IEEE P802.15
Wireless Personal Area Networks

Project	TG6 Body Area Networks	
Title	Samsung MAC proposal for IEEE 802.15 TG6 – Body Area Networks	
Date Submitted	4th May 2009	
Source	Ranjeet K. Patro, Ashutosh Bhatia, Arun Naniyat, Thenmozhi Arunan, Giriraj Goyal, Kiran Bynam, Seung-Hoon Park, Noh-Gyoung Kang, Chihong Cho, Euntae Won, Sridhar Rajagopal, Farooq Khan, Eui-Jik Kim, Jeongsik In, Yongsuk Park	Address: [66/1, Bagmane Tech Park, Byrasandra, C.V.Raman Nagar, Bangalore, India] Voice: :[+91-80- 41819999] Fax: [+91-80- 41819999] Email:[rkp.atd@samsung.com, ashutosh.78@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.	
Purpose	To trigger discussion and initiate merger with other group members of TG6.	
Notice	This document has been prepared to assist the IEEE P802.15. It is offered as a basis for discussion and is not binding on the contributing individual(s) or organization(s). The material in this document is subject to change in form and content after further study. The contributor(s) reserve(s) the right to add, amend or withdraw material contained herein.	
Release	The contributor acknowledges and accepts that this contribution becomes the property of IEEE and November be made publicly available by P802.15.	

Table of Contents

1. Scope

This draft is being submitted to IEEE 802.15 Task Group 6 as a candidate MAC proposal, in response to the Call for Proposal (15-08-0811-02-0006-tg6-call-proposals) issued on 23rd January, 2009. This draft covers entire Media Access Control (MAC) protocol for Body Area Networks that is, fully compliant with the approved Project Authorization Request (PAR) and technical requirements document (TRD) that have been developed by the 802.15 TG6.

2. MAC Requirements of IEEE 802.15 TG6 - BAN

The complete list of MAC technical requirements are derived from the approved technical requirements document (15-08-0644-09-0006-tg6-technical-requirements-document) and 15-08-0831-05-0006-tg6-proposal-comparison-criteria.

- MAC transparency – Support of multiple PHYs
- Support of topology
- Support of scalable data rate
- Support of number of devices
- Medical application traffic latency (less than 125 ms)
- Non-medical application traffic latency (less than 250 ms)
- Non-medical application traffic jitter (less than 50 ms)
- Low power consumption
- Availability of 99%
- Capability of providing fast (<1 sec) channel access in emergency situations (alarm messages)
- Time to associate a node to BAN
- Coexistence of 10 BANs in the proposed implant communication band
- Coexistence of 10 BANs in the proposed on-body communication band
- Support of security

3. Summary of requirements accomplished by the proposal

Sl No.	Technical Requirements	Achieved (Yes/No)	Remarks
1	MAC transparency – Support of multiple PHYs		
2	Support of topology		Star topology, design can be extended to multi-hop star
3	Support of scalable data rate		Flexible channel access mechanism
4	Support of number of devices		Design can support load of 256 nodes with sufficient data rate is availability
5	Packet delay in Medical applications (< 125 ms)	Yes	
6	Packet delay in Non-medical applications (< 250 ms)	Yes	
7	Packet Delay Variation in Non-medical application (< 50 ms)	Yes	Subject to bandwidth availability
8	Low power consumption	Yes	
9	Availability of 99%	Yes	Subject to traffic load
10	Capability of providing fast (<1 sec) channel access in emergency situations (alarm messages)	Yes	
11	Time to associate a node to BAN	Yes	Association latency is reduced drastically in group based association scheme
12	Coexistence of 10 BANs in the proposed implant communication band	Yes	A Mechanism is proposed, simulation results yet to be obtained
13	Coexistence of 10 BANs in the proposed on-body communication band	Yes	A Mechanism is proposed, simulation results yet to be obtained
14	Support of security	Yes	Multi level security protocol is proposed

4. MAC description

The focus of the IEEE 802.15 TG6 can be broadly categorized into two types, i.e. implant communication and on-body communication. Implant communication involves medical applications (e.g. Pacemaker, Glucose meter etc) and on-body communication involves both medical (e.g. ECG, EMG etc) and non-medical applications (e.g. Interactive gaming and Entertainment etc). It is desired to design a single MAC which needs to support transmission of data over implant communication band and on-body communication band, and satisfy the functional requirements of both implant communication and on-body communication.

Network Topology

To meet the application requirements, an IEEE 802.15 TG6 - Body Area Network (BAN) may operate in star topologies or extended star topologies. Samsung's initial proposal is based on the star topology; however the proposed solution has a scope to expand it to extended star topology in future. In a star topology, as shown in Figure , the communication session is established between an end device and a BAN Coordinator. For on-body communication, both coordinator and device can initiate or terminate the communication, additionally coordinator can route data from one device to another device. For implant communication, device can not initiate communication except in occurrence of an emergency event at device. . **In BAN, primarily, a device generates traffic related to one application**. Coordinator may or may not generate traffic related to an application

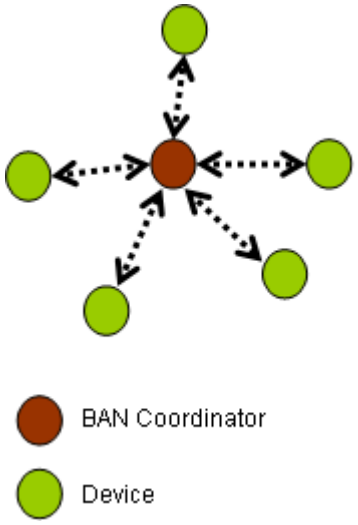


Fig : A star topology

Architecture

An IEEE 802.15 TG6 device may contain PHY1 or PHY2 or both PHY1 and PHY2, which contains transceiver for signal transmission and reception. The PHY1 transceiver operates in a frequency band suitable for implant communication and PHY2 transceiver operates in a frequency band suitable for on-body communication. An IEEE 802.15 TG6 device also contains a MAC and LLC layer to access a channel of a selected frequency band for all kind of data transfer.

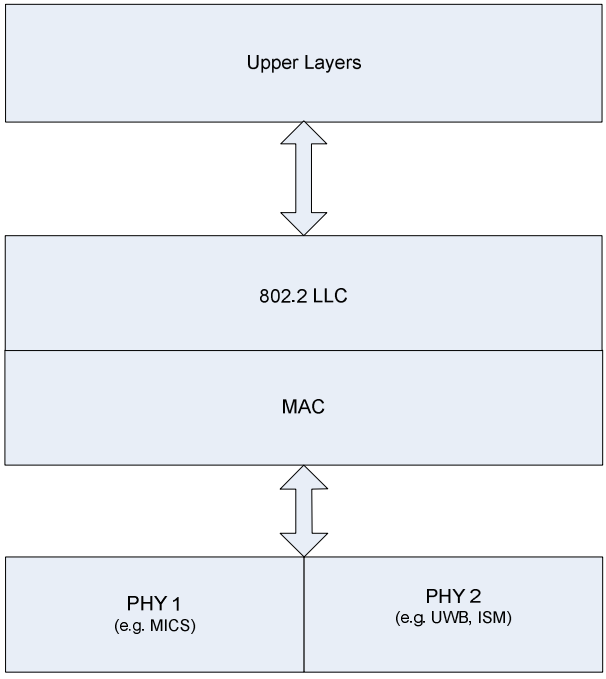


Fig : Device architecture

5. Channel Access Mechanism for On-body Communication

Traffic types and requirements

Class	Description	Performance Requirements	Example
T1	CBR low data rate traffic	• Low power consumption • Packet delay required by the application, like – 125 ms for patient monitoring – 250 ms for Gaming • Support of large number of devices	• Patient Monitoring • ECG • Fitness Applications • Interactive Gaming
T2	CBR high data rate traffic	• Low power consumption • Packet delay	• EMG • Uncompressed Audio
T3	VBR traffic	• Delay and Packet delay variation • Maximization of bandwidth utilization • Power efficiency is optional	• Real-time Multimedia Streaming

Traffic generated from most of the BAN applications can be mapped into one of the three categories as mentioned above. First category refers to the constant arrival low data rate applications where arrival rate at devices of an application is at most 10 kbps. Second category refers to the constant arrival high data rate applications where arrival rate at devices of an application is more than 10 kbps. Third category refers to the applications generating variable bit rate traffics.

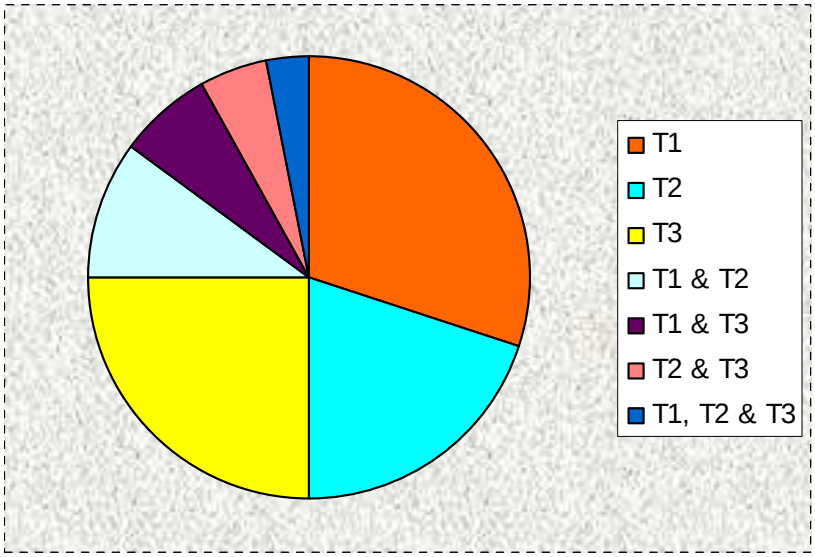
Design approach for on-body communication

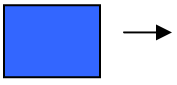
Objective: To design a channel access mechanism that can meet the performance requirements of three class of traffic.

In BAN, the device associated with a coordinator may generate traffics specific to one application. A BAN serving only one application or one class of traffic is a possible scenario. Similarly, device related to multiple class of traffic may be part of the same BAN. Our design theme is

- Standalone applications (e.g. only T1 or T2) should have optimal performance
- Incase of co-existence of multiple class of traffic,
    - Priority order: T1 → T2 → T3
    - Scheduling of low priority traffic should not affect the performance of high priority traffic

Scenario example:



 A BAN network with devices generating T1, T2 and T3 class of traffics

- Performance of T1 and T2 should be close to standalone T1 and T2 performance.
- Admit T3 traffic only if T1 and T2 performance are not affected
- With the above constraint, maximize T3 performance

Why Polling based channel access mechanism?

Polling based channel access mechanism is preferred with the proposed design approach, due to following reasons:

Inherits benefits of TDMA:
Like TDMA, in Polling, coordinator has absolute control over traffic and resource allocation. It can guarantee bandwidth and latency for the applications that require it.

Facilitates independent sleep/wakeup schedule:
Polling channel access mechanism enables fixed scheduling of devices. The poll time of the power constrained devices can be fixed in a frame cycle. This feature of Polling allows devices to sleep between two successive polls destined for the device.

No need of global synchronization:
In polling based channel access mechanism, the reception of Poll message is an indication for transmission time. Since Poll message is device specific, only device being polled can transmit the data. Therefore, device need not have to synchronize with allocated slot time while transmitting data. A coarse level synchronization may be required for better management of sleep/wakeup schedule.

Allocation of variable transmission duration:
Streaming applications generate variable bit rate traffic, where fixed allocation is not the right design candidate. Peak allocation meets the QoS requirements; however bandwidth is under utilized most of the time except burst arrivals. Average allocation may not meet the QoS requirements (delay and jitter). Polling can allocate transmission duration as required by the device to support an application.

Reliability: In BAN, some of the applications (e.g. Pacemaker, ECG etc) have high reliability requirements and the PER can go as high as 10^{-2} (referring to TRD). Polling channel access mechanism has in-built error recovery mechanism, like next Poll can be treated as an ACK or NACK. Polling can even handle lost of ACK packets.

Robustness:
Unicast poll message is the reference message for a device, where as in beacon based network beacon message is the reference message for all devices. Loss of poll message only affects the intended device and can be retransmitted. Beacon is a broadcast message

and is not acknowledged. Beacon loss has effect on network functioning. Beacon message has higher reliability requirement than poll message.

Facilitates ease of integration and Single MAC design:
The FCC rule for implant communication: "Except in an emergency case, an implant device can not initiate communication except to the response from an external coordinator". Polling is the most suitable channel access mechanism for implant communication. Poling mechanism for on-body communication eases out integration aspects of channel access mechanisms and design of Single MAC for Body Area Networks.

Frame structure

A frame design is proposed to TG6 for on-body applications that consist of a Poll Period (PP) and a Contention Period (CP). Poll period is responsible for T1, T2 and T3 traffic transfer and Contention period is responsible for best effort traffic and network management traffic transfer. The detail frame design part will be covered in the next section.

F_c is the frame cycle time, $F_c = PP + CP$

Features of the frame:
- Duration of Poll Period (PP) depends upon the number of device associated
- Frame cycle (F_c) is fixed if T_1 and T_2 traffics are present (F_c does not change even when a new device associates)
- Poll period can extend up to F_c - *min*CP
- *min*CP is the minimum contention interval required for network management traffic transfer

***EOP* message:**
- It is a broadcast message

- Indicates the end of poll period and the beginning of contention period
- Contains length information of contention period
- Contains Piconet related information (Mode of coordinator, Options, Capability of Piconet, etc)

Fixed frame cycle design:

(i) $F_c \leq d_{\min}$ ---------- (1)

The frame cycle length is bounded by the minimum delay requirement. As per the TRD, the minimum delay requirement value is 125 ms.

(ii) $$F_c \geq \frac{\sum_{i=1}^{n}(P_i + S_i)}{R} + 2n * SIFS$$ ---------- (2)

Let us assume that frame cycle needs to be designed for *n* number of devices, given the condition that available data rate is sufficient to support traffic generated from *n* devices. The frame cycle length should be large enough such that it can support data arrival at *n* devices.

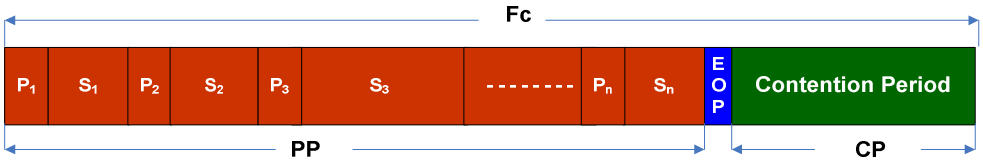
Pi = Poll size for i^{th} device
S_i = Allocated transmission duration for i^{th} device
R = Data rate of the physical channel
SIFS = Short Inter Frame Space duration

(iii) F_c is fixed

Power efficiency is one of the requirements for T_1 and T_2 class of devices. Fixed frame cycle design for T_1 and T_2 allows device to perform duty cycling and save power.

