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	22nd September 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

TABLE OF FIGURES

1 Overview

1.1 General

Wireless body area networks (WBANs) are envisioned to convey information pertaining to medical and entertainment applications over relatively short distances. Most of the WBANs shall operate in a star topology. It is required to design protocols that allow small form factor, power-efficient, inexpensive solutions to be implemented for a wide range of BAN devices. This document defines media access related protocols and solutions for other features required in WBANs.

1.2 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 and related solutions 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.

1.3 Purpose

A complete MAC proposal addressing the functional requirements of implant and on-body communication has been developed. The purpose of this document is to provide detail explanation of proposed solutions, trigger merger discussion and merge with other members of IEEE 802.15 TG6.

2 References

The following documents developed by IEEE 802.15 TG6 are considered to provide the media access control protocol and related solution for wireless body area networks.

- 15-07-0575-09-0ban-ban-draft-par-doc
- 15-08-0407-06-0006-tg6-applications-summary
- 15-08-0033-06-0006-draft-of-channel-model-for-body-area-network
- 15-08-0644-09-0006-tg6-technical-requirements-document
- 15-08-0034-11-0006-ieee-802-15-6-regulation-subcommittee-report
- 15-08-0811-02-0006-tg6-call-proposals
- 15-08-0831-05-0006-tg6-proposal-comparison-criteria

3 Acronyms and abbreviations

ACK	Acknowledgement
AES	Advance Encryption Standard
PER	Packet Error Rate
CAMA/CA	Carrier Sense Multiple Access with collision avoidance
GTK	Group Temporal Key
LLC	Logical Link Control
MSDU	MAC Service Data Unit. Information delivered as a unit between medium access control service access points.
PMK	Pairwise Master Key
PHY	Physical Layer
PTK	Pairwise Temporal Key
Superframe	A periodic time interval used in MAC layer to coordinate packet transmission in the between device
SD	Superframe Duration.
PP	Poll Period.
EPP	Extended Poll Period.
CAP	Contention Access Period
IP	Inactive Period
EoP	End of Poll. A special frame marker sent by the coordinator after completion of PP to advertise the duration of EPP, CAP and IP.
MPDU	MAC Protocol Data Unit. Messages exchanged between MAC entities.
MAC	Media Access Control. The Media Access Control Layer is one of two sublayers that make up the Data Link Layer of the OSI model. The MAC layer is responsible for moving data frames to and from across a shared channel.
FCS	Frame Check Sequence
QoS	Quality of Service

CBR	Constant Bit Rate
VBR	Variable Bit Rate
ARQ	Automatic Repeat Request
LBT	Listen Before Talk

4 General 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.

4.1 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. The 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 1, 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.

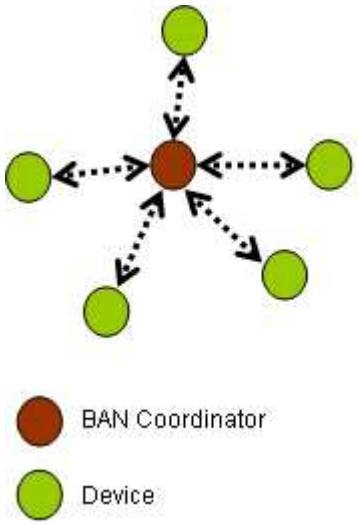


Figure 1 – BAN star topology

4.2 Architecture

Figure 2 illustrates the Architecture for WBAN device. 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.

