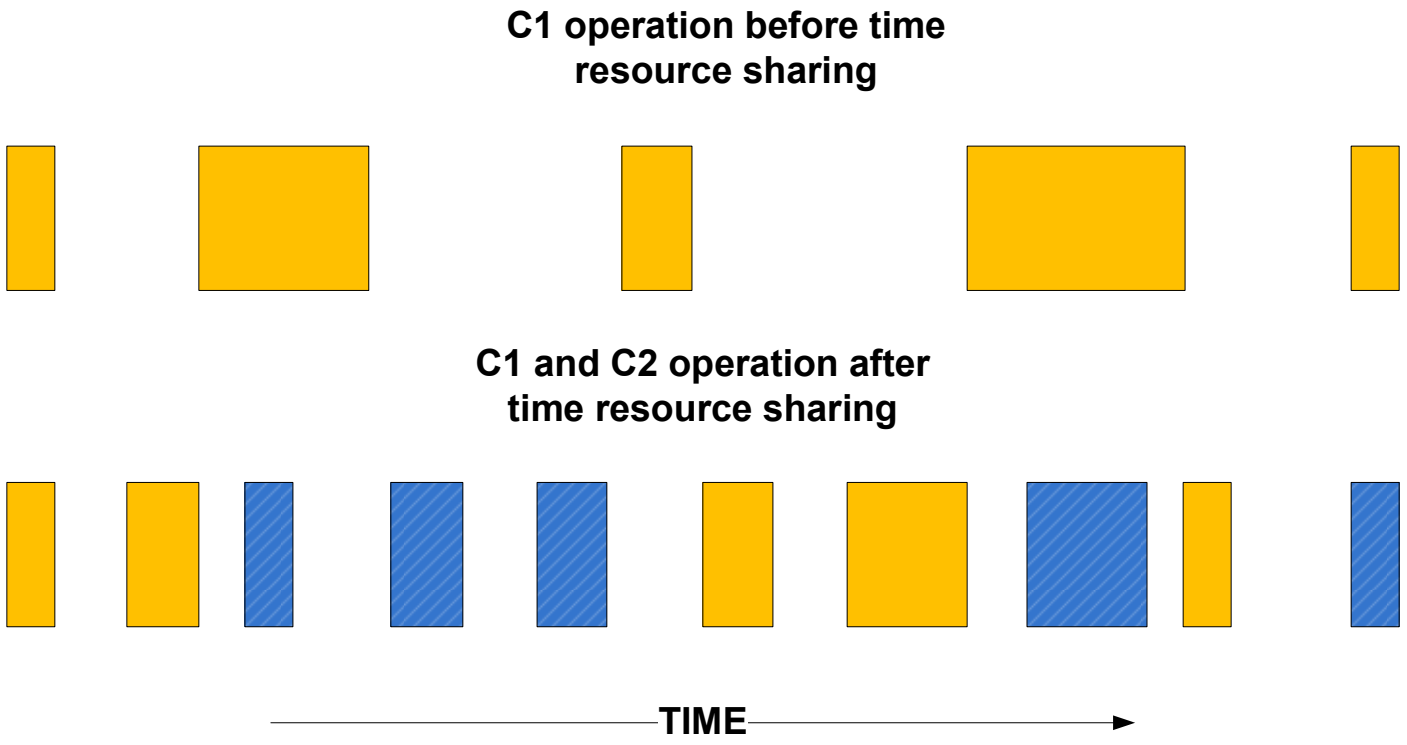


Priority information is sent to allow priority for piconets. For Example, medical devices may require more priority than entertainment devices.
The standard could mandate that existing piconets provide bandwidth sharing to higher priority devices. Medical devices may also have very low activity and hence, may be more amenable to share resources

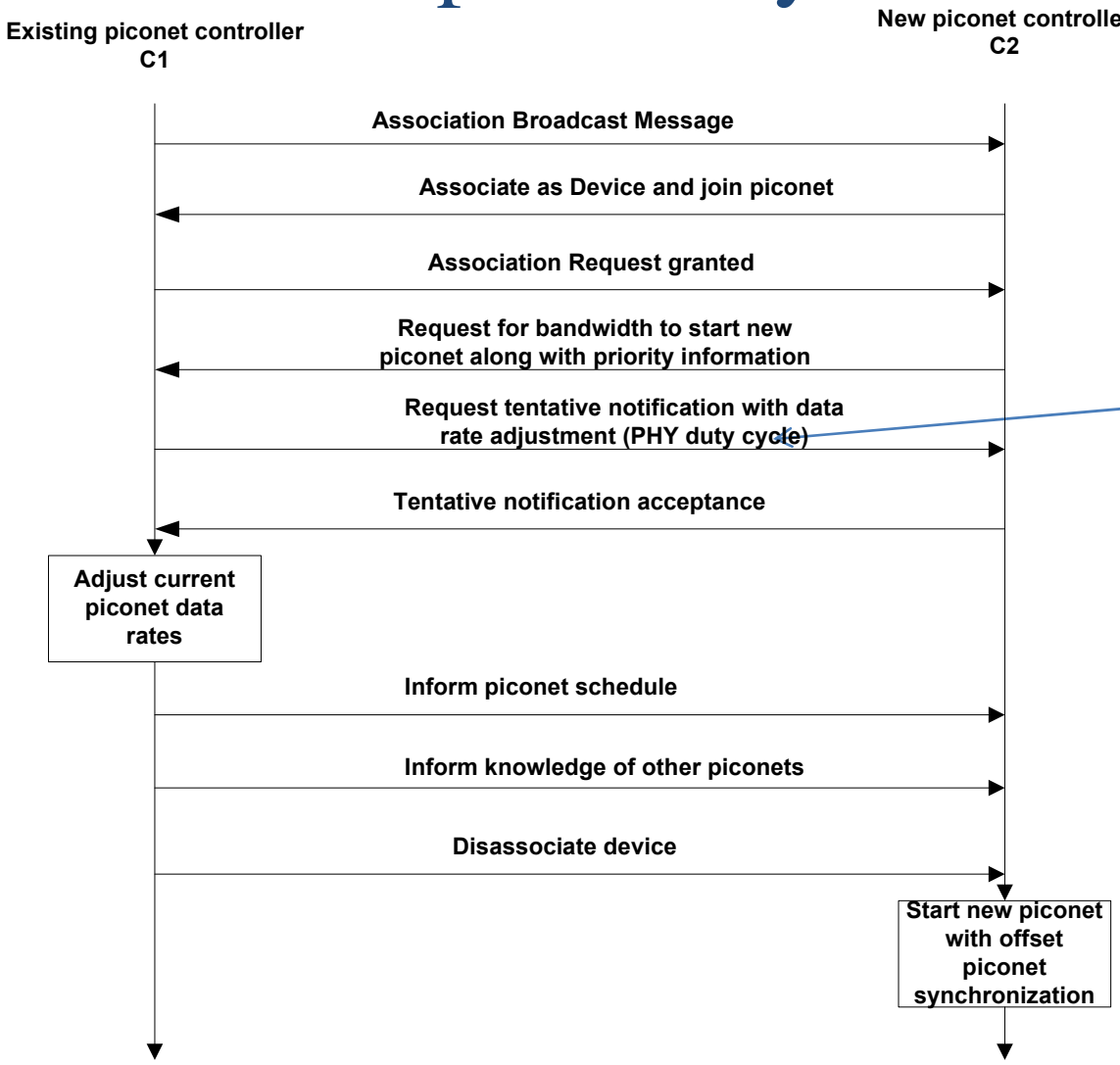
Piconet synchronization is done sequentially. When C2 is being formed, the knowledge of other piconets is sent from C1 to help with logical channel selection. This helps to synchronize among multiple (>2) piconets, when such possibility exists.

All requests and information sharing can be done via Information Elements (IEs)