Polling mechanism for T_1

- A device is polled with period F_c
- **When Polled, device has at most one packet of size < MTU to transmit**
- Arrival rate ≤ $A_{m,}$ Where A_m is maximum arrival rate for T1



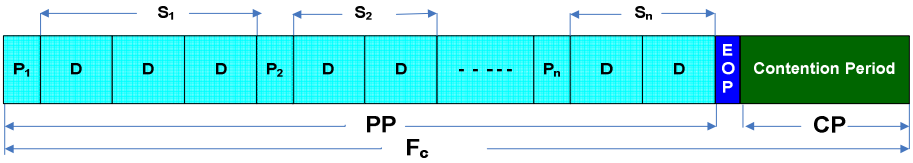
Power saving:
- F_c is fixed, S_i is fixed → Poll time of i^{th} device is fixed
- Device can go to sleep after data transmission and wakeup before the poll time
- Very low data rate devices may perform packet aggregation

Delay:
- Packet latency is bounded by F_c, if data not in error

Bandwidth Efficiency
- Variable allocated slot duration (Si) for different arrival rates

Polling mechanism for T2

- When Polled, device may have more than one packet of size MTU to transmit
- Allocated slot time Si, is to accommodate multiple packet transmission of size MTU
- Arrival rate > A_m, Where A_m is minimum arrival rate for T2
- Si is calculated based on packet arrival rate



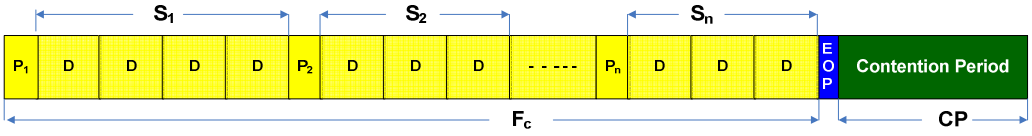
Power saving:
- F_c is fixed, S_i is fixed → Poll time of i^{th} device is fixed
- Device can go to sleep after data transmission and wakeup before the poll time

Delay:
- Packet latency is bounded by F_c, if data not in error

Bandwidth Efficiency
- Single Poll for multiple Packets

Polling mechanism for T3

- ***F_c* is variable, Polling time is not fixed**
- The device transmits all the packets in the buffer that were stored, when polled
- One data packet (D) is of MTU size

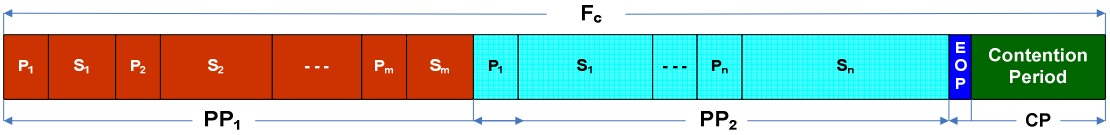


Power
- Power is not a major constraint T3 applications (devices are active all the time)

Delay:
- No fixed F_c , delay is variable

Bandwidth Efficiency:
- Dynamic slot allocation achieves higher throughput

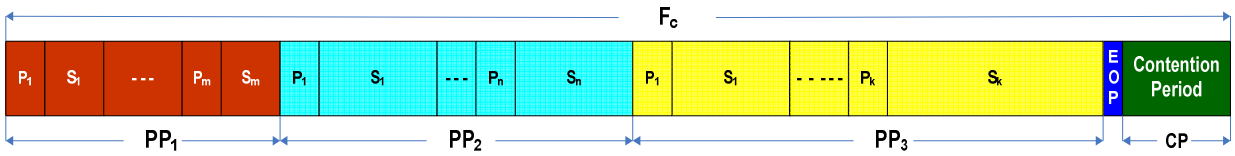
Integrated Frame Structure



Description:

- **T_1 has highest priority**
  - **Bandwidth is reserved to support required applications in T_1, whenever T_1 coexist with other class of traffic**
- Poll time is fixed for T_1 device even in co-existence scenario
- F_c is fixed, $F_c = PP_1 + PP_2 + CP$

Integrated Frame Structure



Description:

1. **T_1 has highest priority**
   - Bandwidth is reserved to support required applications in T_1, whenever T_1 coexist with other class of traffic
2. **T_2 has higher priority than T_3**
   - Admission of a new T_2 application may affect T_3 application (Delay, PDV)
   - Admission of new T_3 application does not affect T_2 application performance
3. **Support of T_3 application is maximized while following 1 and 2.**

- F_c is fixed, $F_c = PP_1 + PP_2 + PP_3 + CP$
- PP3 may take different value in different frame and bounded, $PP_3 \leq F_c - (PP_1 + PP_2 + \text{minCP})$

Error Recovery Mechanism for on-body communication:

In Body Area Networks, Packet Error Rate can go as high as 10^{-2} (Referring to TRD). An error recovery mechanism should be supported by the MAC to achieve the desired availability of 99%. Like any other error recovery mechanism, acknowledgement from destination is the indication of the successful packet transmission from a source to a destination.

Acknowledgement Policies:

Four acknowledgment policies are discussed**: No-ACK, Immediate-ACK**, and **Block –ACK**.

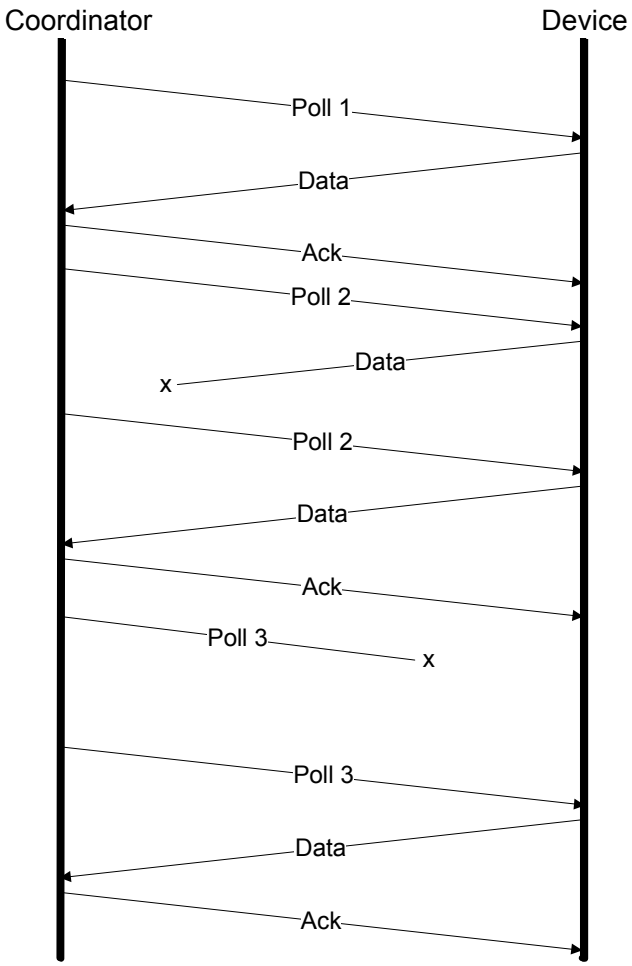
No-ACK:
In "No ACK" policy, the source device assumes that Packet has been successfully transmitted. e.g. EOP message does not require any ACK.

Immediate -ACK:
In immediate ACK policy, on reception of a packet, recipient device sends an ACK immediately. T_1 class of packets requires "Immediate ACK". Detail error recovery mechanism for T_1 class of packets is described below.

Poll packet is transmitted by the coordinator. After transmitting the Poll packet, the coordinator expects to receive data packet in response and takes one of the following actions:

- If the coordinator does not receive data packet from a device, it shall assume either device did not receive the poll packet or device received poll packet and data packet transmitted by the device is lost. To continue the operation, the coordinator shall retransmit the poll packet.
- If the coordinator receives a data packet from a device, the coordinator shall transmit the ACK packet. On receiving the ACK packet device can go to sleep state.
- After transmitting the ACK packet, coordinator shall transmit the Poll packet for next device.
- If ACK transmitted from the coordinator is lost, device goes to sleep mode after receiving the Poll packet of next device or time out. Receiving Poll packet for next device is an indication that data is successful but ACK is lost.

ACK and Poll message are not combined, ACK packet helps in saving power when packet size is small.

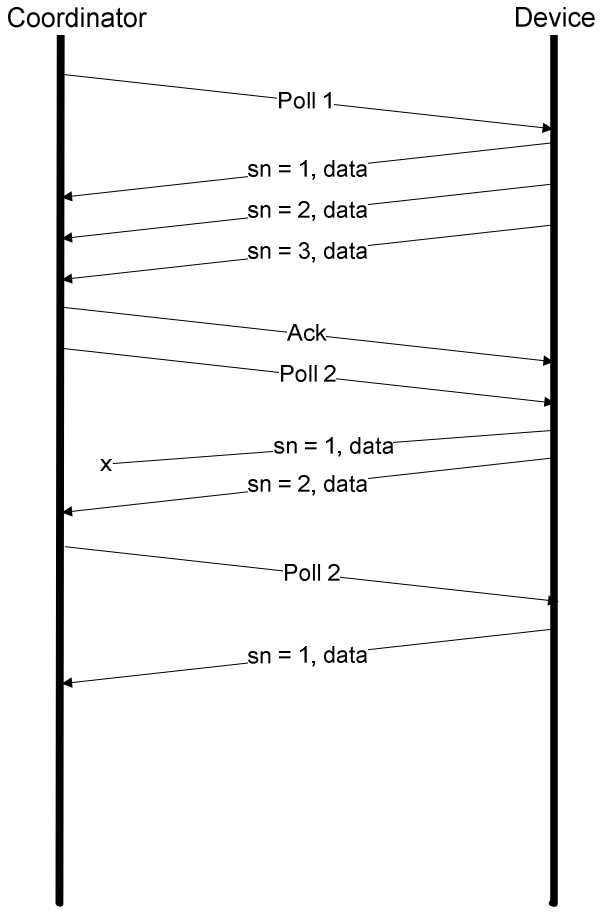


Block -ACK:
In Block ACK policy, on reception of the last packet, recipient device sends a Block-ACK. T_2 and T_3 class of packets requires "Block ACK".

A. Detail error recovery mechanism for T_2 class of packets is described below.

Let us assume, on receiving Poll, device is allowed to transmit L number of MTU size packets. After transmitting the Poll packet, the coordinator expects to receive L number of data packets in response and takes one of the following actions:
- If the coordinator does not receive all data packets from the device, it shall assume either device did not receive the poll packet or device received the poll packet and some data packets transmitted by the device are lost. To continue the operation, the coordinator shall retransmit the poll packet with a bitmap indicating the packets which are not received successfully.
- If the coordinator receives all data packet from a device, the coordinator shall transmit the ACK packet. On receiving the ACK packet device can go to sleep state.
- After transmitting the ACK packet, coordinator shall transmit the Poll packet for next device.
- If ACK transmitted from the coordinator is lost, device goes to sleep mode after receiving the Poll packet of next device or time out. Receiving Poll packet for next device is an indication that data is successful but ACK is lost.

ACK and Poll message are not combined, ACK packet helps in saving power when device has less than L number of packets to transmit.

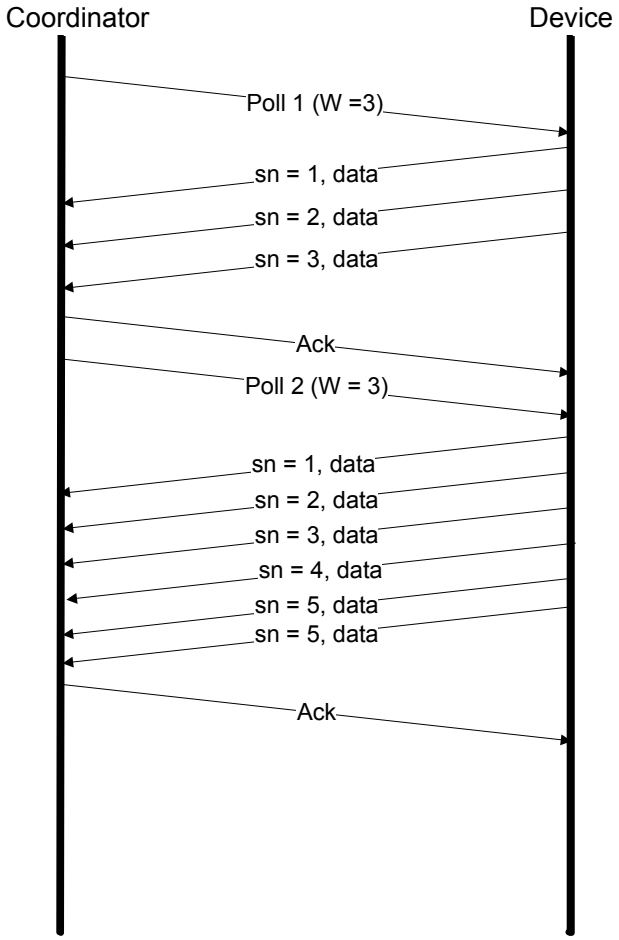


B. Detail error recovery mechanism for T_3 class of packets is described below.

T_3 device can transmit number of data packets present in the queue at the instant of Poll received. For “Block-ACK” policy, a window size (W) is determined by the coordinator. If the number of packets in the queue is more than the W, error recovery is handled in multiple phases.

After transmitting the Poll packet, the coordinator expects to receive W number of data packets in response and takes one of the following actions:

- If the coordinator does not receive all data packets from the device, it shall assume either device did not receive the poll packet or device received the poll packet and some data packets transmitted by the device are lost. To continue the operation, the coordinator shall retransmit the poll packet with a bitmap indicating the packets which are not received successfully.
- If the coordinator receives all data packet from a device, the coordinator shall transmit the ACK packet. On receiving the ACK packet device can go to sleep state.
- After transmitting the ACK packet, coordinator shall transmit the Poll packet for next device.
- If ACK transmitted from the coordinator is lost, device goes to sleep mode after receiving the Poll packet of next device or time out. Receiving Poll packet for next device is an indication that data is successful but ACK is lost.

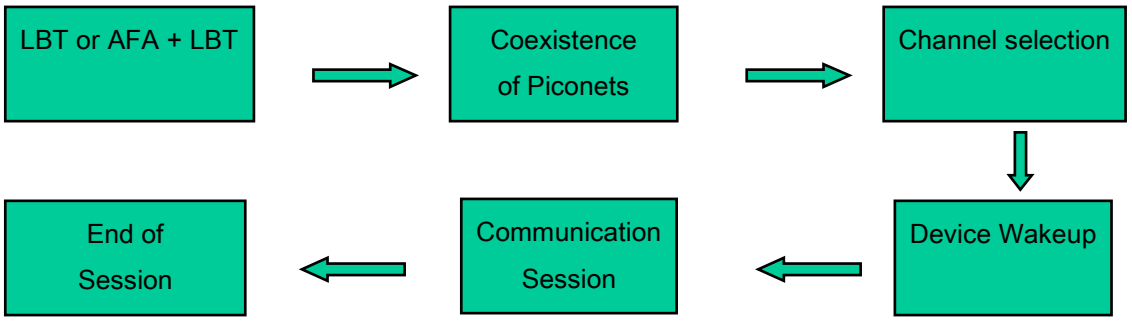


ACK and next Poll packet can be combined for further optimization, as T_3 applications do not necessarily operate in power saving mode.

6. Channel Access Mechanism for Implant Communication

- MICS (402-405 MHz), 10 channels: Suitable for Implant Communication
- MICS Rules:

A. Except in response to a medical implant event, no medical implant transmitter shall transmit except in response to a transmission from a **medical implant programmer/control transmitter** or a **non-radio frequency** actuation signal generated by an external device in which the medical implant transmitter is implanted.
B. Within **5 seconds** prior to initiating a communications session, Coordinator must monitor the channel or channels the MICS system devices intend to occupy for a **minimum of 10 milliseconds per channel**.