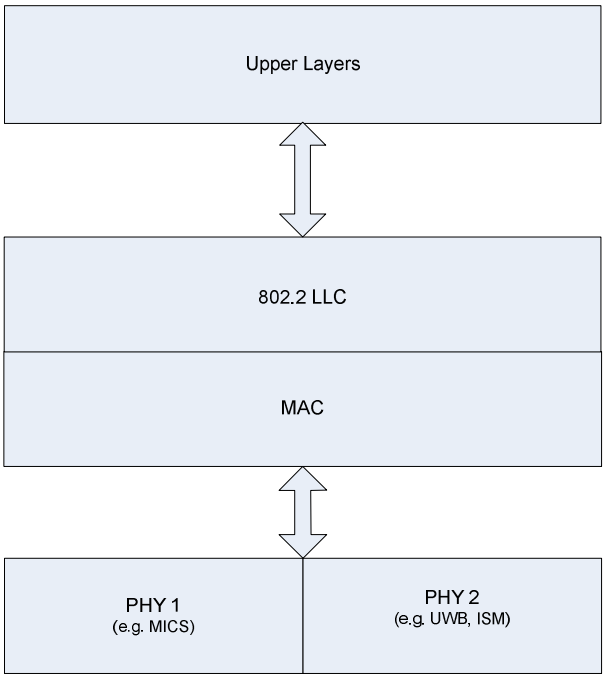


Figure 2 – Device architecture

5 MAC Frame Formats

This section details the format of MAC frames, MAC Protocol Data Unit (MPDU). The frames in the MAC sublayer are described as a sequence of fields in a specific order. All frame formats in this section are depicted in the order in which they are transmitted by the PHY, from left to right, where the leftmost bit is transmitted first in time. All the frames are divided into two level of hierarchy: frame type and sub type. A frame could be of any one of the following type.

- Data frame : used for data transmission and forwarded to the upper layer
- Control frame: used to control access to the medium
- Management frame: The frames which carry the management specific information but not forwarded to the upper layer

Each of this type is subdivided into different subtype, according to their specific function. The Table 1 enlists some of the frames with their type and subtype value.

Table 1- MAC frame type and subtypes

Type Value	Type Description	Subtype Value	Subtype Description
00	Data	-----	-----

01	Control	0000	POLL
01	Control	0001	BITMAP_POLL
01	Control	0010	ACK
01	Control	0011	B_ACK
01	Control	0100	WAKEUP
01	Control	0101	ALARM
01	Control	0110	LOCK
01	Control	0111-1111	Reserved
10	Management	0000	Association request
10	Management	0001	Association response
10	Management	0010	Re-association request
10	Management	0011	Re-association response
10	Management	0100	Disassociation
10	Management	0101	Network enquiry message
10	Management	0110 - 1111	TBD

5.1 Generic MAC frame format

The generic MAC frame format is composed of a Mac Header, a MAC payload, and FCS. Any general frame is formatted as shown in Figure 3

Figure 3 – Generic MAC frame format

5.1.1 MAC Header

This field contains frame control, Sequence number, Addressing field and optional security header.

5.1.1.1 Frame control field

The Frame Control field is 2 octets in length and contains information defining the frame type, addressing fields, and other control flags. The detailed specification of frame control field with their sub fields are yet to be finalized.

5.1.1.2 Sequence Number Field

The Sequence Number field is 1 octet in length and specifies the sequence identifier for the frame.

5.1.1.3 Addressing Fields

The addressing fields consist of information about source and destination related addresses and network id fields. The exact sub fields have not been finalized yet.

5.1.1.4 Security header

The security header shall contain the security specific subfields required to have a secured data transmission. This field is optional, and may not be present if the packet is not secured. MAC Payload

It is a variable length field that contains information specific to individual frame type and subtypes. Some of the frame may not contain a payload

5.1.2 FCS

This field contains 16 bit CRC for error detection.

5.2 Format of individual frame types

5.2.1 Data frame format

<table>
<tr><td>Octets: 2</td><td>1</td><td>2-4</td><td>Variable</td><td>Variable (0-Maximum data transfer unit)</td><td>2</td></tr>
<tr><td rowspan="2">Frame Control</td><td rowspan="2">Sequence Number</td><td rowspan="2">Addressing fields</td><td rowspan="2">Security header</td><td>Frame body</td><td rowspan="2">FCS</td></tr>
<tr><td>Data Payload</td></tr>
</table>

Figure 4 – Data frame format

Octets: 2	1	2-4	Variable (0 Maximum data transfer unit)							2
Frame Control	Sequence Number	Addressing fields	Frame body							FCS
			Length 1	Security Header 1	Data Payload 1	Length 2	Security Header 2	Data Payload 2	…..	