Time resource sharing

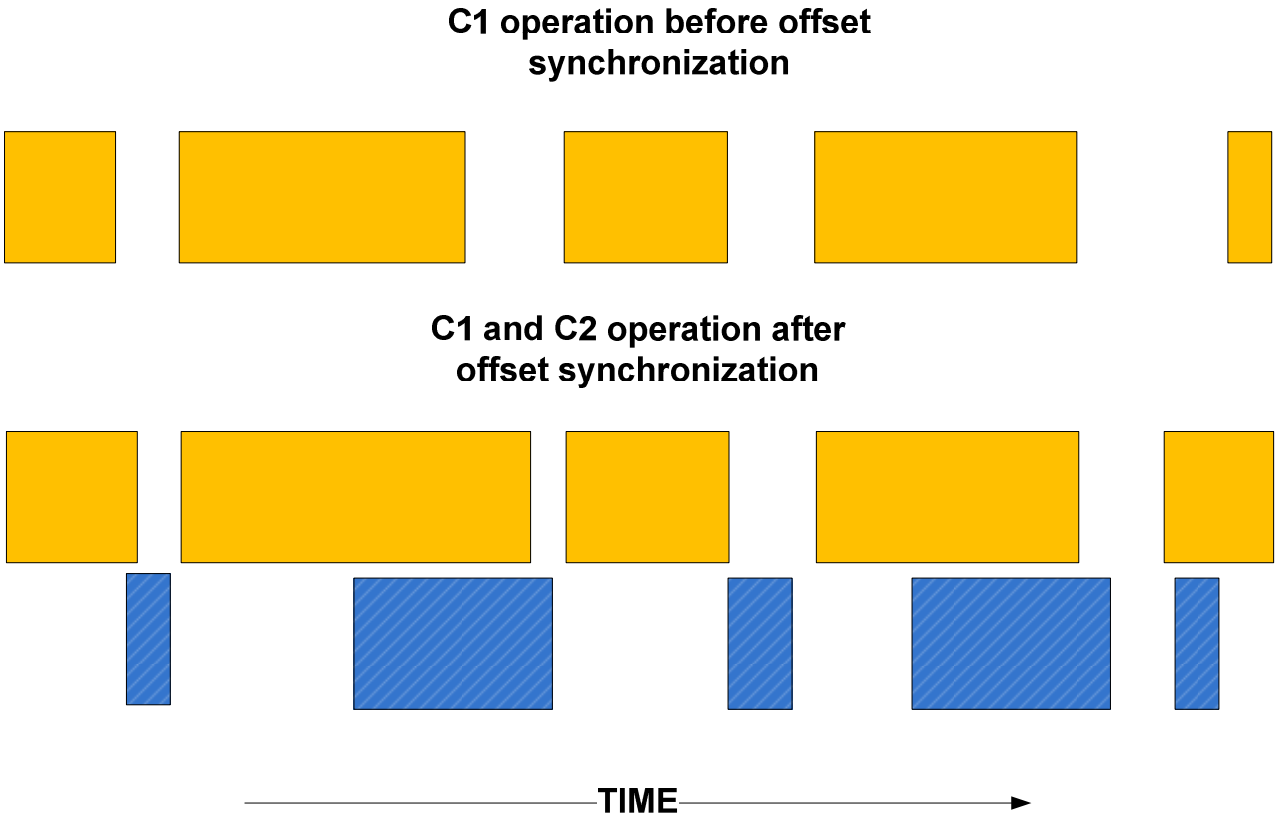


Offset piconet synchronization (NI)



When piconets of similar priority exist, the existing piconet may not be willing to allow priority to the new piconet but may be willing to co-exist by reducing its duty cycle and allowing the new piconet to start an offset synchronized piconet

Offset piconet synchronization



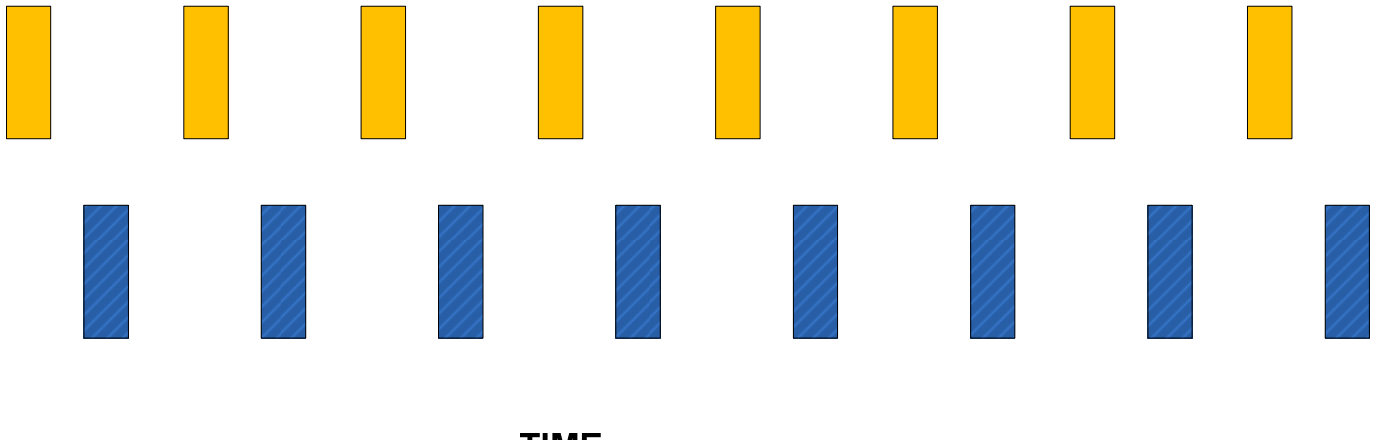
Offset piconet synchronization

Piconet limits data rate for all devices to a certain duty cycle to allow an offset start for other piconets

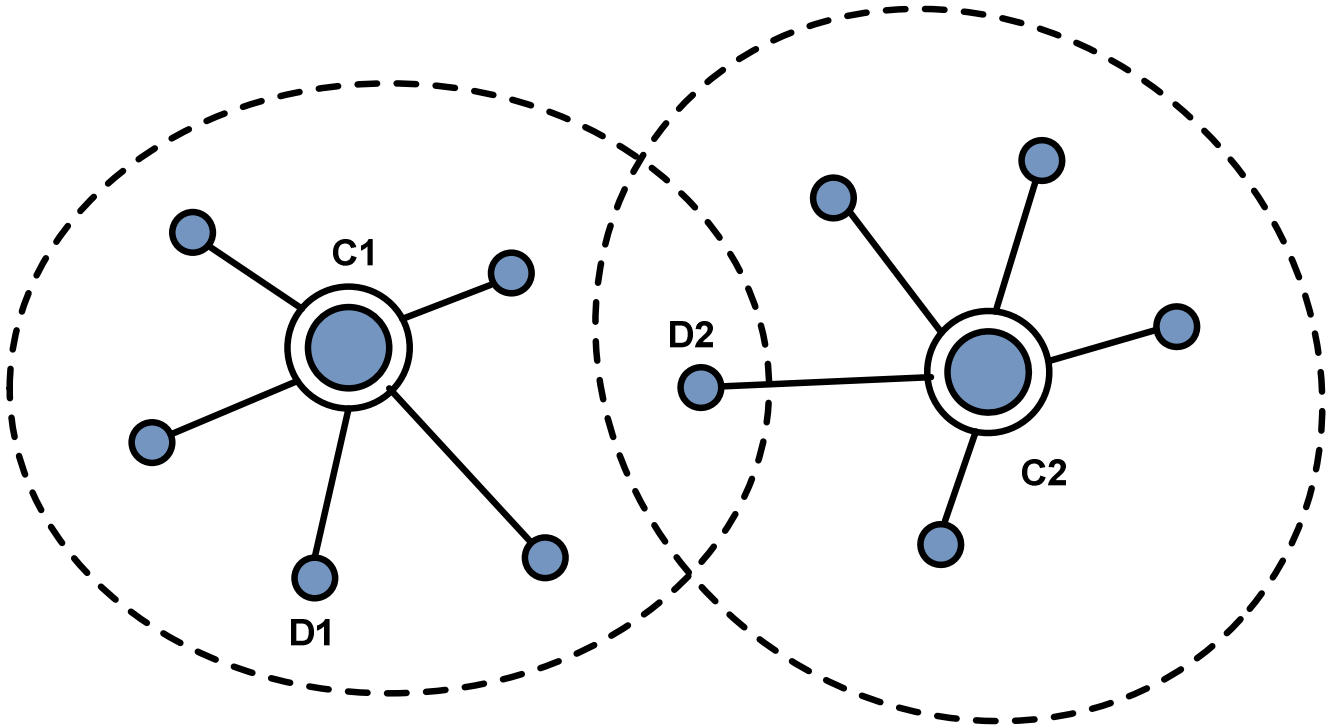
Timing information must be exchanged. C2 uses the EOP of C1 to find the offset it needs to start a new piconet and the data rates/duty cycles it can use.

Allow gap for clock drifting and multipath, if possible

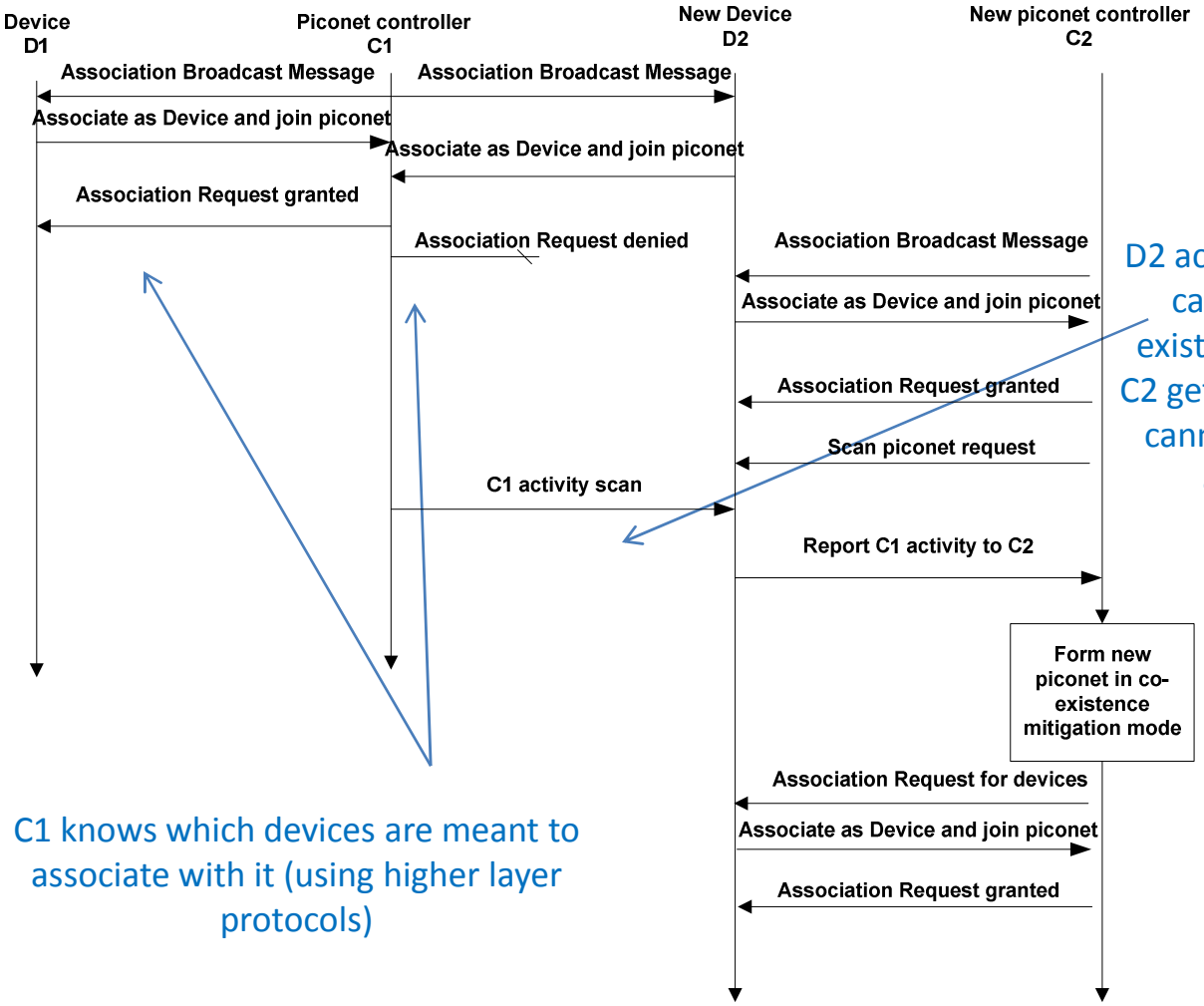
Although packets are overlapping, symbols within packet are not overlapping due to low duty cycle operation and offset synchronization