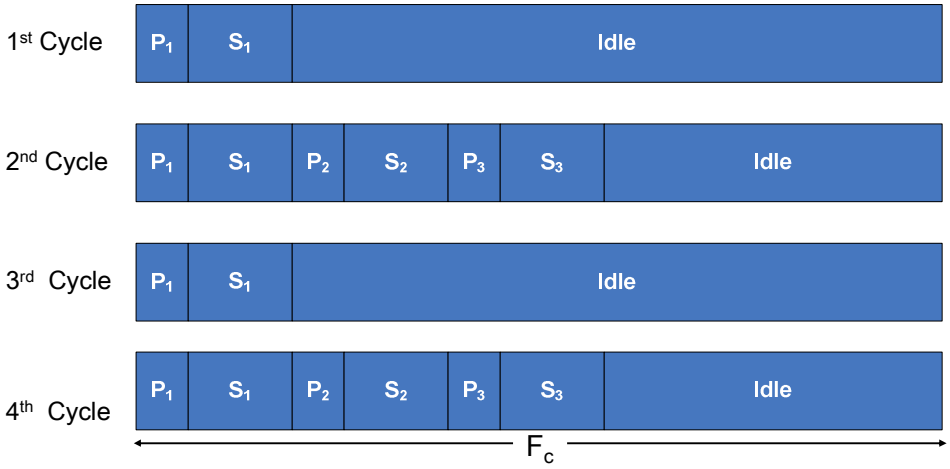


Objective: To design energy efficient channel access mechanism and meet the reliability and delay requirement of Implant applications.

Channel Access Mechanism

1. Data Aggregation
   - Shorter packets suffer from greater overhead leads to energy inefficiency
   - Allow data aggregation at implant device to form optimal size packet over multiple cycles without violating the delay requirement
   - Aggregation of data is optional
2. Variable Polling Rate
   - Implant Arrival rate range: Few bytes/sec – 10 Kbits/sec
   - The implant devices will be polled with different polling rate according to their arrival rates.
   - This avoids power consumption of low data rate devices due to excessive polling
3. Static poll schedule for devices
4. Carrier Sensing is not preferred at implant device
   - Asymmetric Clear Channel Assessment
   - Power consuming

Frame Design for Implant Communication

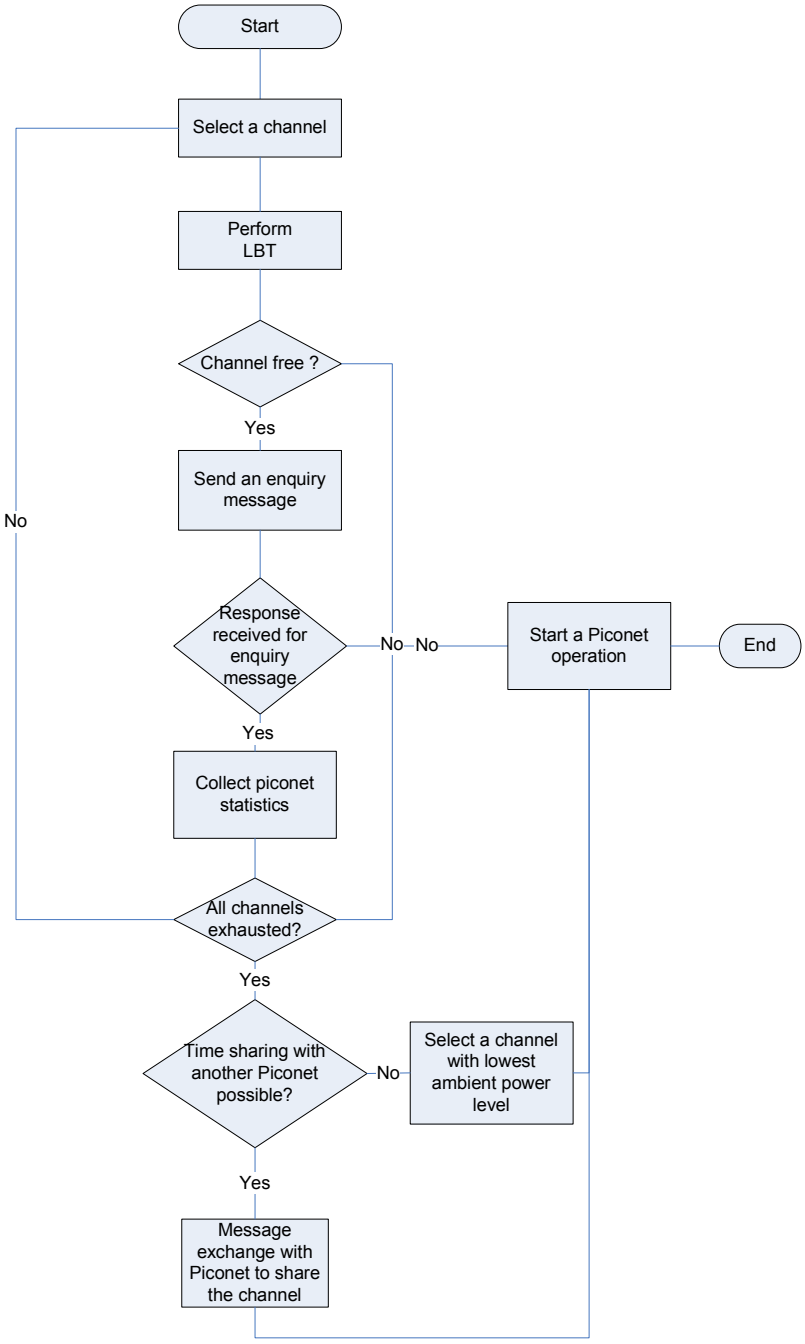


- Fixed F_c allows static poll schedule
- Periodicity of Poll for a device is determined according to the arrival rate
- High rate devices are polled first to maximize idle time
- Idle time can be utilized for integration of implant communication with on body

Example

- Device 1 is polled at F_c
- Device 2 and Device 3 are polled at 2 F_c

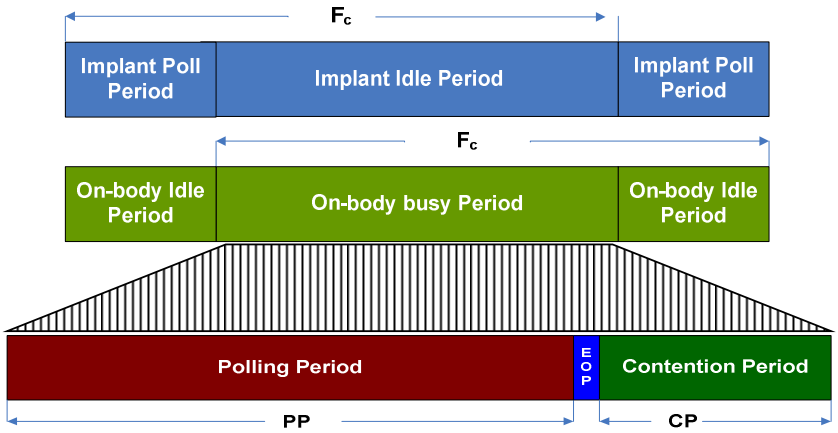
Coexistence in implant communication



- **To select a channel for network operation**
  - Longer LBT required to detect presence of secondary user (Energy inefficient)
  - Perform LBT for 10 ms and qualify access criteria
  - Send an enquiry message
  - Initiate network operation if no response
  - No free channel,
    - Time share with another Piconet, else
    - Select a channel with lowest ambient power level

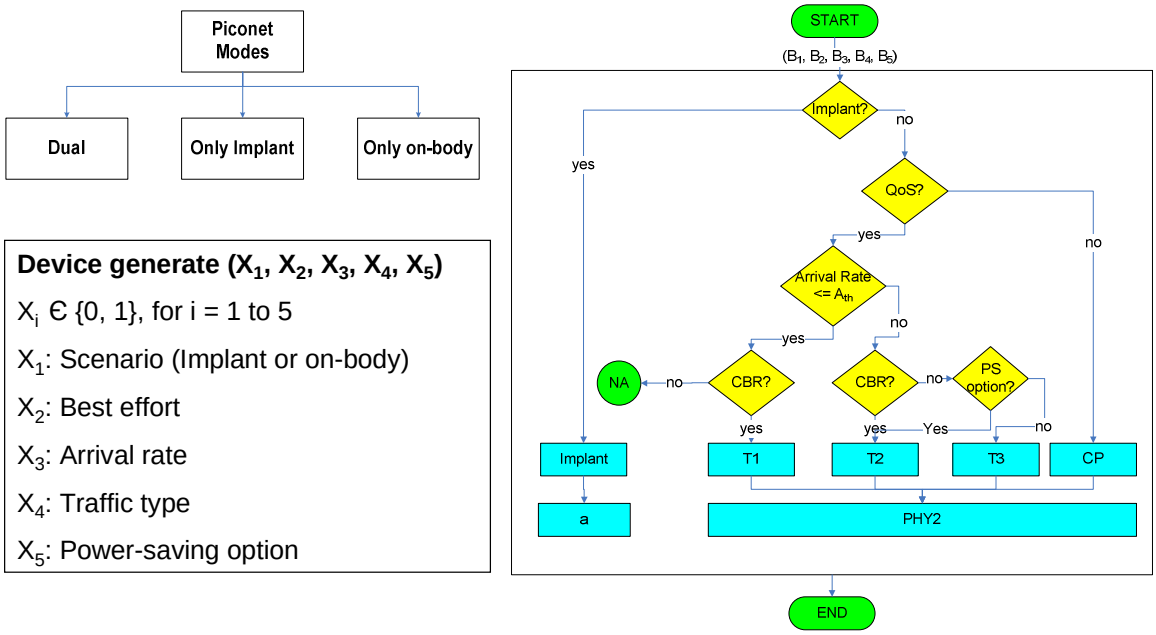
7. Single MAC design

Single MAC Solution



- On-body data communication allowed in Implant idle period only
  - No degradation in performance of implant communication
- On-body busy period is designed based on the minimum Implant idle period
- On-body busy period consist of on-body poling period and on-body contention period

Piconet modes and Device Classifier



8. On-body Coexistence

This section describes the mechanism for co-existence of 10 Piconets. In order to support multiple piconet co-existences in the same frequency band, we provide two different modes of operation. .

1. Shared Non-interference (NI) mode:

- Option 1: Time resource sharing
- Option 2: Offset piconet synchronization

The first mode is a **shared non-interference (NI) mode** where piconet controllers can talk to each other. In this mode, the piconet controllers co-ordinate and share the time resources either by negotiations for the time resource (option 1) or by using an offset piconet synchronization method (option 2). These options are discussed in more details later.

2. Coexistence interference mitigation (IM) mode

- Piconet controllers can not talk to each other
- Best effort piconet selection

The second mode is the co-existence interference mitigation (CM) mode, where either the piconet controllers are unable to talk to each other or do not want to talk to each other or they do not have sufficient resources to accommodate the other piconet. In this case, there is a possibility of

collisions and the logical channel selection for the piconets must be done to minimize the probability of collisions.

Channel description:

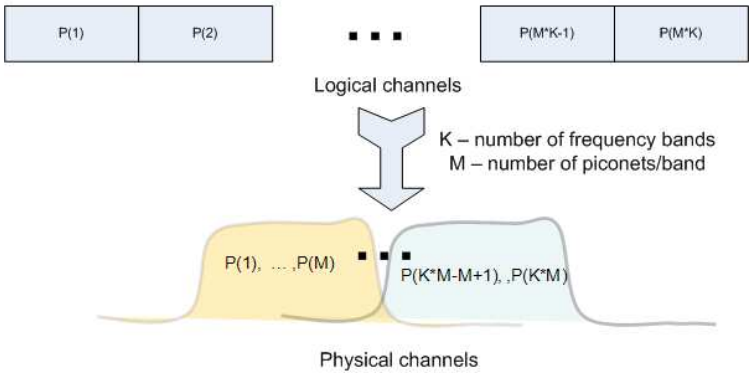


Figure : Logical to Physical Channel mapping

Figure shows a flowchart of a process to assign new logical channels for piconets while minimizing the impact on existing piconets. In this process, the device trying to establish a new piconet first selects a default frequency band (possibly the lowest frequency band available for minimum path loss). It then scans for all piconets numbers assigned to that frequency band. For example, if there are K frequency bands and M piconets per frequency band. It will scan for all M piconets assigned to that particular band sequentially. If no piconet is found to exist in that frequency band, the device can select any new logical channel id and begin operating a new piconet in that frequency band. If a piconet is found from the search, then the device starts looking at the next available frequency band and restarts the process. If there is an operational piconet in all available frequency bands, the piconet controller cannot start a new logical channel randomly and must choose a logical channel number based on its start in a shared NI mode or in the CM mode. It is assumed acceptable 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.

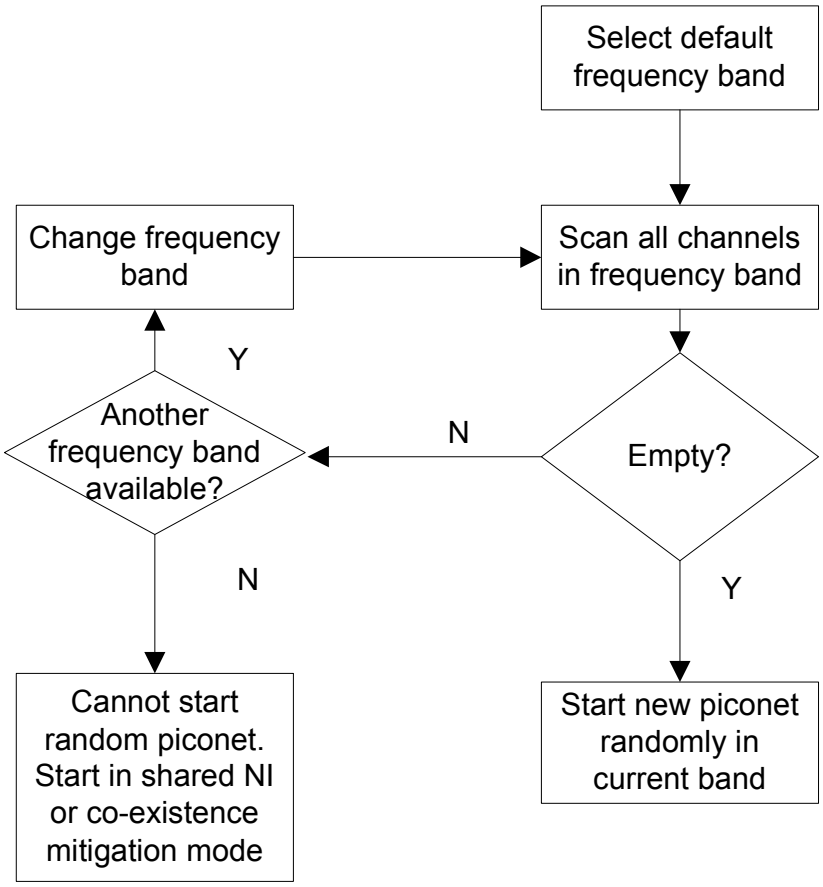


Figure : Piconet formation (Listen before talk)

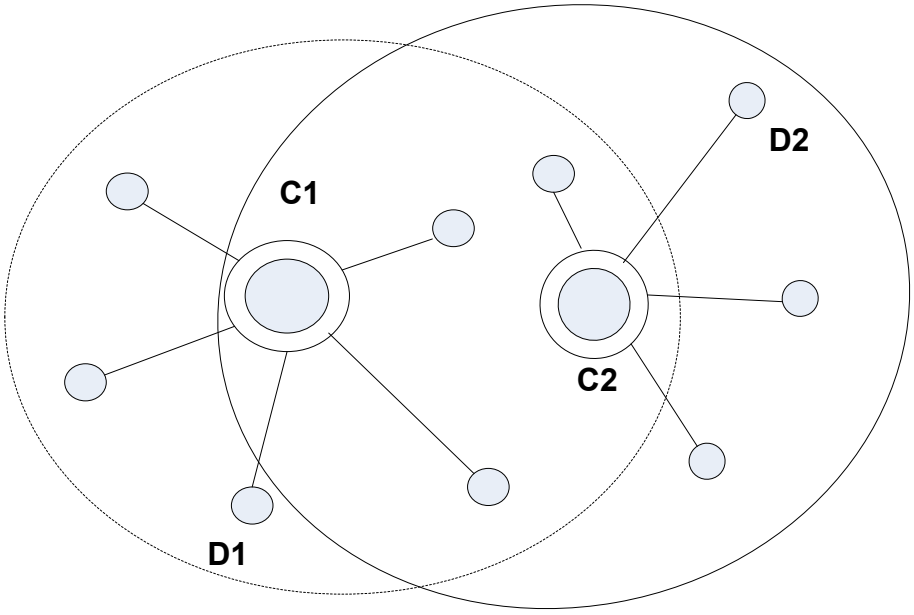


Figure : C1 - C2 can/will talk to each other

Figure shows two piconet controllers C1 and C2 who are within communication distance and can/will talk to each other. As explained above, this allows the NI mode of operation. Two options are possible for the NI mode of operation.