Figure 5 - Aggregated Data frame format

5.2.2 Control Frame format

The general frame format applicable for any control frame is shown in Figure 6. The subtype field in the MAC payload specifies the particular control frame then the rest of the bytes in MAC payload are decoded based on the control frame subtype. The tentative frame format of some of control frames is shown in the following subsections.

Octets: 2	1	2-4	Variable	2		2
Frame Control	Sequence Number	Addressing fields	Security header	Frame body		FCS
				frame subtype	frame subtype specific payload	

Figure 6 – Control frame format

5.2.2.1 POLL

Octets: 2	1	2-4	Variable	Bits : 4	1	1	1	5	variable	2
Frame Control	Sequence Number	Addressing fields	Security header	Frame body						FCS
				frame subtype	on time	sleep	data	window size	Data payload (if data bit is set)	

Figure 7 – POLL frame format

5.2.2.2 ACK

Octets: 2	1	2-4	Variable	Bits : 4	2
Frame Control	Sequence Number	Addressing fields	Security header	Frame body	FCS
				frame subtype	

Figure 8 – ACK frame format

5.2.2.3 EoP

Octets: 2	1	2-4	Variable					2
Frame Control	Sequence Number	Addressing fields	Security header	Frame body				FCS
				Control frame Identifier	Frame Specification	Piconet Specification	Co-existence	

Figure 9 – EoP frame format

5.2.2.4 WAKEUP

Octets: 2	1	2-4	Variable						2
Frame Control	Sequence Number	Addressing fields	Security header	Frame body					FCS
				Control frame Identifier	Wakeup type	Session duration	Channel info	End of Wakeup	

Figure 10 – WAKEUP frame format

5.2.2.5 LOCK

Octets: 2	1	2-4	Variable						2
Frame Control	Sequence Number	Addressing fields	Security header	Frame body					FCS
				Control frame Identifier	Session duration	Channel Info	No. of devices	Identification of devices	

Figure 11 – LOCK frame format

5.2.2.6 ALARM

Octets: 2	1	2-4	Variable					2
Frame Control	Sequence Number	Addressing fields	Security header	Frame body				FCS
				Control frame Identifier	Emergency type	Emergency Subtype	Emergency duration	

Figure 12 – ALARM frame format

5.2.3 MAC management frames

TBD

6 MAC sublayer specification

6.1 Functional description

6.1.1 Data transfer model

Two types of data transfer transactions are supported. The first one is, data transfer to a coordinator (uplink transmission) in which a device transmits the data to the coordinator and the second one, is data transfer from a coordinator (downlink transmission) in which the device receives the data from coordinator. Each data transmission is subdivided into two subcategories: single data transfer and block data transfer.

6.1.1.1 Data transfer to a coordinator (Uplink Transmission)

6.1.1.1.1 Single data transfer

In the poll based access, when a device wishes to transfer a single data to a coordinator or coordinator has to collect a pending data from the device, the device first listens to the POLL message and transmits the data to the coordinator. The coordinator may acknowledge the successful reception of the data by transmitting an optional NULL_POLL or acknowledgment frame. The sequence of operations is summarized in Figure 13.