Piconet controllers cannot talk to each other (C1 – D2- C2)



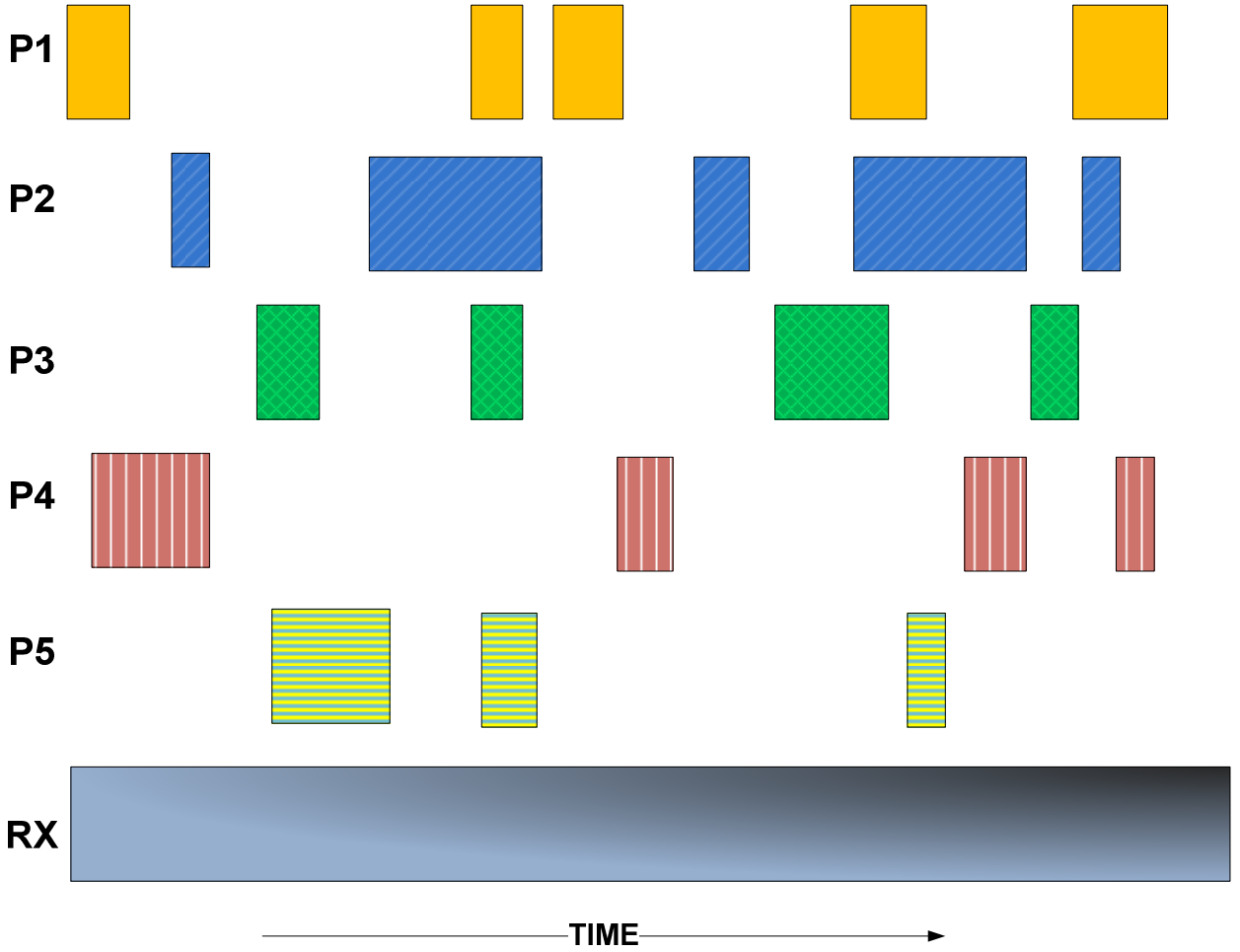
C1-C2 not possible but C1-D2-C2 (CM)



D2 acts as a "listen-only" relay for C2 in this case and relays information about the existence of another piconet to C2. Hence, C2 gets limited visibility into C1. Although C2 cannot talk to C1, C2 can learn about C1's activity for operation in CM mode

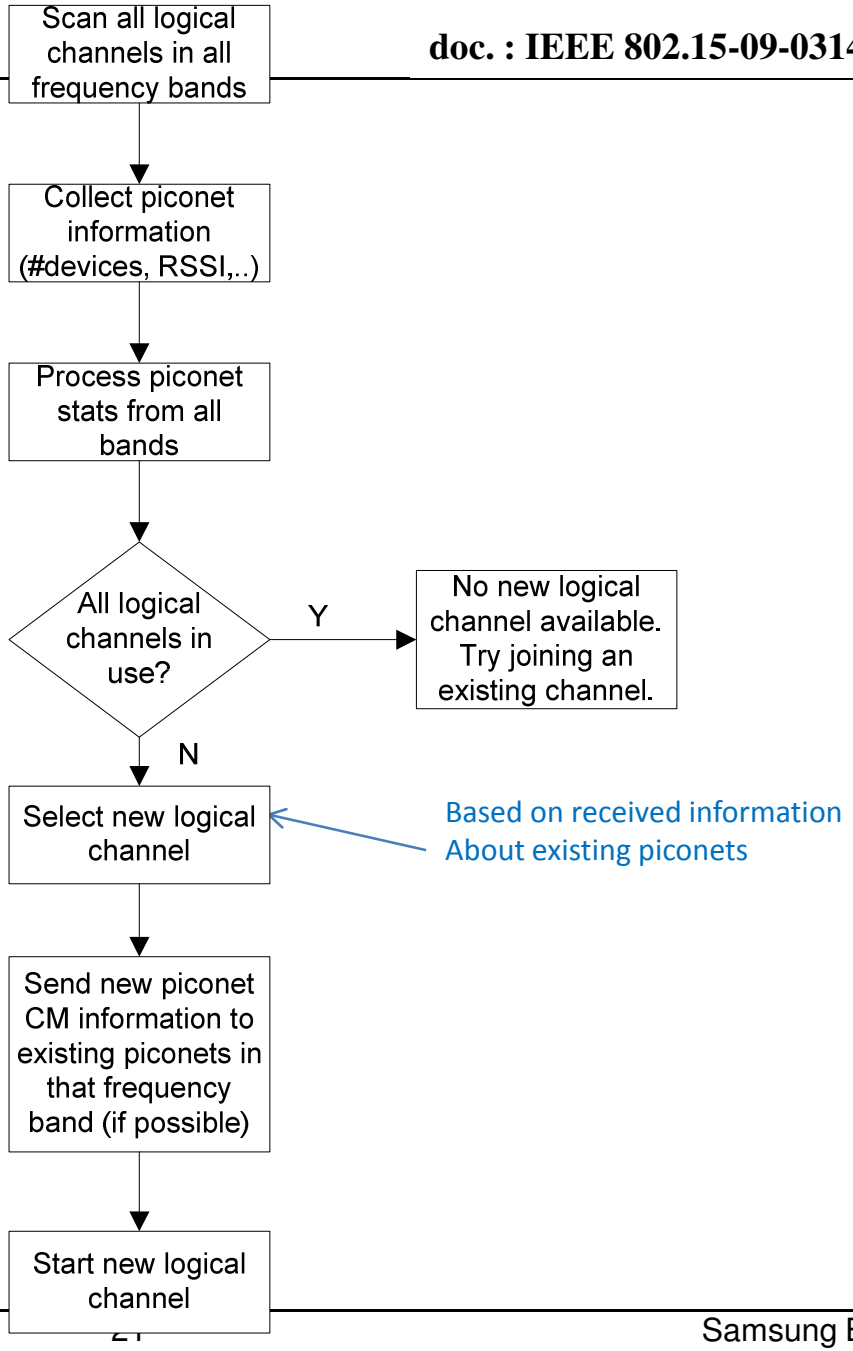
C1 knows which devices are meant to associate with it (using higher layer protocols)

Co-existence mitigation (CM) – Unsynchronized piconets (collisions possible)



Co-existence mitigation Mode

(best effort channel selection to minimize collisions)



Parameters used for new channel selection in CM mode

Number of devices in an existing piconet:

- This data provides information on the probability of interference seen and the amount of bandwidth available in an existing piconet.