Option 1: NI mode Time resource sharing:
We propose a time resource sharing mode and communication method in order to support multiple piconets without interference. In this mode, the new piconet controller C2, on finding an existing controller C1, joins the C1 piconet as a device and communicates its requirements for bandwidth. Priority information is sent to allow priority for piconets. For example, medical devices may require higher priority than entertainment devices for body area networks. The standard could also mandate that existing piconets provide time resource sharing to higher priority devices. Medical devices may also have lower activity than entertainment applications and hence, may be more amenable to sharing resources. Once the request is received, the existing piconet controller adjusts its timing and informs its new timing schedule to piconets controller C2. C1 is now free to utilize the remaining resources for its applications. C1 also informs C2 of its knowledge of existing piconets to help it see other piconets that C2 can see but are not in range of C1. This helps to use this mechanism to synchronize across multiple piconets, even when all piconet controllers cannot see each other but are able to form a link to distribute information about each other. All requests and information sharing can be done using information elements (IEs) in the MAC protocol. Figure shows the sequence of operations between C1 and C2 in the time resource sharing NI mode.

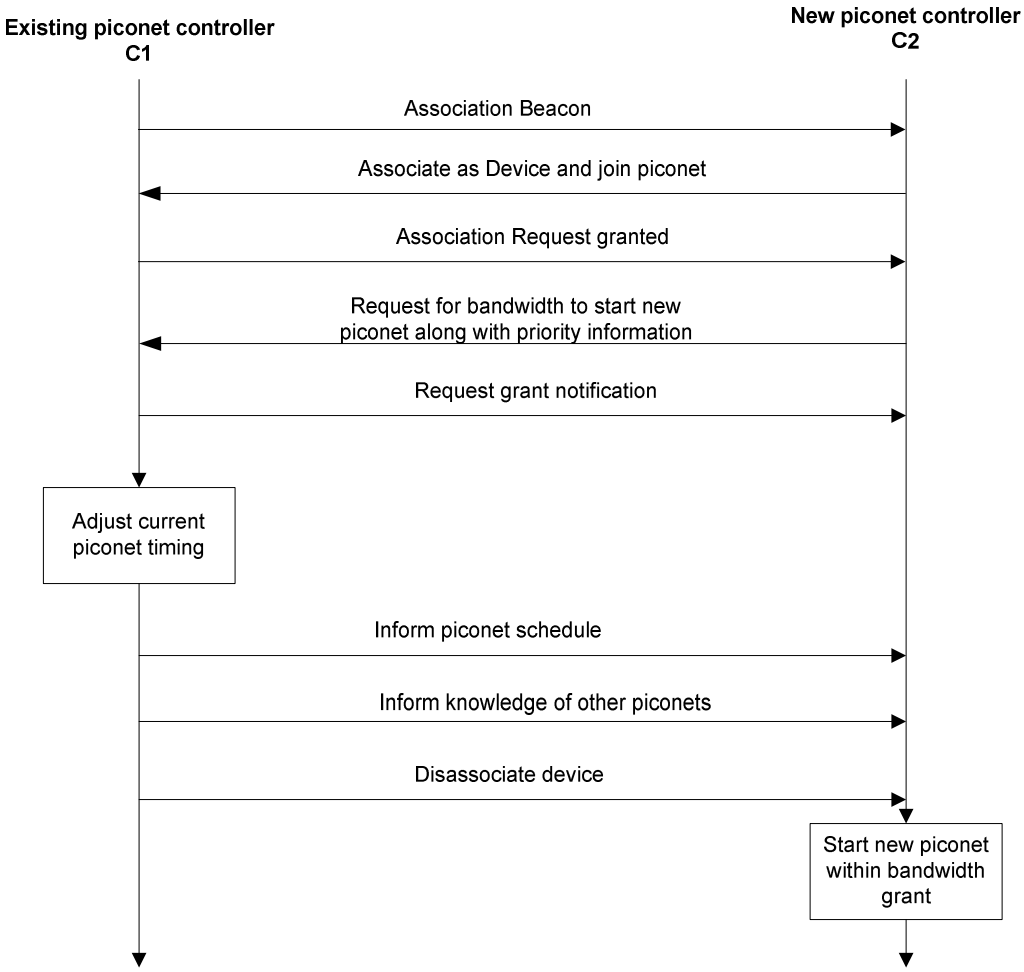


Figure : NI time resource sharing mode

Figure shows the piconet timing in the NI time resource sharing mode. As can be seen, C1 adjusts its piconet timing schedule to allow C2 to start its own piconet in the available time slots.

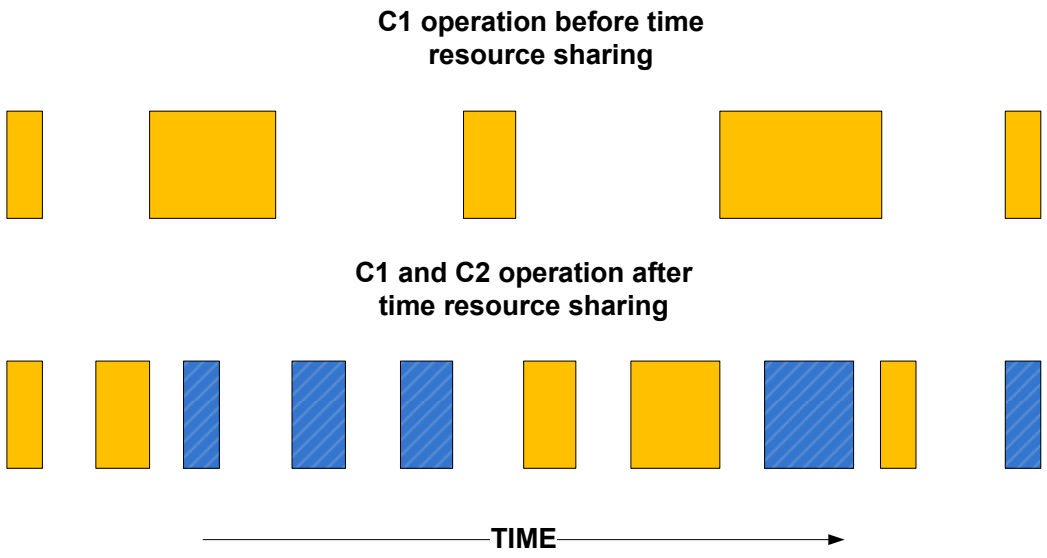


Figure: NI time resource sharing mode timing

Option 2: NI mode Offset Piconet Synchronization:

We propose an offset piconet synchronization solution and communication method to allow piconets to co-exist in a non-interference mode of operation. 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. The idea here is that body area networks could use a physical layer with a low duty cycle option using modulation such as on-off keying for low power consumption. This is as shown in Figure 1. This aspect could be exploited in order to provide co-existence as long as the duty cycle is kept to less than 50%. This mode can be used when time resource sharing mode is not possible due to limited time resources being available on C1's piconet or when C1 is having an equal or higher priority than C2 and refuses to allow releasing its time resource to other piconets but is willing to adjust its data rates or limit its duty cycle.

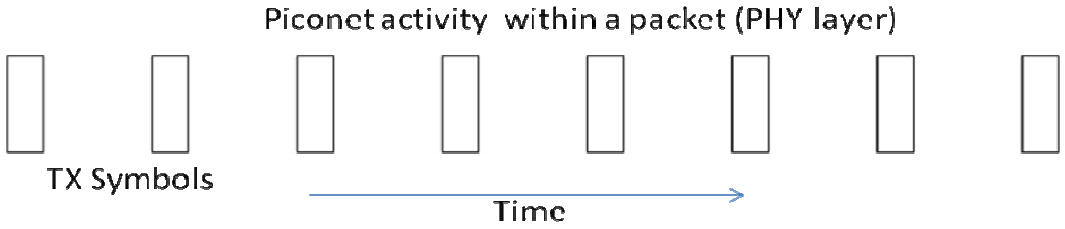


Figure 1: Tx activity within a packet in PHY mode with low duty cycle

The sequence of communication between C1 and C2 is shown in Figure 2. In this case, C1 informs C2 that it cannot release time resource to C2 but is willing to adjust its physical layer data rate/duty cycle to make sure all devices in its piconet have the same duty cycle during operation. The timing information must be exchanged between the two piconet controllers. C2 uses the beacon information of C1 to find the offset it needs to start a new piconet and the data rates or duty cycles it can use. While starting a new piconet in this manner, gaps should be allowed for clock drifting and multipath.

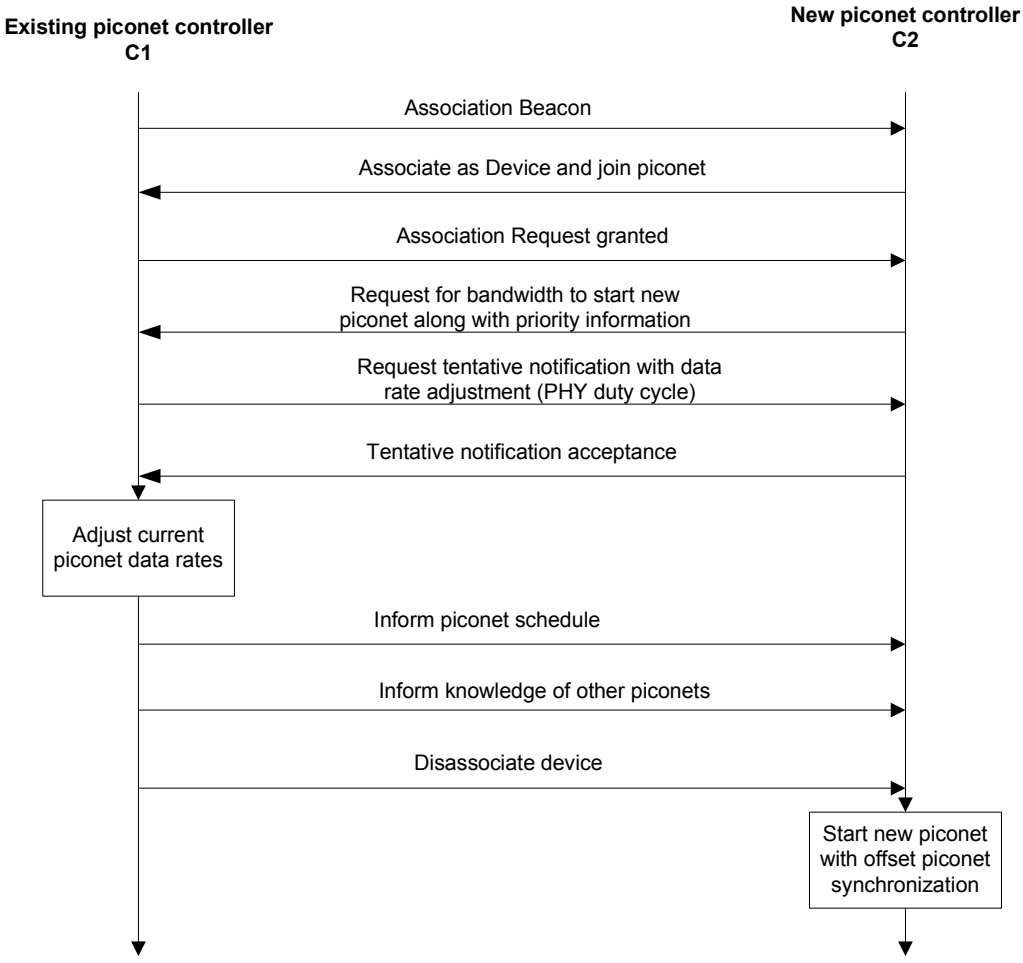


Figure 2: NI offset piconet synchronization

Figure 3 shows timing operation of C1 and C2 in the offset piconet synchronization mode. As can be seen, C2 tries to utilize free spaces in C1's schedule but allows for the possibility of overlaps in time between packets of C1 and C2. The interference management is actually handled on the PHY layer with offset piconet synchronization so that even though the packets may seem to collide in time at the MAC layer, in reality, the offset and low duty cycle ensure non-interference in practice. Ideally, the

new piconet should start with its center at the center of the existing off-time within the symbol in C1's duty cycle. This non-interference at the symbol level (within a frame) is shown in Figure 4.

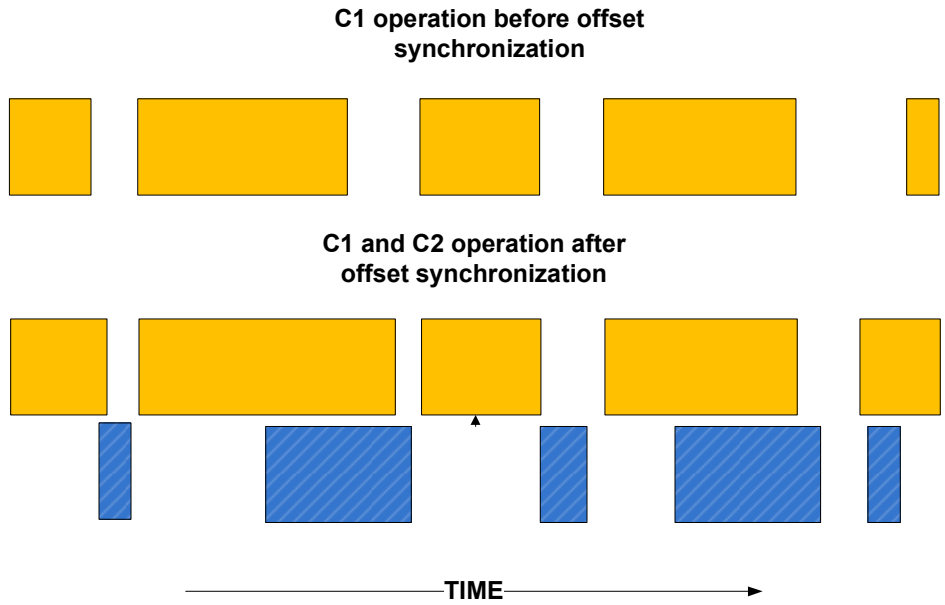


Figure 3: Offset piconet synchronization (frame level)

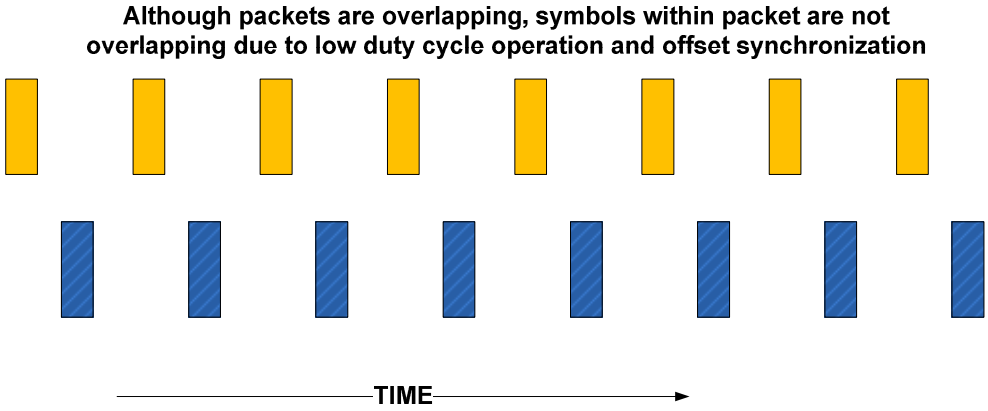


Figure 4: Offset piconet synchronization (symbol level)

We show the communication method when both the shared time resource mode and offset synchronization mode is not possible for multiple reasons such as denied time resource or denied association.