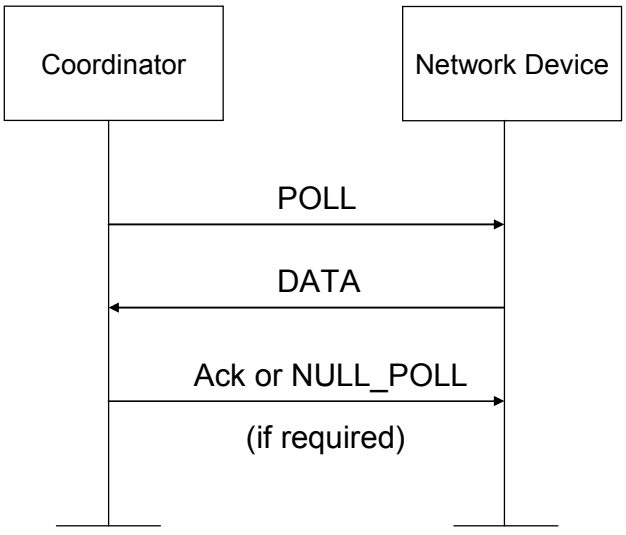


Figure 13 – Single data transmission to coordinator (uplink transmission) in poll based access

In a non poll based access, when a device wishes to transfer data to a coordinator, it simply transmits the data to the coordinator using contention based access. The coordinator may acknowledge the successful reception of the data by transmitting an optional acknowledgment frame. The sequence of operations is summarized in Figure 14.

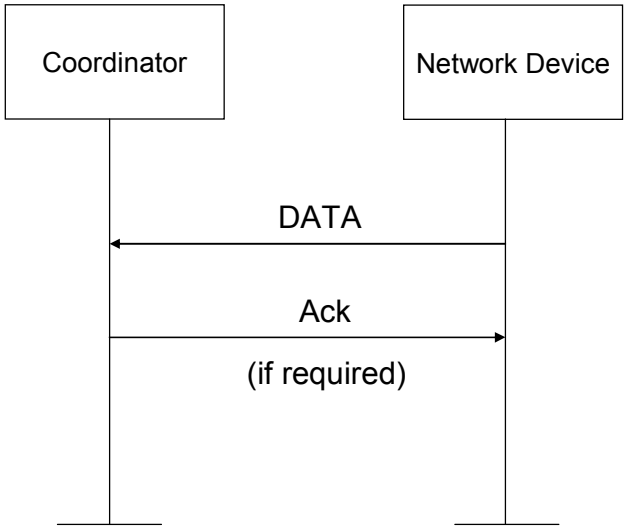


Figure 14 - communication to coordinator (uplink transmission) in contention based access

6.1.1.1.2 Block data transfer

When a device wishes to transfer block of data to a coordinator or coordinator has to collect multiple pending data from the device using poll based access, device first listens to the POLL message transmitted by the coordinator and transmits the block of data to the coordinator. The coordinator may acknowledge the successful reception of the data by transmitting an optional NULL_POLL or block acknowledgment frame. The sequence of operations is summarized in Figure 15.

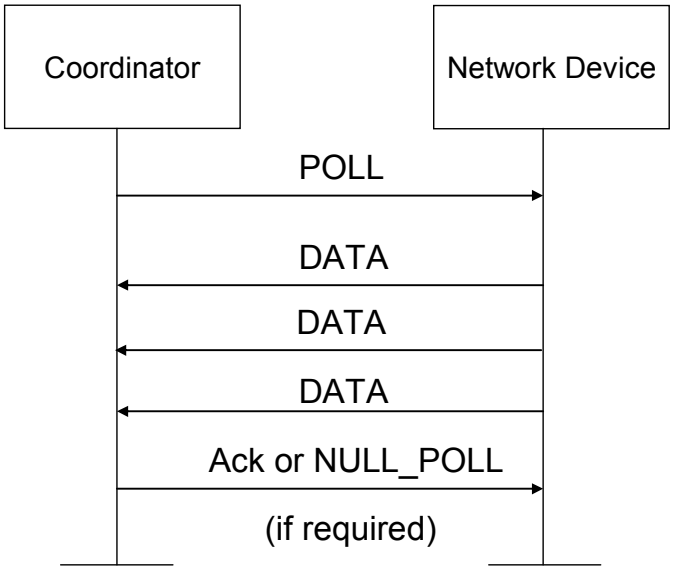


Figure 15 – Multiple data transmission to coordinator (uplink transmission) in poll based access

When a device wishes to transfer block of data to the coordinator in a non poll based access, it simply transmits the multiple data to the coordinator using contention based access. The coordinator may acknowledge the successful reception of the data by transmitting an optional acknowledgment frame. The sequence of operations is summarized in Figure 16.