Received signal strength indicator(RSSI)

- By looking at this information for an existing piconet, a controller trying to form a new piconet can tell how far away the devices are and what is the SINR to be expected at the receiver.

Data rates used in existing piconets:

- This information will tell the amount of interference the existing piconets will be able to tolerate if a new piconet will be formed by the controller.

Medical or QoS sensitive devices in piconet:

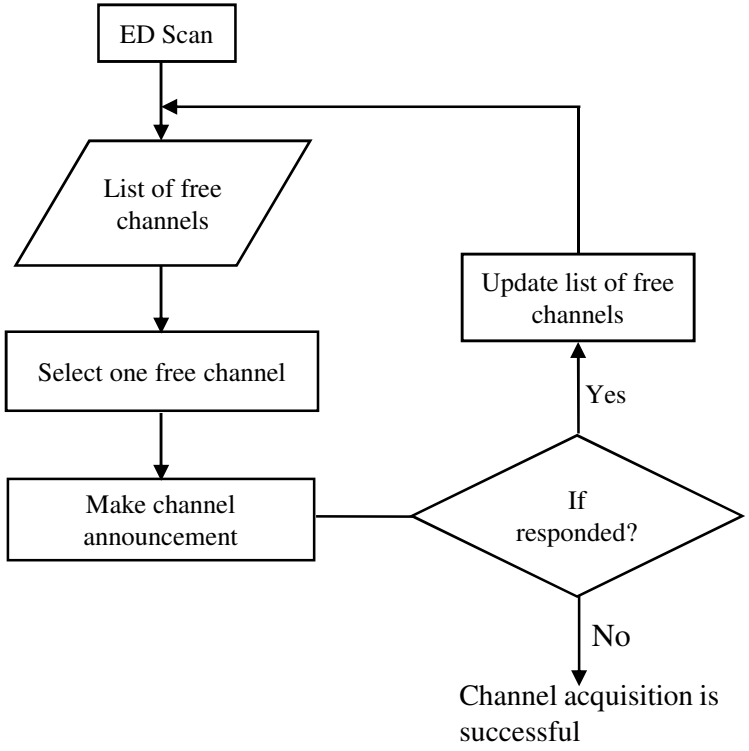
- This information will help manage co-existence to give priority to piconets that support such devices.

Agenda

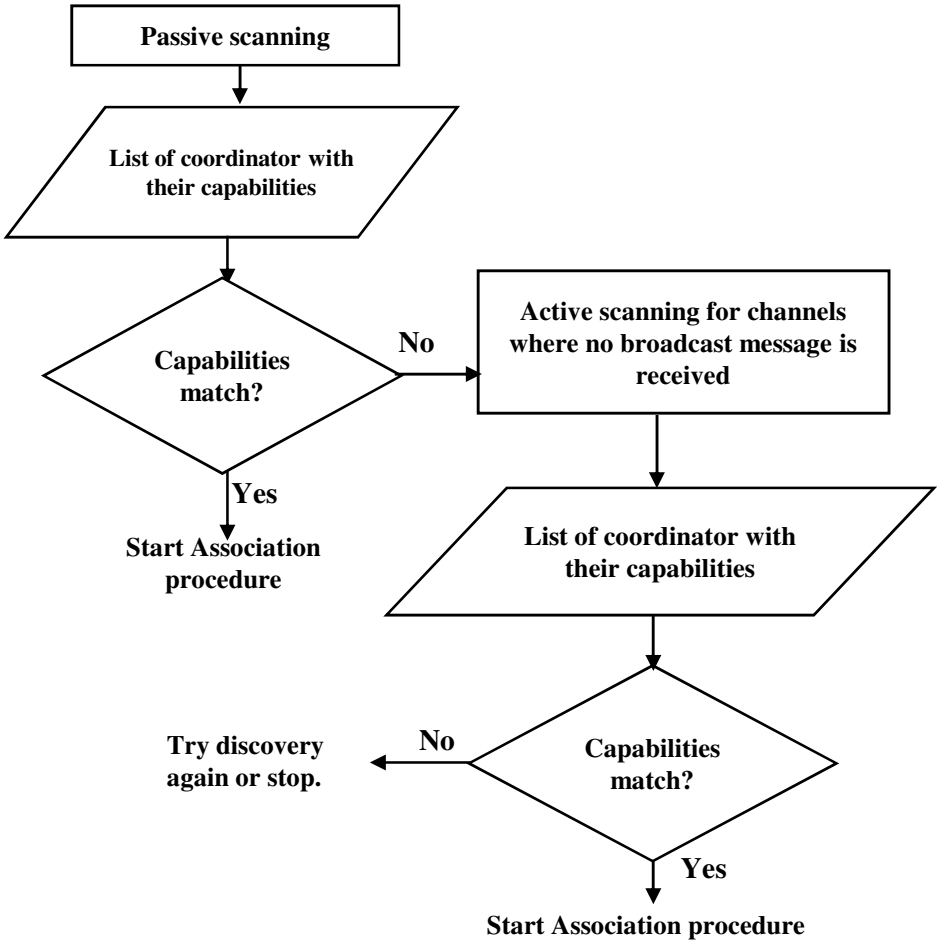
- Co-existence
- Network Management
- Security