Figure 5 shows the communication pattern between C1 and C2 when both shared time resource mode and offset synchronization modes are not possible for communication. When existing piconet C1 has higher priority, the existing piconet may not be willing to make any adjustments to its schedule and/or willing to change its data rates/duty cycle 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 (if it sees sufficient time resources available) or start in CM mode, if there is not sufficient time resources. This mode is called the denied time resource mode of operation.

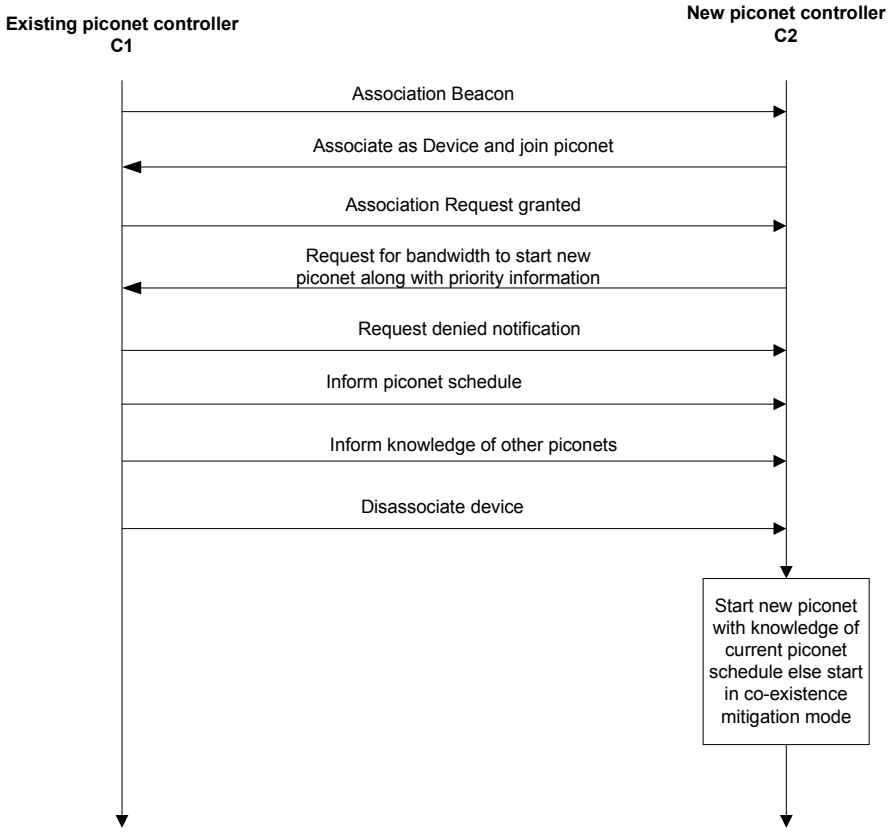


Figure 5: Denied Time resource mode

Figure 6 shows the sequence of communication between C1 and C2 when C1 refuses to communicate with C2. This could be due to multiple reasons. C1 may be doing some high priority service and may be unwilling to respond to C2 or may not have

sufficient time or resources to encourage new devices or piconet controllers to associate. In this case, C2 has no option but to start a new piconet in the co-existence mitigation (CM) mode.

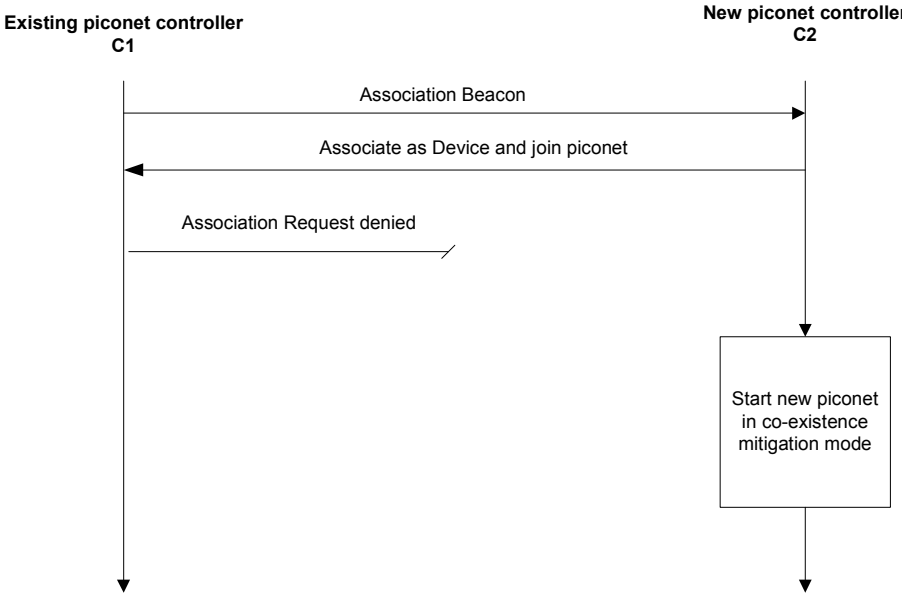


Figure 6: Denied Association mode

Co-existence mitigation (CM) mode:

We propose a co-existence mitigation scheme for unsynchronized piconets when piconets cannot or do not want to talk to each other. As mentioned earlier, it may be possible that piconet controllers may not be able to or want to talk to each other. In this case, piconets will have to start in an unsynchronized manner and hence, there is a possibility of collisions. While the PHY layer can be designed with good preamble codes and error correction codes to minimize the impact of collisions, the MAC can further help with logical channel selection to minimize interference. A logical channel number that is already in use by an existing piconet should not be used for the new piconet as there is no way for the PHY layer to distinguish packets for that piconet vs. an existing piconet. Figure 7 shows 5 unsynchronized piconets that are active. Hence at the receiver of a desired piconet, one may receive transmissions from other piconets as well and may have overlapping transmissions. However, some piconets may be closer than others and some piconets may have higher activity than others. Hence, it may be possible to make a better decision on which logical channel to use to start a new piconet.

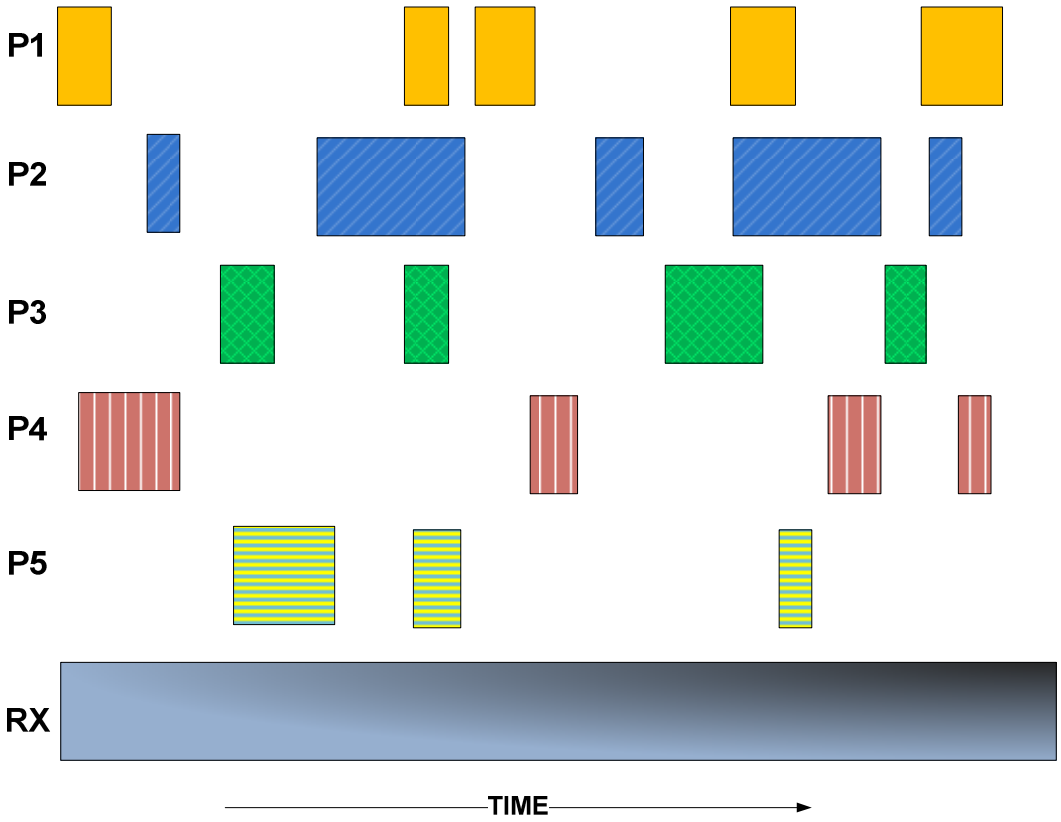


Figure 7 : Co-existence of 5 simultaneously operating piconets in CM mode

Hence, the logical assignment of a new piconet has to be managed intelligently to minimize the impact on existing piconets.

Figure 8 shows a flowchart of a process to assign new logical channels for piconets while minimizing the impact on existing piconets. The piconet controller first scans all logical channels in all frequency bands, Once a particular piconet is found to already exist, the device will gather relevant piconet information such as the number of devices on that piconet to obtain a traffic estimate and the received signal strength indication to figure out how far away the devices on that piconets are from the current device trying to form a new piconet. The current device may obtain this information either by listening to beacons and decoding this information or possibly joining that piconet if necessary in order to obtain this information. At the end of the search, the device trying to establish a new piconet will look at the collected information from the scan and make a decision about selecting a new logical channel and frequency band. If all logical channels are in use, the new device cannot establish a new piconet and will either have to join an existing piconet or wait and repeat this process until a new logical channel becomes available.

We propose the type of information that is needed to be exchanged in order to make decisions on new logical channel selection. For selecting a new logical channel based on the available information, the following aspects are used:

(a) **Number of devices in an existing piconet:** This data provides information on the probability of interference seen and the amount of bandwidth available in this piconet. If there are a significant number of devices in a piconet, it increases the probability of interference. Also, if no new piconet is available, it also provides information whether a device could merge into this piconet and still support its applications with other devices.

(b) **Received signal strength indicator:** By looking at this information for an existing piconet, a piconet controller trying to form a new piconet can estimate the distance to the devices of the existing piconet and the expected SINR at the receiver. This will provide information on the amount of interference seen and the data rates that will be able to be supported on the new piconets

(c) **Existing data rates used by devices:** 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 device.

(d) **Priority information about medical or QoS sensitive devices**: This information will help manage co-existence to give priority to piconets that support such devices.

We propose a notification scheme when a piconet controller decides to form a new piconet in the CM mode. Once the piconet controller decides to establish a new piconet, it can send the intention to start a new piconet in the CM mode to existing piconet controllers in the frequency band that it can talk to. This helps existing piconet controllers to be aware of the new piconet and allows piconets to make better decisions for co-existence. This communication between the new piconet controller and existing piconet controllers in the CM mode is shown in Figure 9.

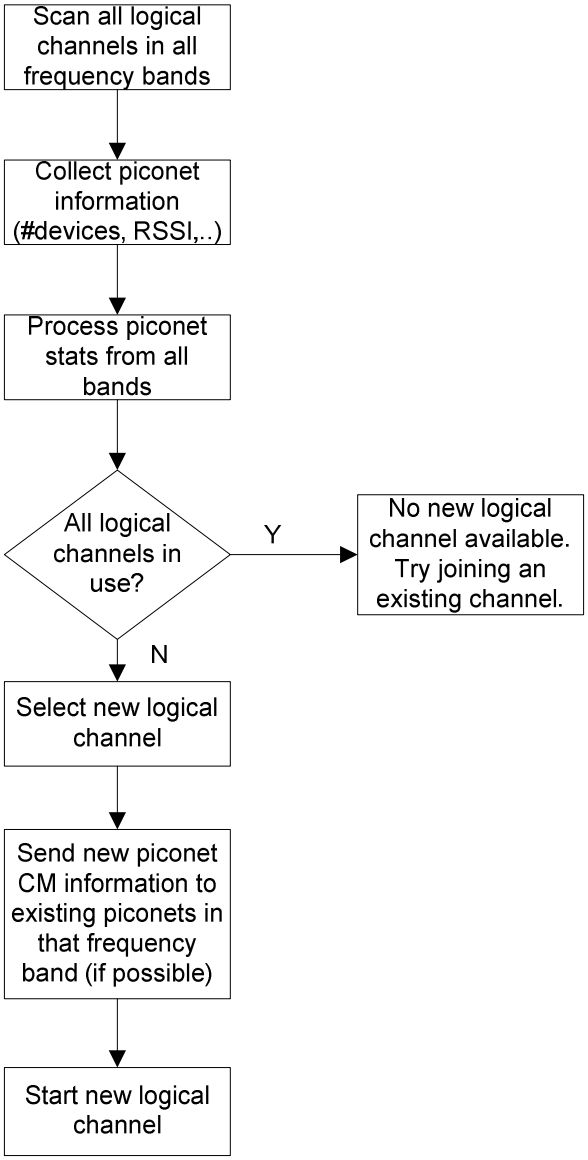


Figure 8 : Logical channel selection process for interference mitigation

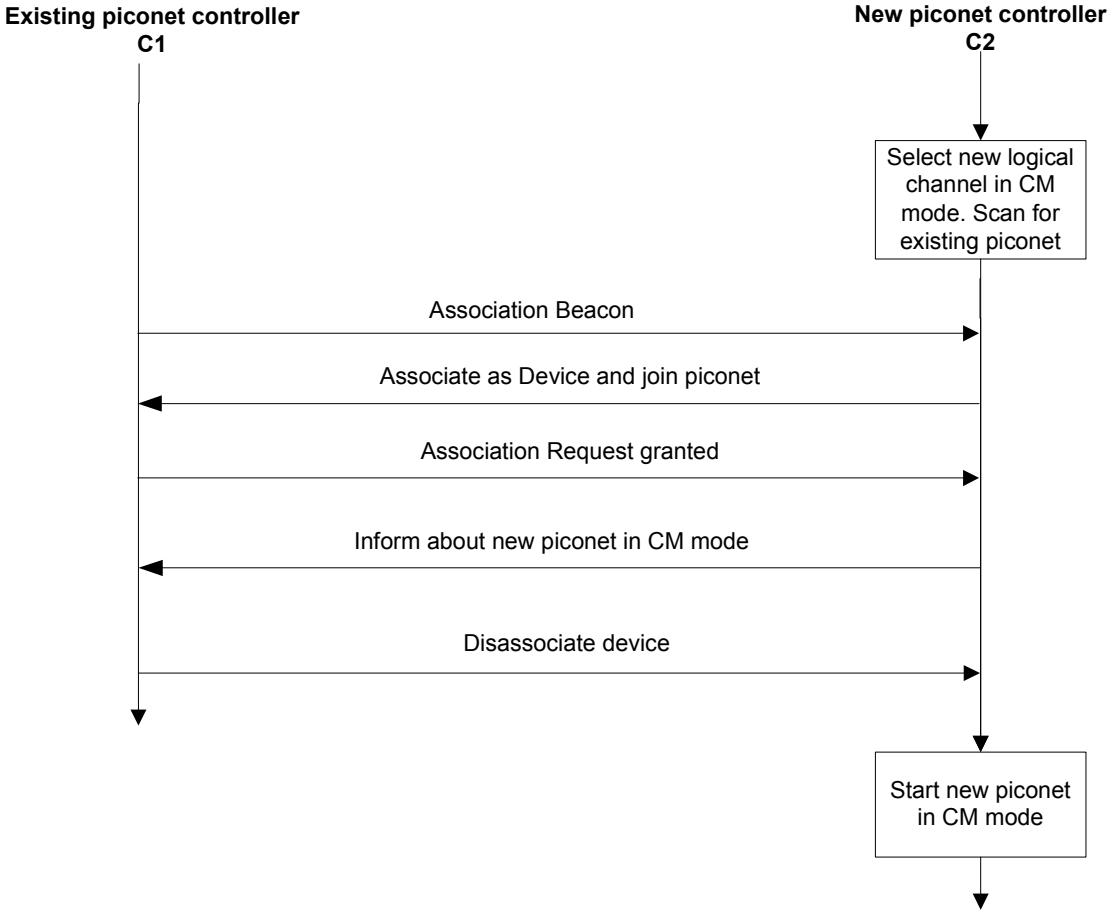


Figure 9 : Notification in CM mode

9. Network management

This document describes network setup procedures for IEEE 802.15.6 standard. Network setup part of body area network can be divided in to processes as listed in the below table.
As listed below, most of these processes for both implant applications and on-body applications, while few processes has slightly different procedure, and those are differentiated in their respective sections.