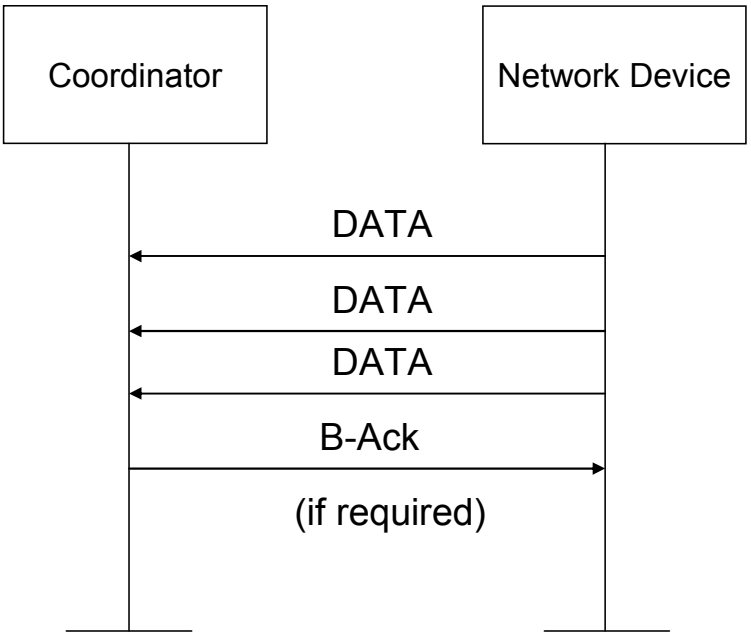


Figure 16 - Multiple data transmission to coordinator (uplink transmission) in contention based access

6.1.1.2 Data transfer from a coordinator (Downlink Transmission)

6.1.1.2.1 Single data transfer

When the coordinator wants to transfer data to a device, it can simply send the data. The device may acknowledge the successful reception of the data by transmitting an acknowledgment frame. This sequence is summarized in Figure 17.

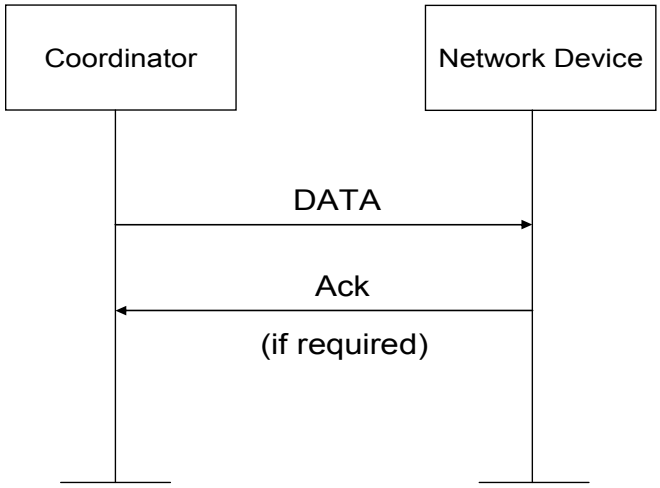


Figure 17 - Single data transmission from coordinator (downlink transmission)

Sometime the coordinator can also combine downlink data transmission with uplink data transmission by putting data as payload of POLL message. This model of downlink data transmission is restricted to the limited data which can be easily fitted to the POLL message. . This sequence is summarized in Figure 18.