Network setup (On-body devices) - 1

Channel selection process

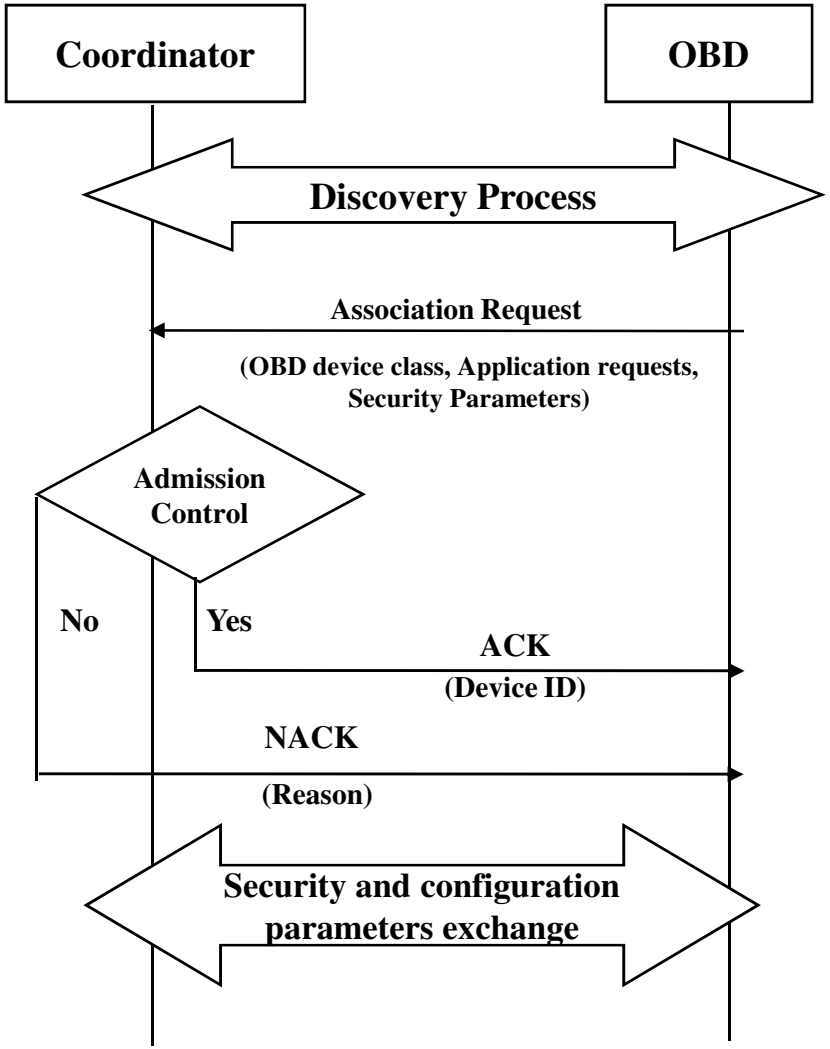


Discovery process

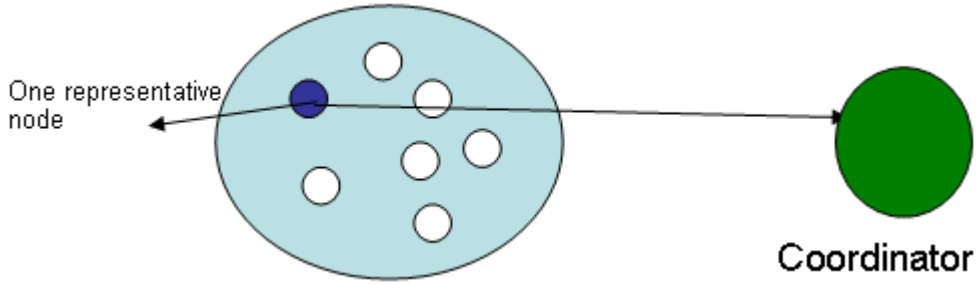


Network setup (On-body devices) - 2

Piconet join process



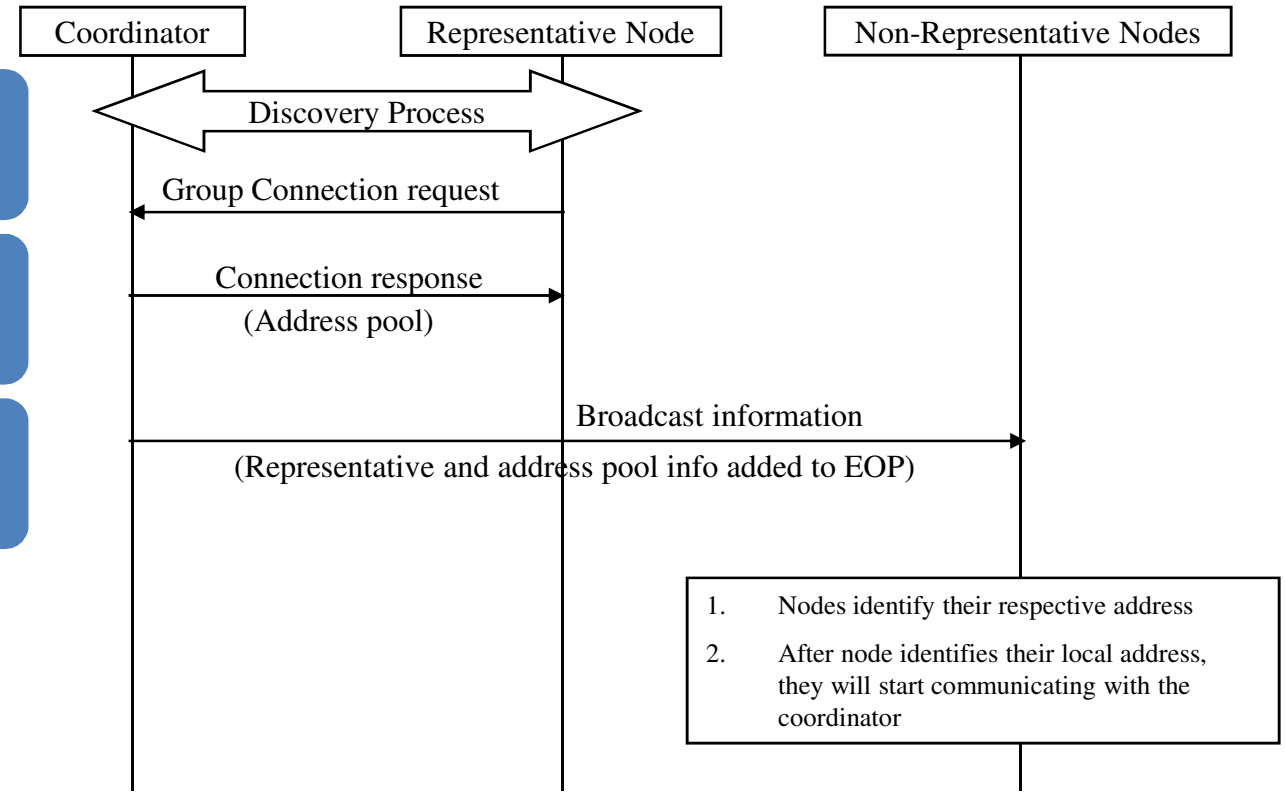
Group association for On-body



- One representative node handles association for all the devices of a group application (EEG, ECG, EMG, Gaming)
- Coordinator provides a pool of device IDs to representative
- Multiple representatives to increase robustness

Group association process

- Association latency is reduced by multifold
- Energy saving by avoid individual node association
- Ensures all the group devices are connected to a single coordinator



Network Setup (Implant)

Wakeup devices

Start the Piconet

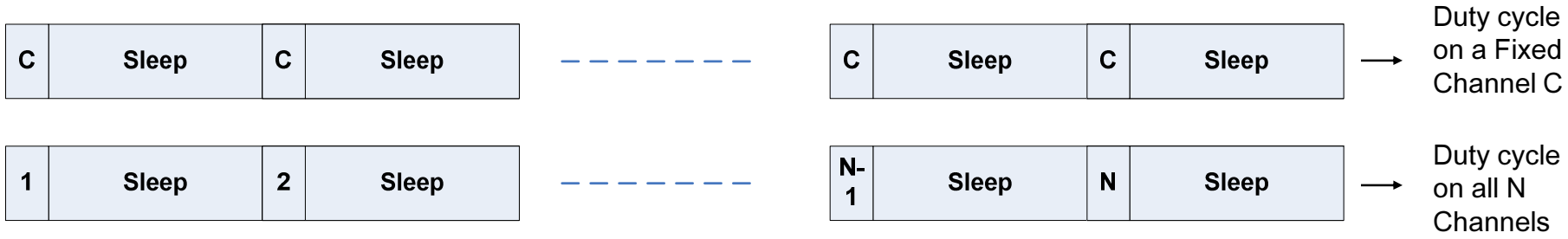
Single Device Wakeup

Wake up mechanism:

- In-band and out-of-band wakeup mechanisms are proposed

In-band Wakeup Mechanism

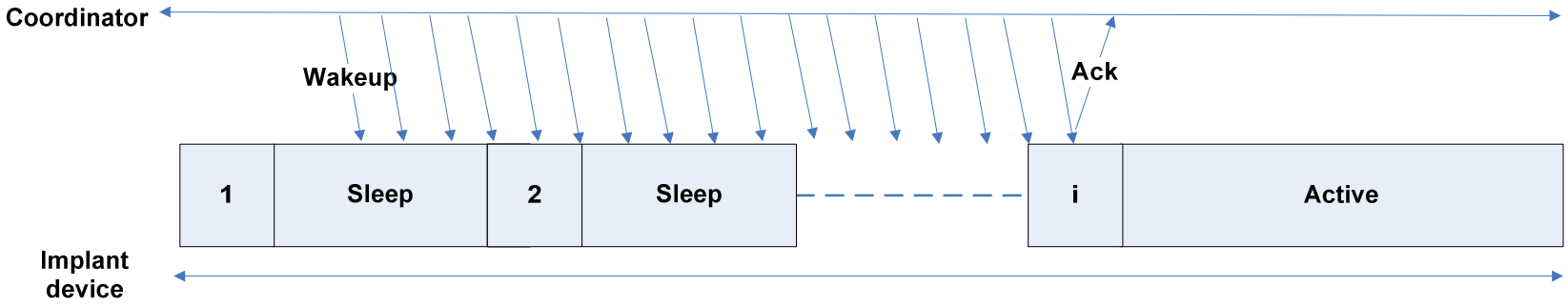
- MICS channel(s) cannot be fixed to wakeup an implant device due to LBT access criteria
- Implant device shall hop in all MICS channels to detect/wakeup signal sent by the coordinator
- Energy detector of implant receiver is duty cycled to detect wakeup signals



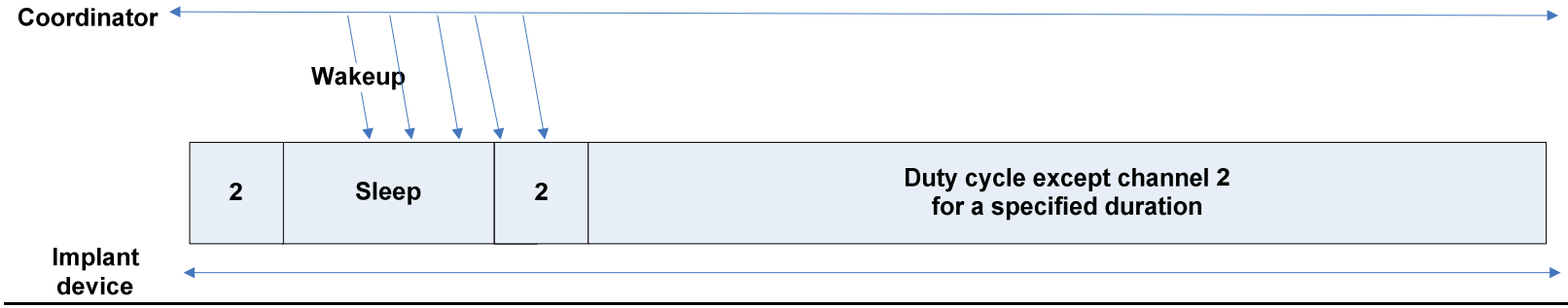
In-band Wakeup Mechanism – Single Device

- Coordinator performs LBT and selects channel
- Implant device sends an ACK on reception of intended wakeup signal and becomes active
- On reception of signal (other than intended wakeup) device stops duty cycling on the channel for a specified duration