Process	**Implant applications**	**On-body applications**	**Comments**
Discovery	×	✓	NA
Channel Selection	✓	✓	Different
Wakeup	✓	×	NA
Emergency signaling by IMD	✓	×	NA
Association (Piconet Joining)	✓	✓	Different
Security	✓	✓	Same *(On-body group applications has additional process)*
Configuration Handshakes	✓	✓	Same/Different (*Depending upon channel access mechanisms*)
Disassociation	✓	✓	Same

Before starting a network set up for implant communication, IMD and coordinator would be in deep sleep and idle mode respectively.

Implant communication:

Implant in Deep Sleep State:

For IMDs wakeup mechanism, a coordinator will have one non-MICS band transmitter (say 2.4 GHz TX) and IMD will have the receiver for the same non-MICS band r (say 2.4 GHz RX).

Even when a IMD is in deep sleep mode, the non-MICS receiver will keep listening for wakeup signal from coordinator in a non-MICS channel which has least interference. The energy detector in the IMD non-MICS receiver can detect signals that are above a certain threshold. When a signal is received on the channel, sync detector module, at IMD non-MICS receiver, checks if it is a BAN wake up signal. If continuously 2 or 3 non-BAN signals are detected (say BT or WiFi signals), then the receiver will shift to listening on the next frequency that is with lesser interference And IMD non-MICS receiver will lock on less or no interference non-MICS channel.

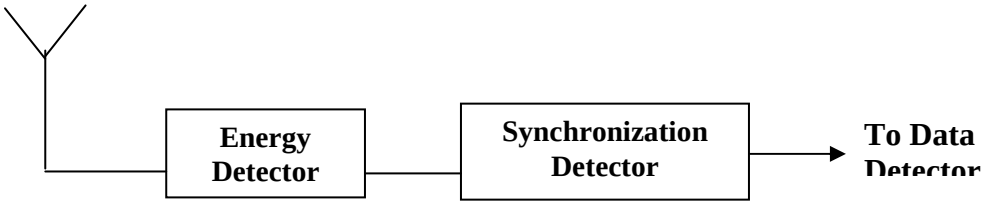


Figure 10: Receiver at IMD device

An example below shows where IMD locks on f_3 as it is found to be less interference channel. An IMD device, in order to conserve energy, periodically, listens for signals only for a fraction of time and shuts off its RF for certain duration of time. In Figure 2, the listen and off period together is shown as T duration.

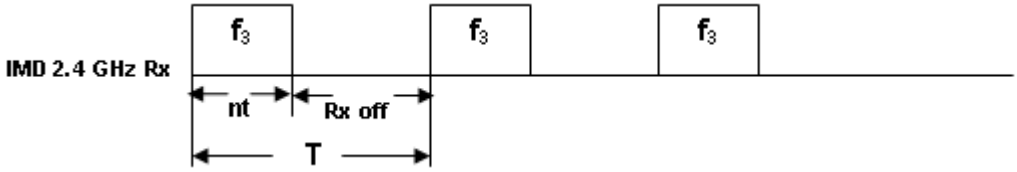


Figure 11: IMD non-MICS RX energy detector duty cycle

Where t is time for a single attempt of wake up process, and n is number of attempts of wake up process to increase reliability. T is periodicity of duty cycle.

Idle State of coordinator for MICS channel

During idle mode of coordinator, it is only energy detector of MICS RX which would be active and duty cycling as shown below.

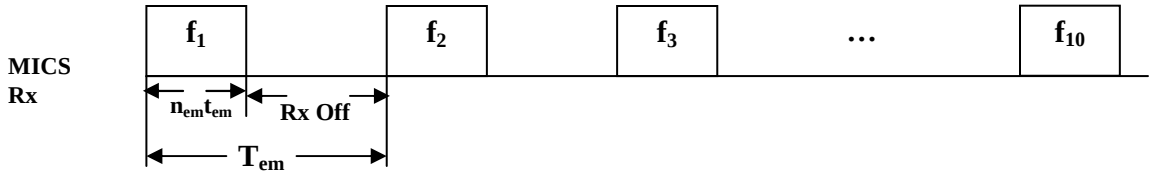


Figure 12: A coordinator MICS RX duty cycling for emergency signal in idle state

MICS Rx energy detector module would be ON for $\mathbf{n_{em}t_{em}}$ time (where $\mathbf{t_{em}}$ is time to receive one emergency signal and send its acknowledgement, and $\mathbf{n_{em}}$ is number of emergency signal that can be detected in ON cycle to increase reliability of emergency communication. The module would be switched off for the rest of time in a period of $\mathbf{T_{em}}$). After receiving energy, sync detector module will verify the emergency signal.

An emergency signal and normal signal can be differentiated using a different preamble or a frame bit. An emergency bit will require full radio to be active to verify an emergency signal.

Channel Acquisition for Implant Applications

- In order to acquire a channel, a device (coordinator generally or IMD in case of emergency only) has to sense a channel for p ms. If the channel is free, then start transmission on that channel, otherwise switch to another MICS channel assessment.
- Minimum value of p is defined as per MICS regulations and it requires sensing a free channel for minimum value to confirm its acquisition.

- If period of inactivity on the acquired channel equals to or exceeds p ms, then the acquired channel (as well as piconet session) would be lost and a device (a coordinator) has to follow MICS acquisition step again for further communications, if any.
- After MICS channel acquisition, if period of inactivity on the acquired channel equals or exceeds p ms, coordinator can hold the captured MICS channel by sending NULL packet periodically in p ms on the captured MICS channel.

Wake-up mechanism

Out of band (non-MICS band) wake up mechanism is proposed here. One of the non-MICS band, that can be used for wakeup mechanism is 2.4 GHz band (or 5.7 GHz as an other option). The non-MICS Band is divided in to N channels (N = 5 can suffice the requirements), with 1MHz bandwidth and equidistantly located inside the band.

Base station (coordinator) Transmitter side does a carrier sense for a fixed duration on a non-MICS channel and if interference is not detected at that channel, it will start sending wake up signal in that frequency. This process is repeated for all frequencies (f_1 to f_N) periodically as shown below.

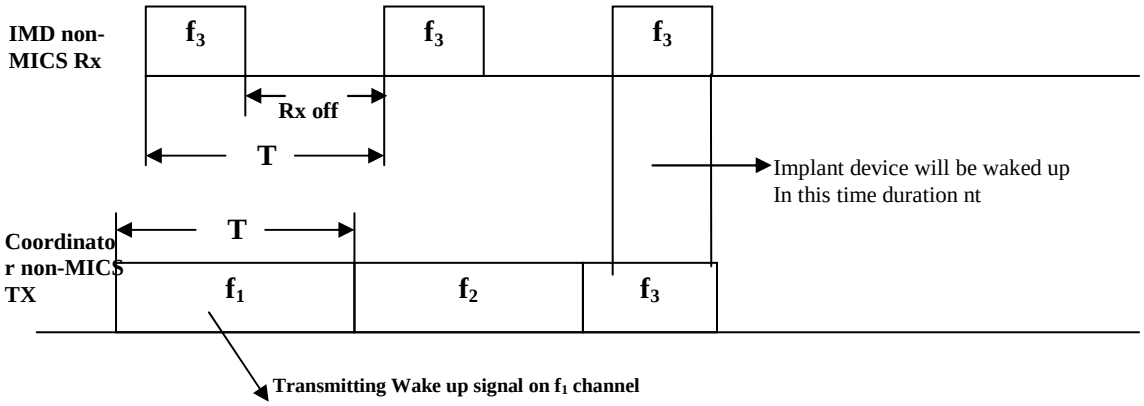


Figure 13: Wakeup mechanism for IMDs

Wakeup signal from coordinator will wake up implant device for further communication, as shown above.

Interference level setting for non-MICS channel selection

As described in previous sections, both coordinator and IMD avoid channels with higher interference. There is a possibility that a channel felt as less interference by IMD and it is locked to it, a coordinator discard the same channel as it is sensing interference on the channel. This would lead to failure of wake up process.

In order to avoid the above issue, different interference levels are chosen for IMD and coordinator such that a channel selected by IMD would not be discarded by coordinator due to interference.

The interference level for coordinator would be set at a level +55dbm lower than the IMD device. This will ensure that a particular channel selected by IMD device as less interference must be paged by coordinator with wakeup signal.

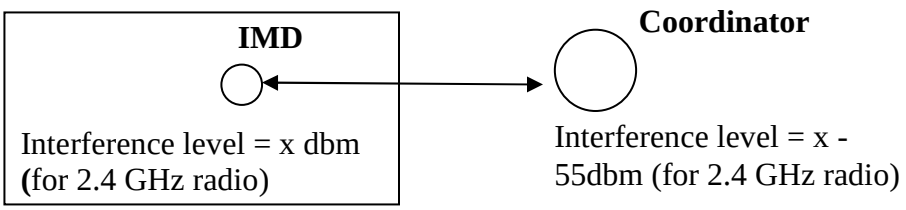


Figure 6: Different interference level for IMD and coordinator

Message sequence chart for wakeup mechanism

This section describes multiple methods of handshakes during wakeup procedure. Those methods are mainly divided in to two categories –

- Method 1: When polling is not must on MICS channel and any external radio or non-radio command is sufficient to allow IMD to transmit
- Method 2: When polling is required on MICS channel in order to allow a transmission from IMD

Wakeup Mechanism:

The diagrams below show handshakes and flow chart for wake up process for method 2.

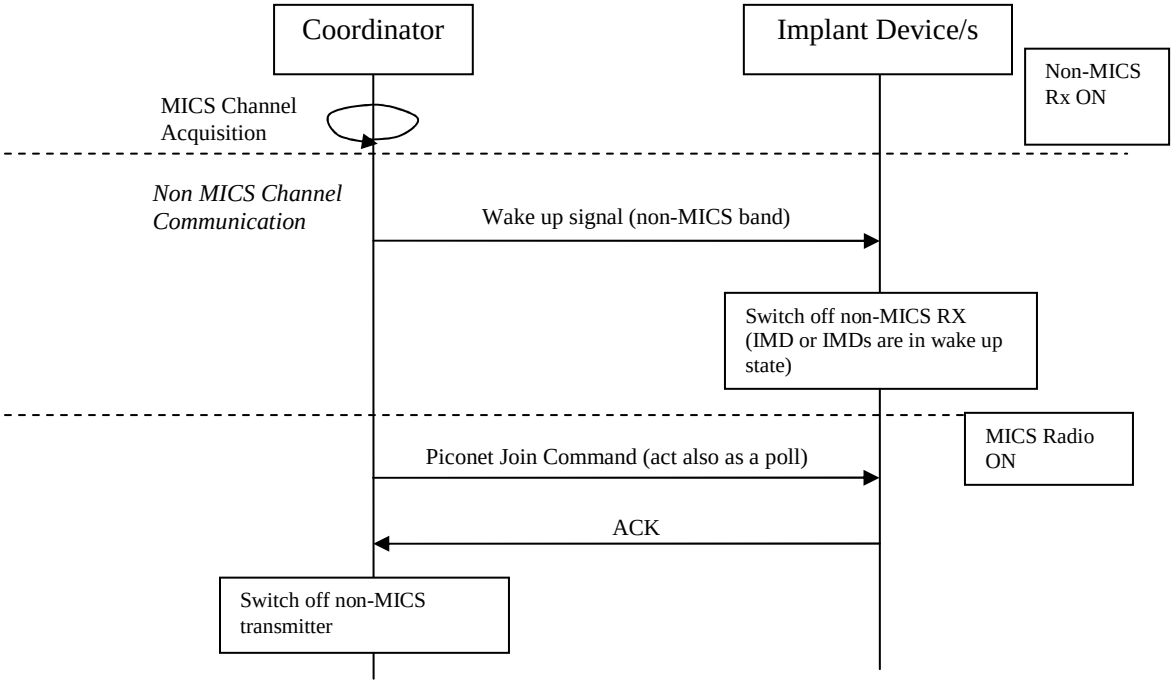


Figure 14: Wakeup process handshakes when polling is must on MICS channel

Waking up multiple IMDs:

For Waking up multiple IMDs, wakeup process can be done in two ways –

- Wakeup signal contains address of multiple IMDs and all the IMDs are woken up with single wakeup signal command.
- Wake up signal is sent to one IMD and then complete association with that IMD. After this send wakeup signal to another IMD and so on.

When multiple IMDs are waked up together, the IMDs will perform csma/ca on the MICS channel before sending ACK message.

Piconet join process for implant applications:

The diagram below shows message exchanges for piconet joining procedure.

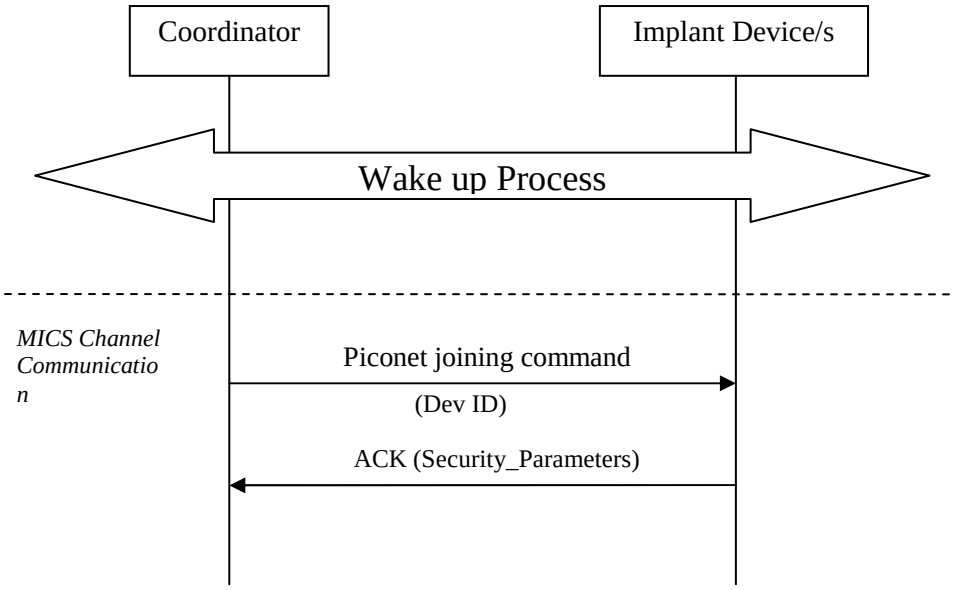


Figure 15:Piconet joining handshakes

Piconet joining command will carry a Device ID (1-2 bytes) for IMD device assigned by coordinator, along with source and destination address. All future communication with IMD device will happen with Device ID instead of 8 byte IMD device address. The Security_Parametes which include the security features that are required by the implant device is also exchanged during piconet join. The Security_Parameters is explained in the Security section.