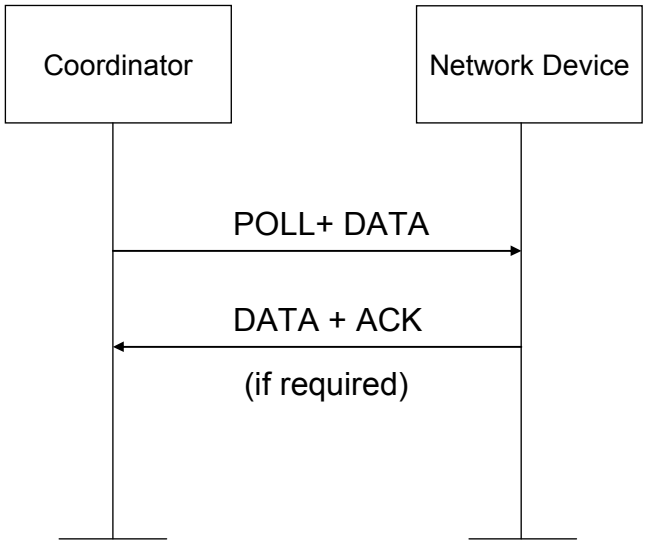


Figure 18 - Single data transmission from coordinator (downlink transmission) combined POLL

6.1.1.2.2 Block data transfer

When the coordinator wants to transfer multiple data to a device, it can simply send the block of data without waiting for acknowledgement. The device may acknowledge the successful reception of the block of data by transmitting a block acknowledgment frame. This sequence is summarized in Figure 19.

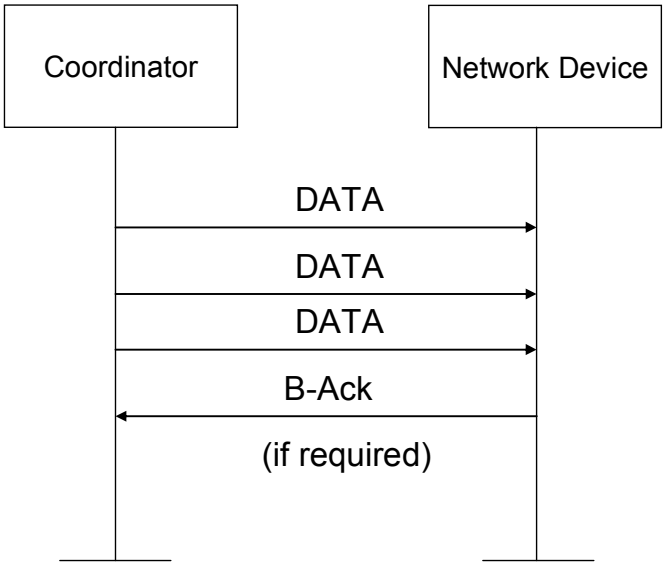


Figure 19 - Block data transmission from coordinator (downlink transmission)

6.1.2 Superframe structure

A time interval established by coordinator divided into multiple parts to facilitate various channel access method to the network devices. The superframe duration (SD) is decided by the coordinator to meet the communication requirement of all connected devices to the network. The detailed calculation of superframe duration can be found in Appendix 'C'. The superframe is divided in to three major parts.

6.1.2.1 Generic Superframe Structure

6.1.2.1.1 Poll Period (PP)

This period is used by the coordinator to provide poll based channel access to the network devices by polling each device as per polling mechanism and poling scheme employed for the device. This period is mainly used for transmission of data frames to and from the coordinator. The size of poll period in a superframe depends upon number of devices and allocated time interval (allocation interval) to each device. The size may or may not very across the superframes depending upon the employed polling mechanism.

6.1.2.1.2 Extended Poll Period (EPP)

This period is used to handle the additional data transmission and retransmission required by device/coordinator due to packet drops, variability in packet arrival rate and on demand traffic. Allocation intervals in EPP are not pre-scheduled and it is scheduled run-time during the poll period of superframe to a device for additional data transmission and/or retransmission of frames. The actual length of EPP in a superframe is not fixed across superframes; it depends upon the dynamic requirement of devices and channel conditions. The size of EPP in a superframe can very from 0 to (SD – PP – minCAP – IP).

6.1.2.1.3 Contention Access Period (CAP)

This portion is used for transmission of data/control/management frames to and from the coordinator. The channel access mechanism implied in this portion is contention based in which devices first contend to acquire the channel for before data transmission. The CAP may be absent if not required. The length of contention access period is dynamic across the superframes. When present, the duration of CAP (if present) may very from minCAP to (SD – poll period – EPP – IP).