Intended Wakeup Signal



Unintended Wakeup Signal



In-band Wakeup– Multiple Devices

Wakeup of devices one by one would lead to higher wakeup latency

Sending broadcast wakeup message for multiple devices

- Collision between acknowledgement packets

Different device may be listening at different channels

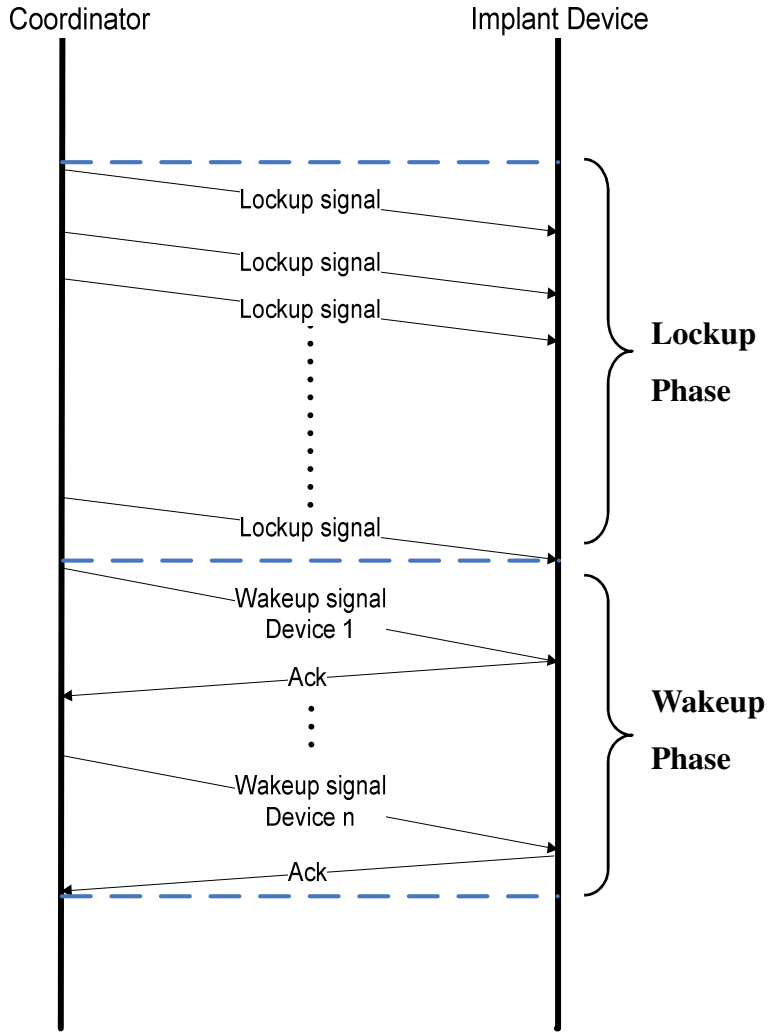
Two Phases

Lockup Phase

- Intended devices get locked to the coordinator and go to active state
- Unintended devices stops duty cycling on the channel for a specified duration

Wakeup Phase

- Locked up devices in phase 1 are woken up individually

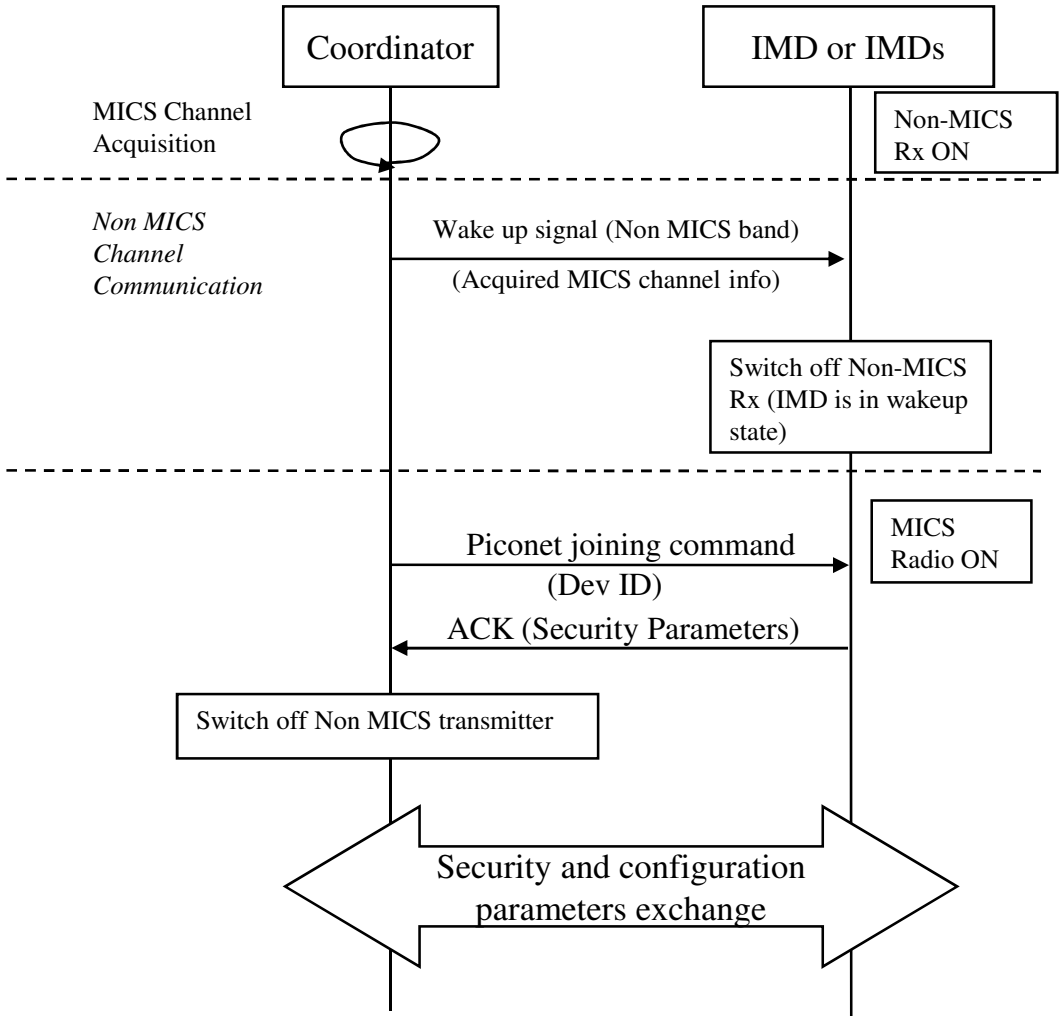


Network setup (Implant Devices) with Out-of-Band Wakeup mechanism

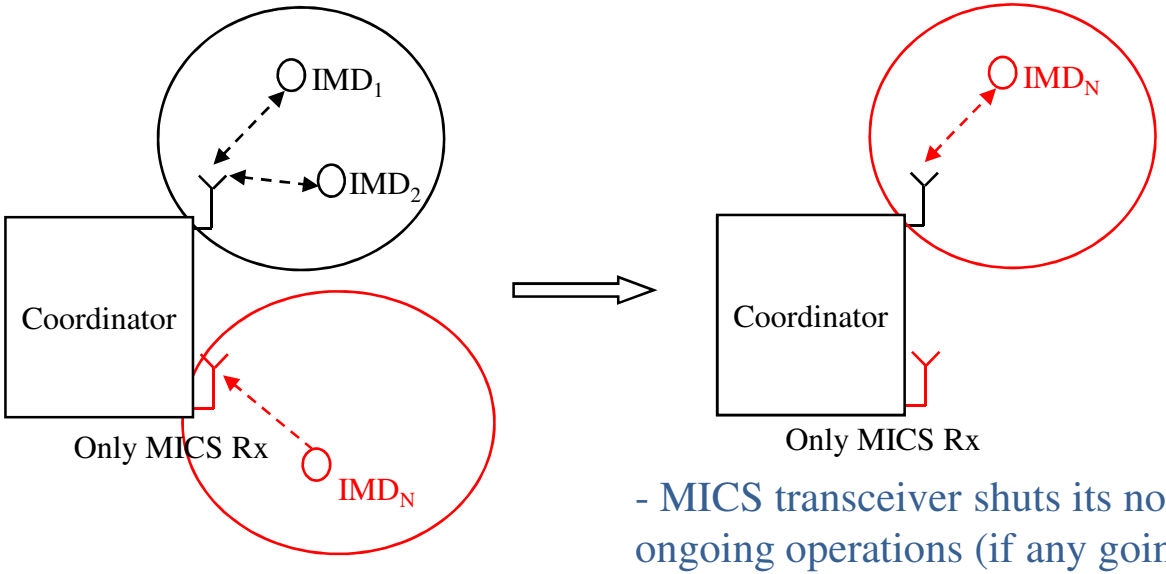
IMD wakeup & association are initiated by coordinator.

Wake up signal on non-MICS and following communication - independent events, communicated on different radio. conserves energy by reducing duty cycle of the non-MICS receiver

Implant network does not require discovery process. Coordinator pre-configured with MAC address of IMDs.