Piconet joining command would be followed by ACK from IMD device, thereby completing piconet joining procedure.

On-Body Applications:

Channel acquisition for on-body applications:

- A coordinator detects energy on channels allocated for on-body communication, a process known as ED scan (energy detection scan).
- A coordinator selects least energy channel which is lesser than susceptible interference level.

- If a coordinator X when finds a new channel, it broadcasts a channel acquired message n times (to provide reliability of message).
- If there is no other coordinator which has occupied the same channel, then coordinator X does not receive any reply for the broadcast message.
- If there is another coordinator Y which has also selected the same channel prior to the coordinator X, the channel acquired message from coordinator X would be responded back by coordinator Y, stating that this channel is already occupied.

- After receiving the channel acquired message reply, coordinator X will leave the channel and search for another free channel.

The flow chart below depicts the above steps.

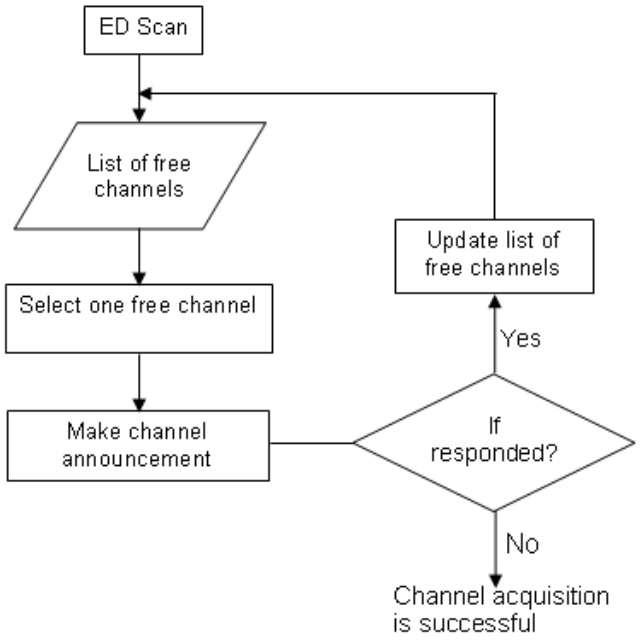


Figure 16: Channel acquisition flow chart

This is implementation specific that a coordinator scans all the channels at once and then selects a free channel or it select a free channel whichever it finds it first.

Piconet Phases:

After channel acquisition, piconet existence is divided into two phases:

1. Phase 1 - When no device which require poll is associated. In this phase, coordinator need not to indicate EOP (end of poll) or start of csma/ca period and its length, because in that case whole channel access mechanism is csma/ca only.
2. Phase 2 - When one or more device/s which require poll is/are associated. In this phase, it is required for coordinator to indicate start of csma/ca length (done by EOP message) and its length, so that devices which want to join or communicate with coordinator can know position of csma/ca period.

Discovery Process

An OBD when switched on starts discovering coordinator with their matching capabilities. There are two ways in which an OBD can discover an appropriate coordinator –

1. Passive scanning – scan for broadcast message (if any) from coordinator which contains its capabilities and ID.
2. Active scanning – An OBD sends capabilities information request in csma/ca period.

The section below examines discovery process in the two phases of a piconet:

Discovery process option for Phase 2

For active scanning in phase 2, it is must for an OBD to scan for EOP message to know where csma/ca period starts. After knowing csma/ca start, it will handshake with coordinator to know its capabilities.

To save on time and energy from active scanning, it is proposed to add coordinator's capabilities into EOP message itself. Then the process will become passive scanning.

Therefore, it is suggested to always do passive scanning in phase 2 of a piconet.

Discovery process option for Phase 1

In phase 1, the only channel access mechanism is csma/ca and there is poll/data mechanism. There in phase 1, it is possible to do both active and passive scanning by OBDs.

In phase 1, the channel access mechanism is carrier sense multiple access with collision avoidance (CSMA/CA), wherein periodic broadcast message (EOP or beacon) may or may not be present. Therefore in phase 1, it is possible to do both active and passive scanning by OBDs.

Based on passive and active scanning, a coordinator state in phase 1 is as follows:

- No Capability broadcast message mode (default)
- Capability broadcast message mode (configuration)

Broadcast message will contain following information:

- Capabilities of coordinator
- ID of coordinator (name identifier etc.)

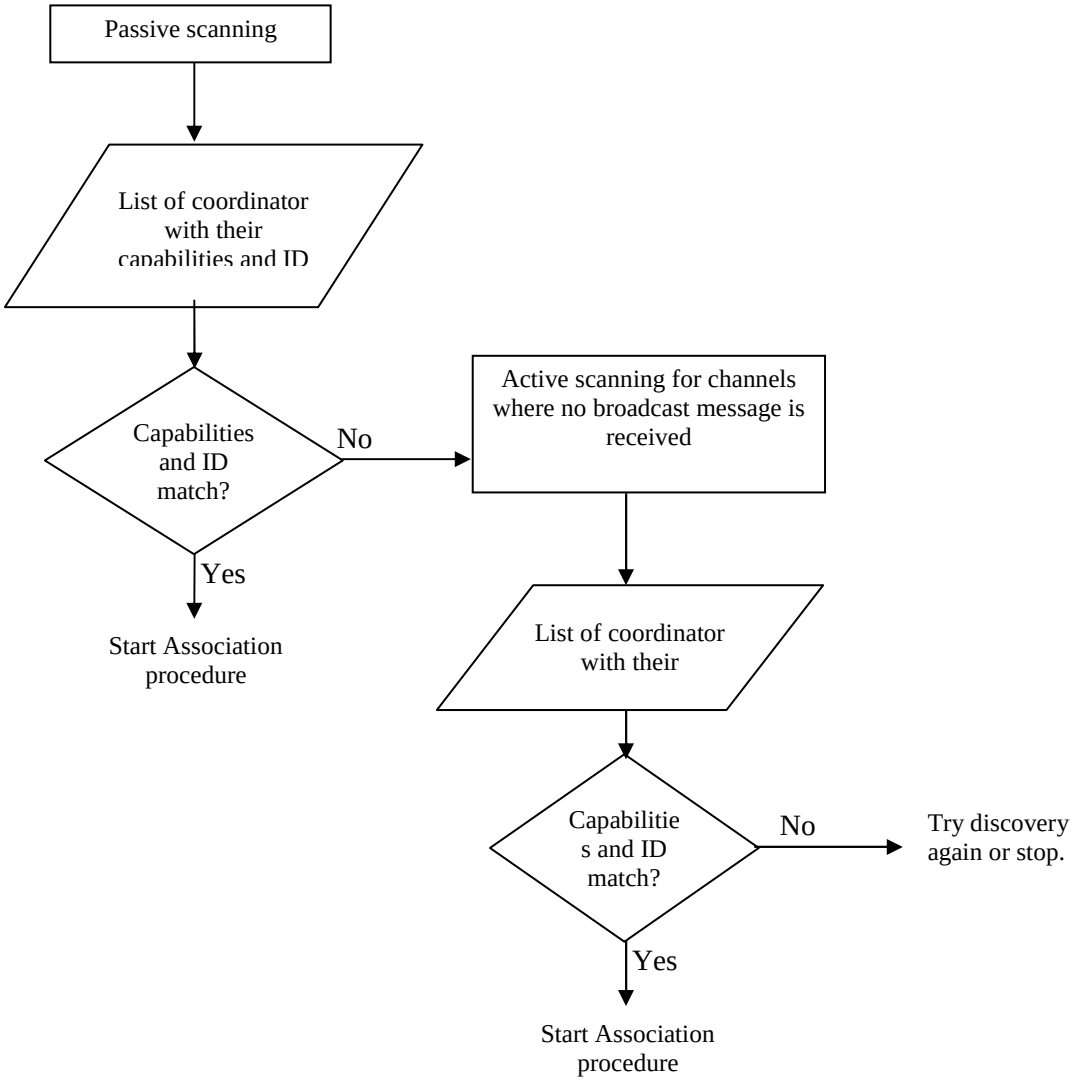
In passive scanning mode, a coordinator should broadcast its capabilities and ID at regular intervals. (The interval can be same as of F_c duration defined in channel access mechanism to maintain consistency of passive scanning in phase 2).

For active scanning, OBDs will perform csma/ca and send capabilities request command to coordinator. Then, coordinator responds back with its capabilities and ID.

Discovery steps followed by OBDs

Passive scanning - An OBD does not know whether coordinators are in phase 1 or phase 2. Without this knowledge, it can not start sending discovery request on each channel. OBD must do first passive scanning to listen for EOP to know about coordinators.

Active scanning – If an OBD does not find relevant coordinator during passive scan, then it will go for active scan on channels where no EOP is listened (coordinators are in phase 1). OBD will send capabilities request command to find out coordinator. A coordinator, if present, will respond with its capabilities and ID.



This is implementation specific that an OBD scans all the channels at once and then select appropriate coordinator or it matches coordinator capabilities as and when it finds one.

In addition, there are scenarios when multiple OBDs wants to join a piconet, so active scanning will lead to lot of traffic on network, resulting in energy loss and increase in association latency. Therefore it is suggested to configure coordinator to Capability broadcast message mode for such scenarios in phase 1.

Piconet join procedure

There is a slight difference between piconet joining process of implant and on-body applications, as shown in table below.

Differentiating Factors	**Implant Applications**	**On-body Applications**
Device responsible for initiating piconet joining	▪ Coordinator	▪ OBD (in general) ▪ Coordinator
Admission control	Since piconet joining is initiated from coordinator side, this handshake will always be	Since piconet joining is initiated from device side, coordinator may accept/reject

	successful (assuming no packet drop).	the request depending upon its admission control parameters, if any.
Group Association	×	✓

☞ Piconet joining is part of wakeup mechanism itself in method 2.

Piconet join process for on-body applications

Piconet joining process is as shown below in message sequence chart diagram.

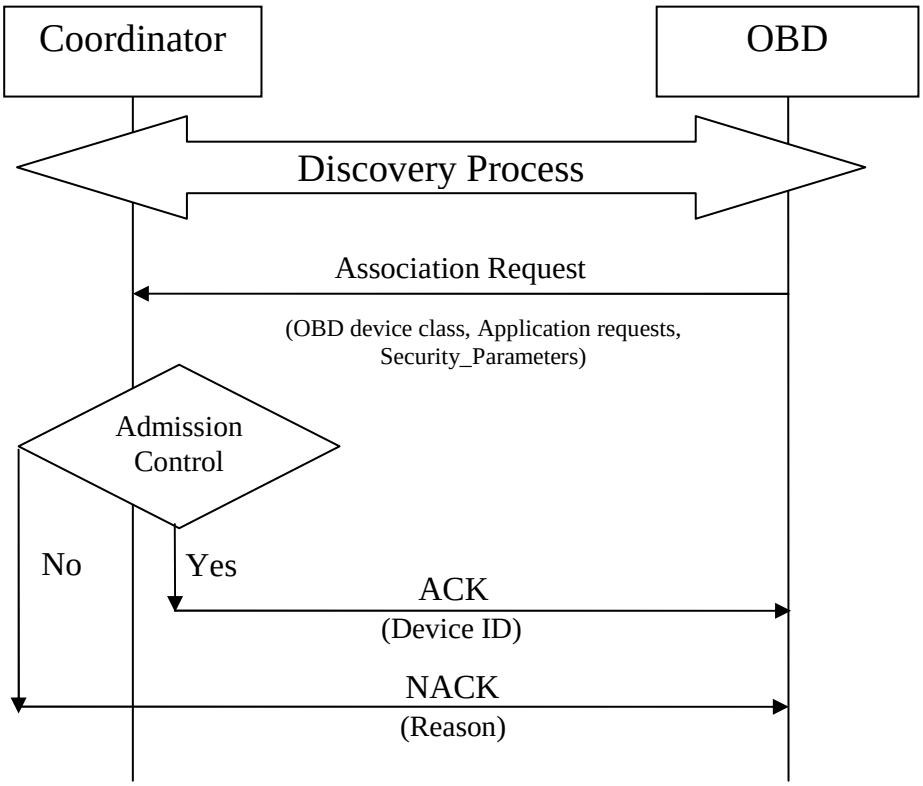


Figure 17: Message sequence for piconet join process

An OBD sends piconet joining request to discovered coordinator which contains following parameters along with source and destination address –

- OBD Device Class (video, physiological sensor etc)
- Application requirement (data rate, packet size etc)
- Security_Control_Field, Security_Alogrithm_Used values

A coordinator evaluates OBD piconet joining request based admission control module defined by channel access mechanism.

If admission control allows piconet joining for the OBD, coordinator sends Acknowledgment (ACK) in response to piconet join request. ACK response will contain Device ID for the piconet. For all further communications, Device ID would be used by OBD in place of 8 byte MAC

address.

If admission control does not allow piconet joining for the OBD, coordinator sends Negative acknowledgement (NACK), with the reason for not accepting piconet join request.

Piconet joining is also possible to be initiated from coordinator for OBD, in cases if a coordinator is preconfigured with OBD MAC address. Then a broadcast message or EOP can be utilized to initiate association from coordinator side.

Group Association:

There are applications in Body Area Network like EEG, ECG, EMG, and Gaming etc which comprises of multiple sensor nodes connected to a single coordinator.

In order to ensure that all independent device joins a single piconet and in a time and energy efficient manner, a group association mechanism is proposed, which is as follows:

1. A device is selected / marked as representative of all devices of a BAN group application.
2. All the devices of a group application, including coordinator, are numbered sequentially from 0 to N-1, where N being number of nodes in group application.
3. All the devices in group application should have their representative device private key information (it could be representative node's IEEE MAC address).
4. The representative device is responsible for network joining, that is, associating to a coordinator.

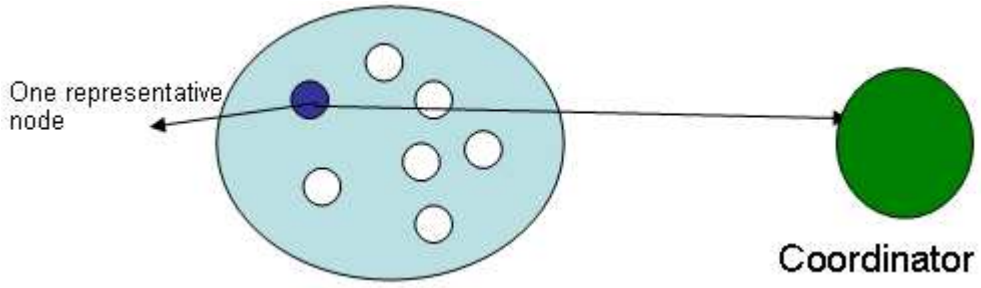


Figure 18: A group application is represented by one node for association and disassociation process

5. The representative device, while associating with the coordinator, requests for association for whole group in a single piconet joining command. The association command contain number of device, the representative device is representing to.
6. The coordinator device, in response, assigns a pool of device IDs with pool size equivalent to number of devices in group application.
7. In cases when coordinator does not have continuous pool of Device IDs, it will assign in sections, so it should provide that information in its response to representative device. For example, if for 50 devices, the pools are 4-40, 57-59, the coordinator should indicate 2 pools with each pool length.
8. A coordinator should start polling the group devices in its polling cycle as per its normal channel access mechanism.
9. The device ID pool along with their representative private key information would be added to EOP message.
10. All the device of a group application should keep on scanning for EOP message which contains their representative key information.
11. As soon as a device from group application finds EOP message with their representative

private key information in it, it will calculate its Device ID from this message by adding its sequential number to start device ID from device ID pool allocated by the coordinator.