6.1.2.1.4 Inactive Period (IP)

The superframe can also have optional inactive portion. During inactive portion either coordinator may enter into a low power mode or use the inactive period to share the channel bandwidth with other coexisting networks.

6.1.2.1.5 End of Poll (EoP)

A special frame marker End of Poll (EoP) is sent by the coordinator after completion of PP to advertise the duration of EPP, CAP and IP.

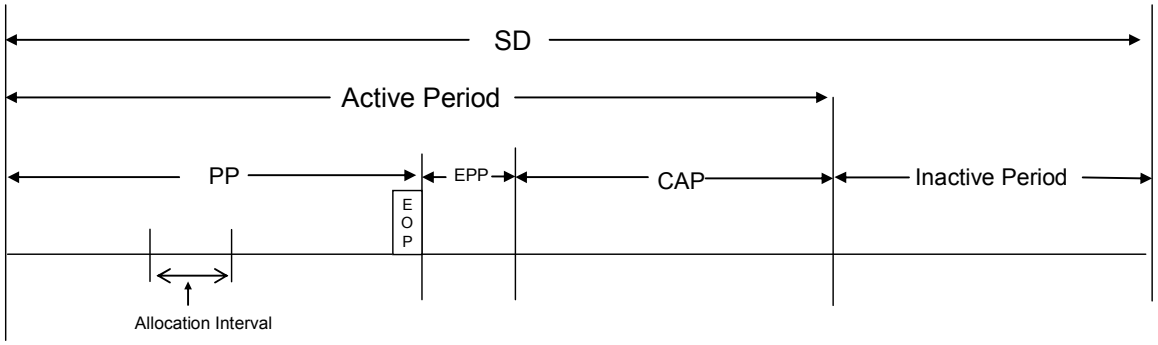


Figure 20 – Generic superframe structure

6.1.2.2 Specific Superframe structures

The superframe duration (SD) is not always fixed, in certain cases superframe duration may very across the consecutive superframes. The periods discussed in generic superframe are optional. No superframe structure is defined, if EPP and CAP are absent and PP is dynamic. The possible superframe structures are outlined below.

6.1.2.2.1 Superframe without inactive period

The coordinator may decide based upon load and traffic requirements not to have any inactive period in the superframe. In case inactive period is present the coordinator may choose not to sleep in this period in order to receive emergency messages in case of implant or to support coexistence of other networks in the same channel. Figure 21 shows superframe structure without inactive period.

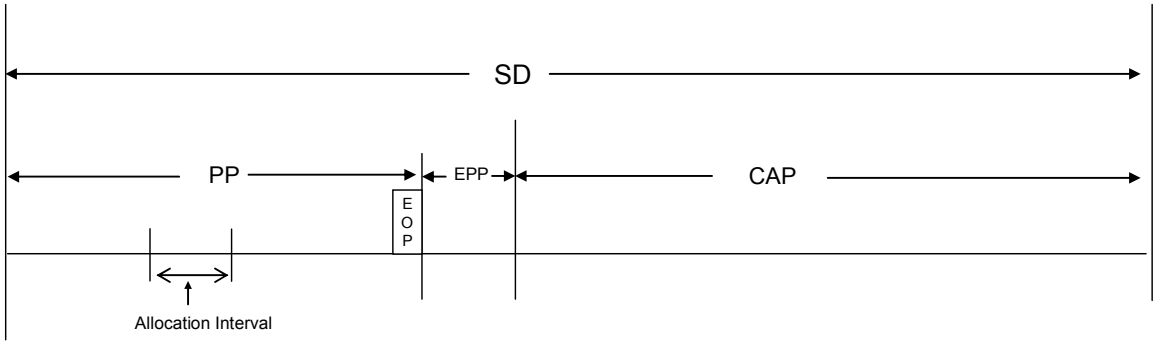


Figure 21 – Superframe structure without inactive period

6.1.2.2.2 Superframe when CAP is not present

In certain cases especially for implant where number of implant devices are very less as compared to on body devices. The implant devices may be pre associated at the time when they implanted or the association of implant device may be coordinator initiated. In this case the implant device may not require contention access mechanism to further reduce its complexity and power consumption. Figure 22 shows superframe structure when CAP is not present.