Emergency Handling



- Emergency transmitted by IMD
- Emergency signal will have different preamble or frame bit

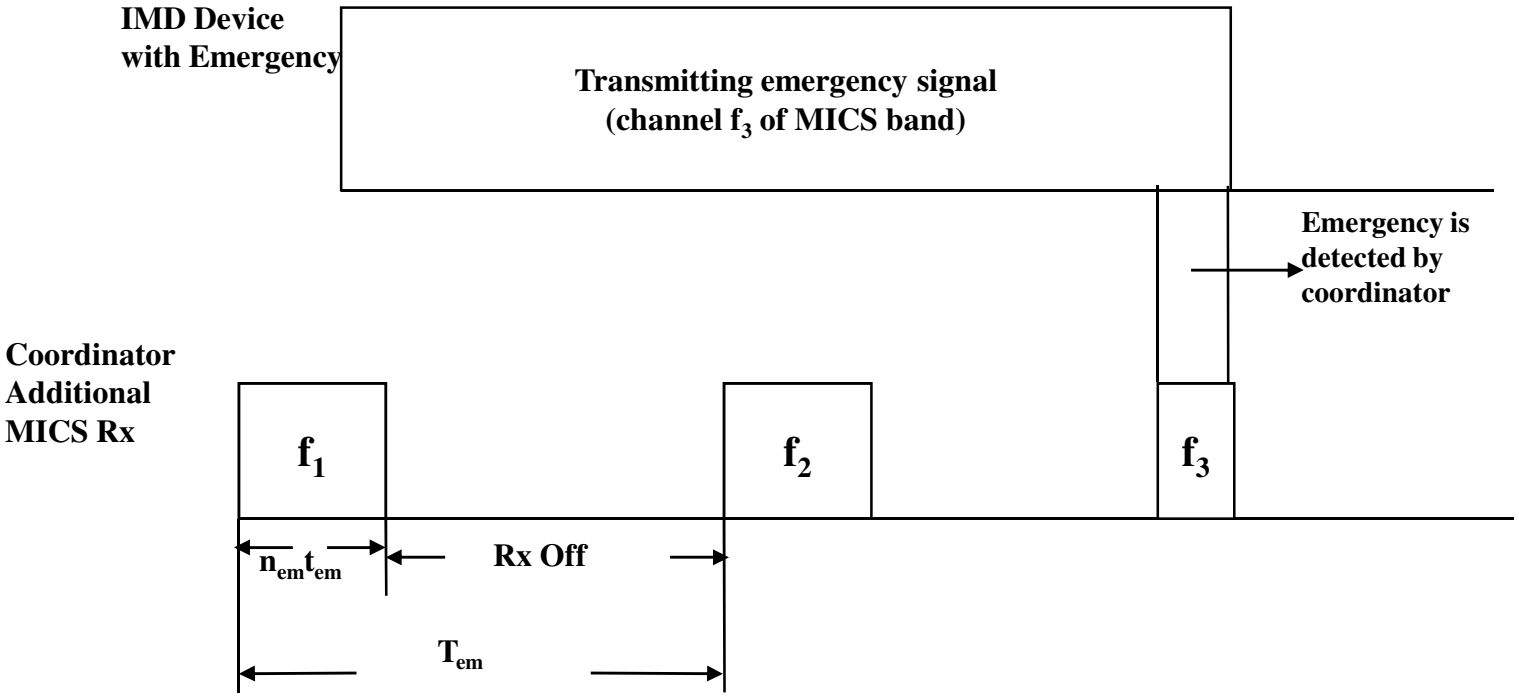
- MICS transceiver shuts its normal ongoing operations (if any going on) and handle only emergency.
- MICS transceiver shifts to the channel selected by emergency device.

Handles multiple emergency

Latency < 1 sec

Simple, low energy and reliable

Duty cycle of energy detector module of additional MICS RX



Agenda

- Co-existence
- Network Management
- Security

Security in BAN

BAN Requirements:

- Multi-level security is desired
- Highest level of security shall be equal to or stronger than that provided by AES 128 bits

Features Supported:

- Authentication,
- Integrity
- Confidentiality
- Replay protection

Security procedure

One security level negotiated per session. The security parameters negotiated depend on application and device requirements.

A device (client) has the capability to store temporal keys and frame counters until keys are renegotiated in a later session.

Coordinator preconfigured with following details

- Security Table that stores shared keys for a client. Keys are identified by an identifier: Master Key ID- MKID
- One of the MKID is set as the default key

BAN device(client) also preconfigured with security keys and the corresponding MKID.

Security Control Field defined to facilitate the device to select one of the multiple levels of security available for wide range of devices and applications.

Security Algorithm specified in the Security_Algorithm_Used field.

Security Control Field, Security_Algorithm_Used are exchanged during piconet join procedure.

Security procedure (contd.)

Authentication uses a 4-way handshake procedure which authenticates that both the peer devices share the same master key. Keys necessary for integrity and privacy protection are generated

Privacy - AES counter mode

Integrity – AES CBC-MAC used for MIC

For group devices - After association, only the representative node does the authentication procedure and then the coordinator broadcasts the MKID and random nonces used in key generation

Replay protection is provided by using a incremental counter that is present in data frames exchanged from BAN device.

Standard frames like Poll, Ack or other control frames, sent from the coordinator need not be encrypted or integrity protected; (this is to avoid possible brute force attack, with known plaintext.)

Bit 0 – Authentication	Bit 4 – Use 64 bit keys
Bit 1 – Integrity protection	Bit 5 – Use 128 bit keys
Bit 2 – Privacy	Bit 5 – Use 256 bit keys
Bit 3 – Replay protection using frame counters	Bits 6-7 – RFU

Simulations

Presented as part of Samsung PHY and MAC proposals

Continuing testing and validation of design

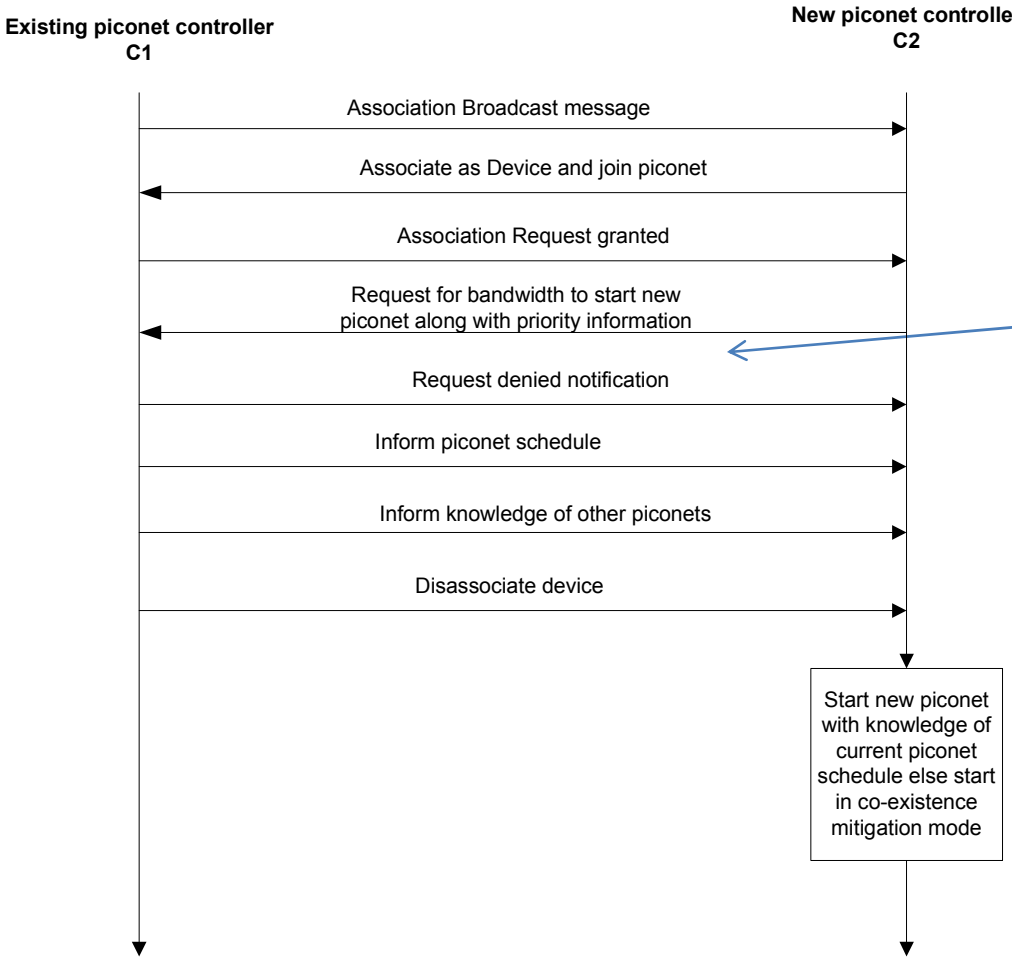
- Value input for collaboration

Summary

- Piconet co-existence among the most important issues for UWB in BAN
- MAC can assist in piconet co-existence in BAN by forming non-interference and co-existence mitigation modes
- Several methods proposed to attain piconet co-existence
- Joint MAC and PHY design proposed to solve co-existence for BAN
- Network management and security mechanisms also proposed for body area networks