12. As soon as a device from group application identifies their respective Device IDs, it should start listening for its poll message and enter to polling cycle.
13. A coordinator can remove the pool information along with representative information from its EOP message, when all the devices start responding to their respective poll commands.
14. In case, an erroneous device from group application, when does not start communication with coordinator for a defined period of time, then broadcast message should remove device ID pool and representative information. The respective device can also be freed.

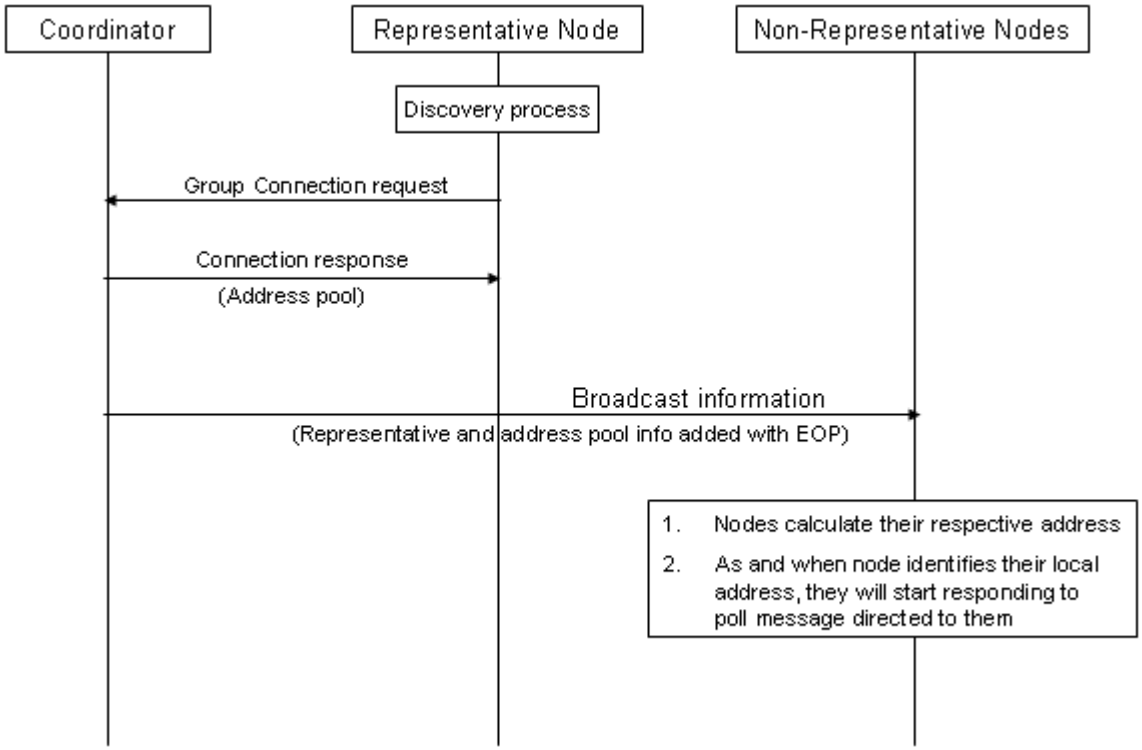


Figure 19: Message sequence for group association

Multiple representatives

There may be practical scenarios when representative node itself is erroneous. In those cases, whole application will not work just because of representative being erroneous. To avoid such situations, it is being proposed to have 2-3 representatives.

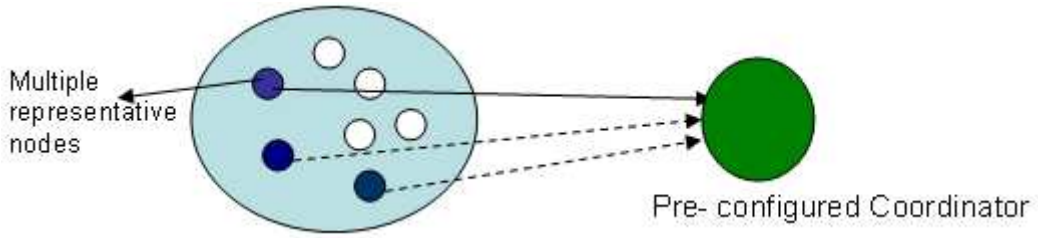


Figure 20: A group application is represented by multiple nodes for association and disassociation process

The procedure for group association with multiple representatives will differ as –

1. A coordinator is preconfigured for private key or keys depending if they have same private key or separate private key respectively.
2. All representatives of group application will try to associate with a coordinator.
3. The coordinator will reject association request from other representatives after one succeeds in association stating that one of their representative has succeeded in association, and providing them also their group device IDs pool, thereby saving their time of scanning.

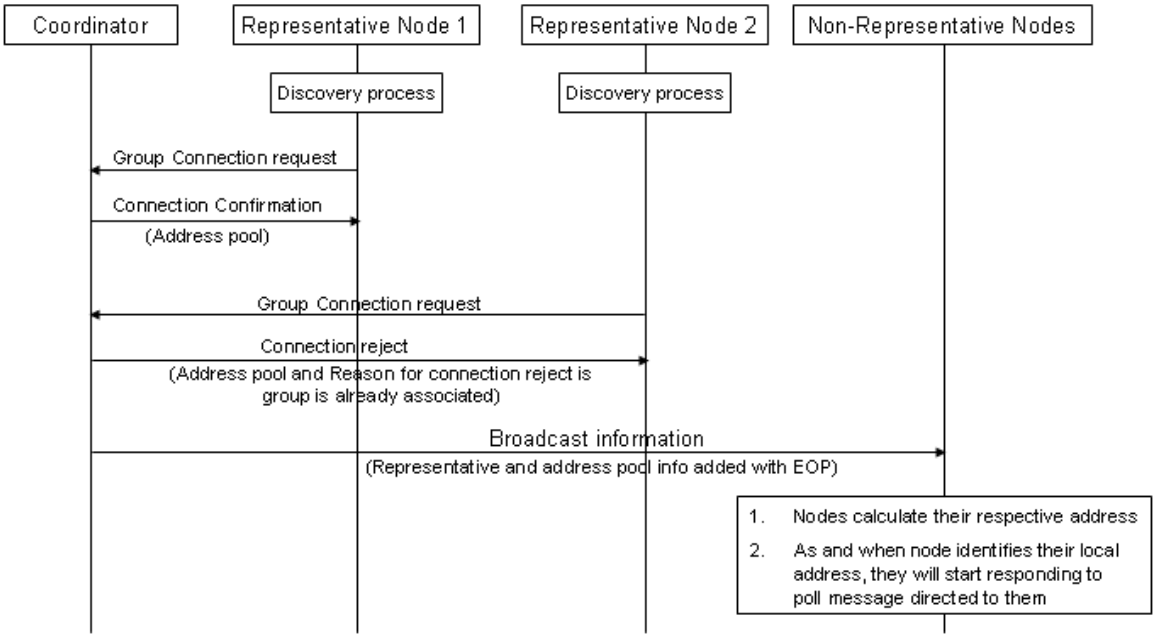


Figure 21: Message sequence for group association when there are multiple representative

10. Security in BAN

Security mechanisms are provided in the LLC and MAC for the following features: Authentication, Integrity, Confidentiality and Replay protection.

A BAN is made up of several types of devices each requiring different levels of security. An implant device that reports medical data to a coordinator may require highest level of authentication, integrity and privacy protection. The propose security method is a highly flexible method for choosing multiple levels of security protection. A single byte control data is sent for exchanging security levels that will be used by BAN device. The key sizes that are to be used for integrity and privacy protection for the data communication are also kept flexible for each session. Since the BAN communication is typically consisting of short sessions, the same security level is used for all the data and control exchange in a session.

Security level is represented using a one byte bitmap. Each bit is used to enable/disable the security features as -

I. Bit 0 – Authentication
II. Bit 1 – Integrity protection
III. Bit 2 – Encryption/Decryption
IV. Bit 3 – Replay protection using frame counters
V. Bit 4 – Use 64 bit keys
VI. Bit 5 – Use 128 bit keys
VII. Bit 5 – Use 256 bit
VIII. Bits 6-7 – RFU

When No security protection is to be used then all the bits in the Security_Control_Field are set to 0. The default key size used can be 128 bit keys. With 8 bits in the Security_Control_Field, several different levels of security are possible for BAN devices that can be chosen according to the application requirement.

Security_Algorithm_Used field is used to indicate the security algorithm that is used for the security mechanisms. It is defined a single byte field, that carries a hex value indicating the security algorithm that will be used by the security mechanism.

The following assumptions are made the coordinator and BAN device (client) for implementation of the security mechanism.

1. One security level per device, per session
2. No Frame level security – all frames exchanged during a session use the same security level
3. Currently, group or broadcast keys are not covered.
4. A device (client) should have the capability to store temporal keys and frame counters until the keys are renegotiated in a later session.
5. A coordinator would be preconfigured with following details
    - Max Security modes that a BAN devices can support.
    - Security Table
        - Shared keys for this client (multiple keys identified by identifier, called Master Key ID- MKID)
        - Maximum Security level supported at client
6. A BAN device would also be preconfigured with security keys and the corresponding MKID as in the coordinator.

Frame counter for replay protection. A two byte frame counter can be used. The value of the frame counter from a previous session needs to be save at the coordinator and client. The frame counter can be re-initialized when the security keys are again negotiated at a later session).

The algorithm used for the security mechanism is also mentioned as a parameter that is exchanged along with the Security_Control_Field. Default Algorithm used is - AES.

Authentication Procedure:

After a BAN device successfully joins the piconet, the coordinator initiates the authentication

procedure.. Authentication uses a 4-way handshake procedure which validate that the peer device shares the same master key.

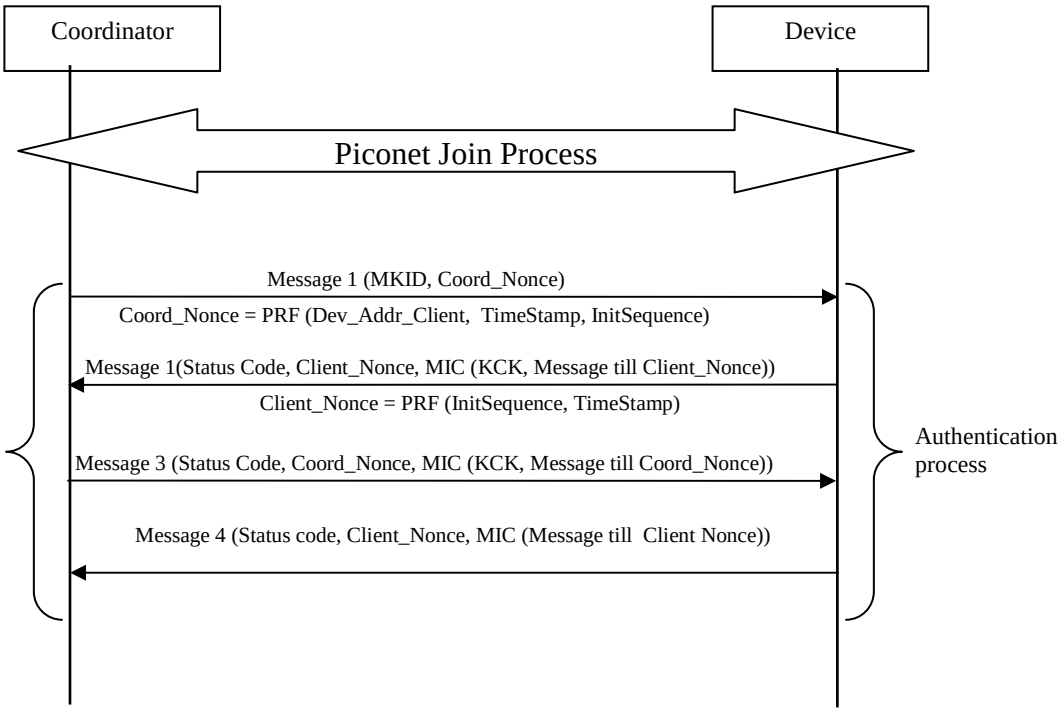


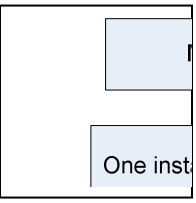
Figure 8: Message sequence for authentication process

A coordinator initiates the authentication security process and sends Message 1 as shown in above diagram. Message 1 includes the master key ID MKID and a random nonce called the Coord_Nonce that uses the device identifier of the client. The MKID is the shared secret that is used to authenticate both the client and coordinator.

On receiving Message 1, the device checks if it has the corresponding MKID. If not, it returns the Message 2 with status set to Failure. If MKID is available at the client, he client also derives a random nonce called Client_Nonce. Using MKID and the two nonces, Coord_Nonce and Client_Nonce, the device derives a new keys for this session Pairwise temporal Key (PTK), key check key (KCK)and sends Message 2. The coordinator similarly then derives a PTK, KCK and calculates the MIC (KCK, Message till Client_Nonce). The calculated value should be same as what is received in Message 2. Coordinator authenticates that client has the same key by sending message 3. The device then recalculates MIC (KCK, Message 3) and verifies that it is same as what is received from Coordinator. The Client authenticates that coordinator has the same key. In each of the messages 2, 3, 4 the coordinator and device return a status field that is used to indicate the success or failure of the authentication process.

After these security handshakes, both devices now have a temporal key which can be used for Integrity and Confidentiality protection for the subsequent communication.

- If Authentication is not required for the current session, then the temporal keys agreed during the previous session will be used.
- Freshness or replay protection is required so that the data received from an implant is not again replayed by say an on-body malicious device.



Privacy protection using Encryption/Decryption:

AES-128 counter mode can be used for data encryption. The PTK key agreed during authentication is the key used for encryption/decryption procedure.

Integrity protection using Message Integrity Check in the Data Frame:

AES-128 cipher block chaining-message authentication code (CBC-MAC) can be used for MIC calculation. The MIC will be included in the Data frames.

Security in BAN application consisting of Group of devices:

- All devices in the group share a common set of master keys and IDs. The master key is installed by out of band mechanism not covered in this protocol.
- After association, only the representative node does the authentication procedure.
- The coordinator and the representative node will broadcast the Master Key Id, Coord-Nonce and Client-nonce used for the key generation in the poll message, so that all the devices in the group can generate the same key.
- The first communication with any device from the coordinator will involve a challenge, response sequence to verify that the devices have the same keys and then data communication begins.

The above simple method does not require the coordinator to maintain individual keys for each member of the group communication.

The MAC protocol can use the privacy and integrity protection only in the frames that are sent from the BAN device. Standard frames like (poll or other control frames) sent from the coordinator need not be encrypted or integrity protected. Since, this will make brute force attack possible by way of have know plain text and encrypted text.

11. Conclusion

- The proposal minimizes power consumption at the expense of bandwidth utilization while meeting the delay and reliability requirements of the BAN applications
- No degradation in performance of implant communication in case of dual mode
- Single FSM for MAC leads to simple system implementation
- Most of the comparison criterions are covered