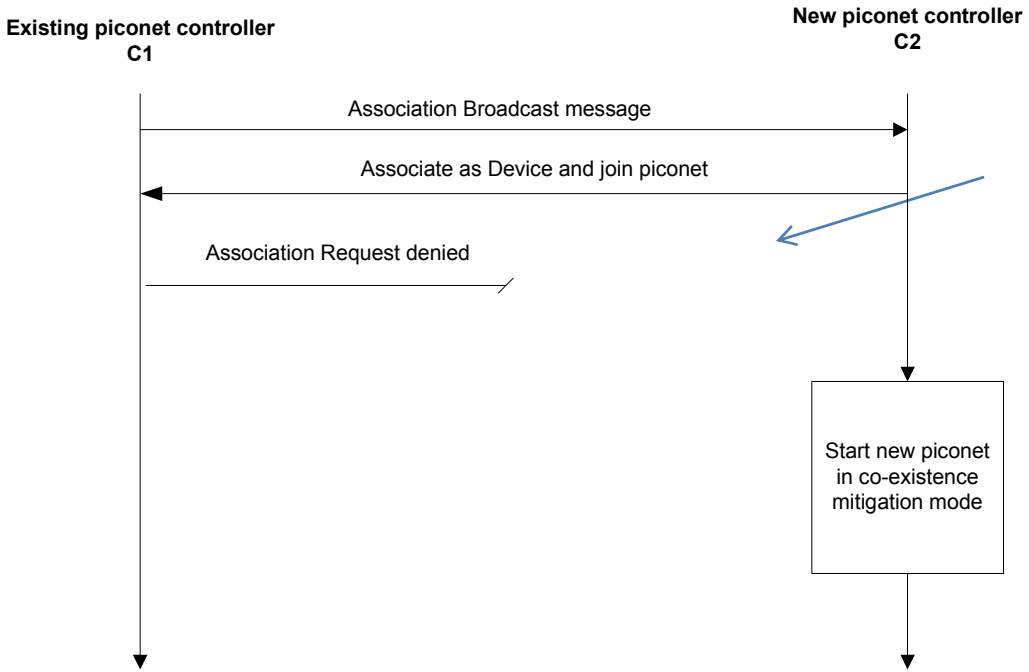
Back-up Slides

Denied Time Resource (NI/CM)



When existing piconet has higher priority, the existing piconet may not be willing to make any adjustments but may provide information about its schedule to the new piconet allowing the new piconet to decide whether it can start a new piconet in that band in a NI mode or start in CM mode

Denied association (CM)



When existing piconet has higher priority, and is doing some critical applications, it may refuse to associate any new devices or new piconet controllers.
In this case, C2 will have to start in a CM mode

Resource allocation

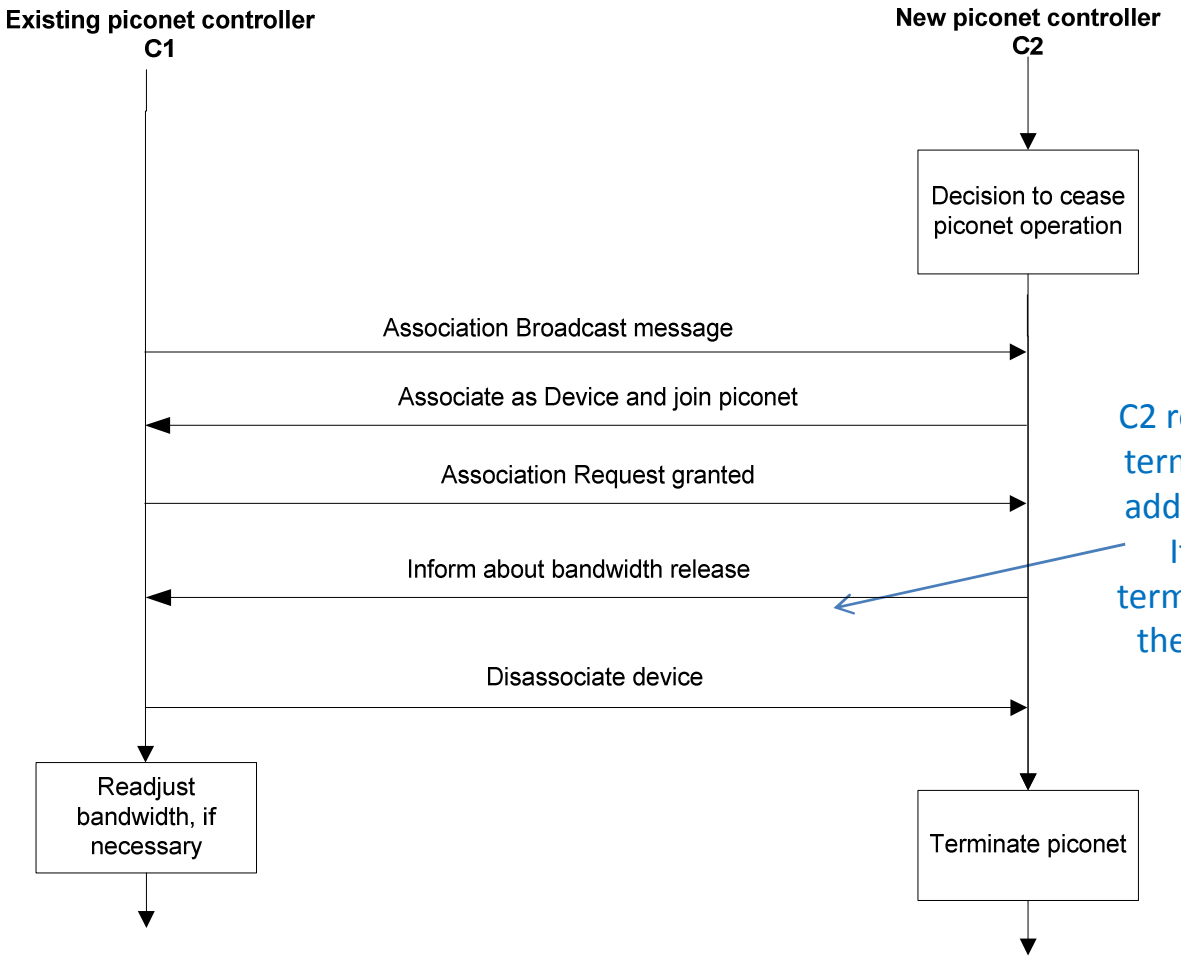
Each piconet can have a guaranteed resource reservation of up to x%. Piconet can reserve excess bandwidth for its applications, based on its estimate, which must be released for sharing with piconets, with higher or equal priority, when the controllers can talk to each other. [medical piconets]

- x = 10% (20% per frequency band) to support 10 medical piconets

Bandwidth management is performed only during piconet formation and termination

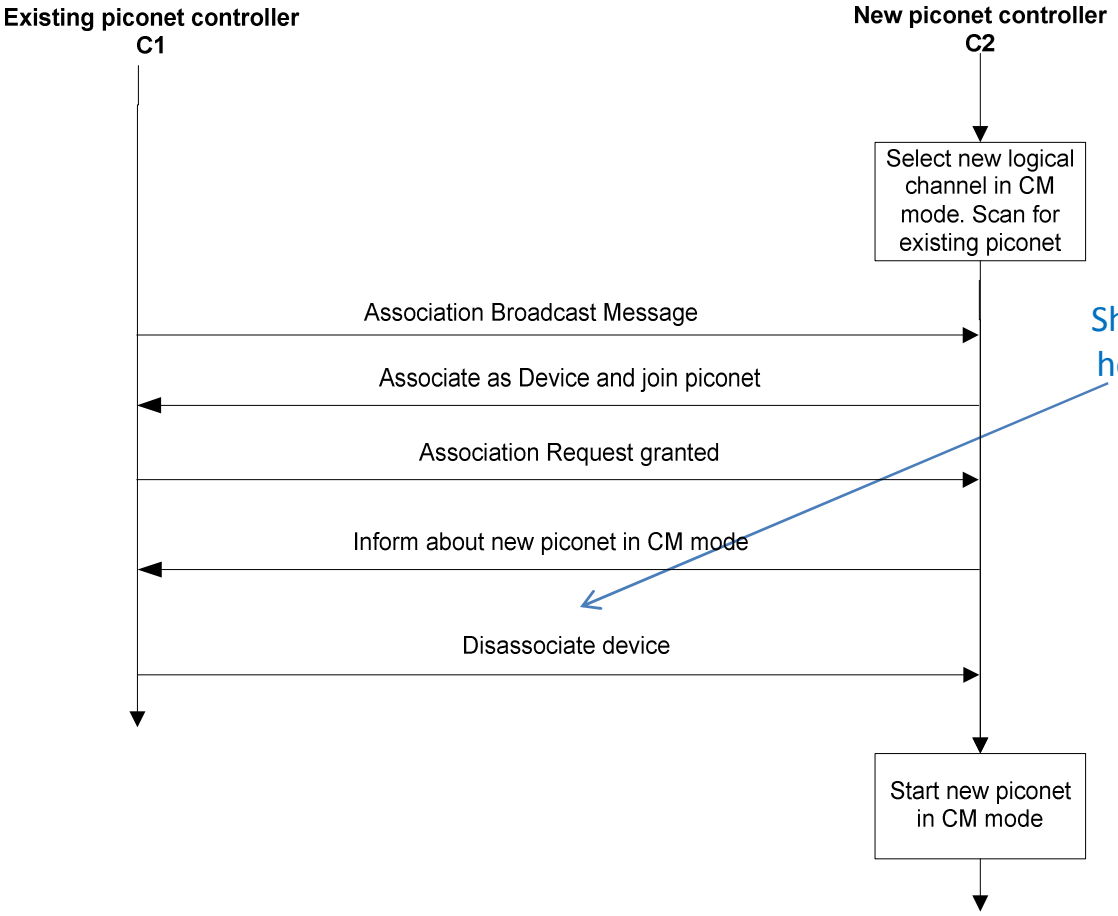
- May require significant time to optimize across multiple piconets in a dynamic environment

Piconet termination



C2 releases bandwidth to C1 upon piconet termination. C1 can now make use of the additional bandwidth for its applications. If there are “n” piconets before the termination that are talking to each other, they can get a (n/n-1)X improvement in bandwidth.

Sharing new CM piconet formation



Sharing information about new CM piconet helps existing piconet to make decisions in the future for better co-existence