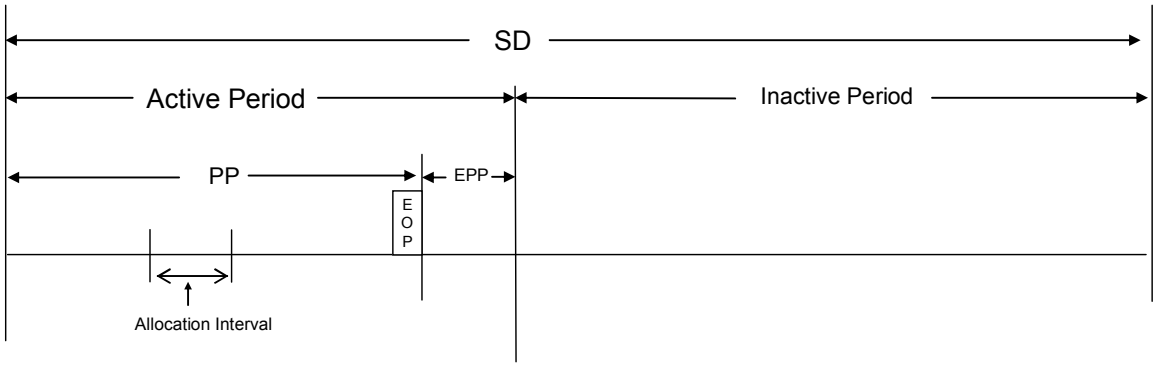


Figure 22 - Superframe structure without CAP

6.1.2.3 Fixed length Vs Variable length superframe

The size of superframe may be fixed or variable. The fixed superframe is useful for power constraint devices (medical) with deterministic or periodic packet generation. The fixed superframe provides a deterministic sleep and wakeup schedule for the device. The variable superframe is useful to support data transfer from non-medical devices with non-deterministic and busty packet arrivals. Typically, non-medical applications have stringent QoS (Delay and Jitter) requirement. In case of variable superframe, the EPP is not required as the variability and retransmission is handled by varying the size of superframe. Figure 23 and Figure 24 shows superframe structure with fixed and variable superframe duration respectively.

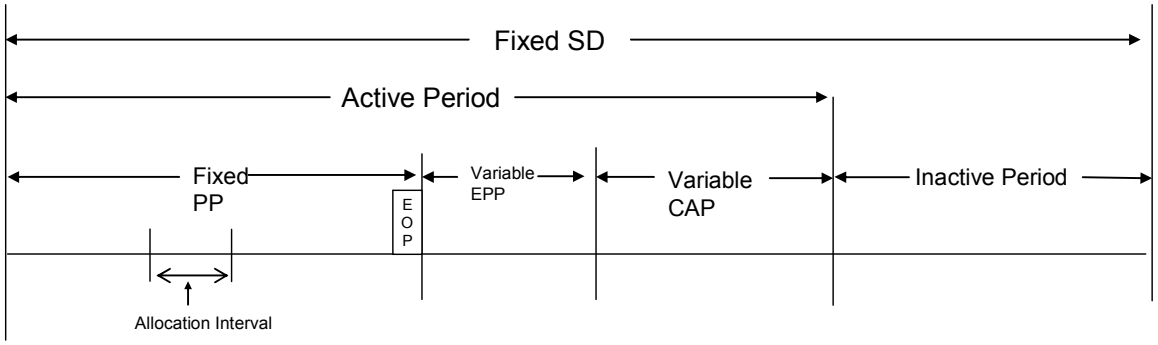


Figure 23 – Fixed length superframe

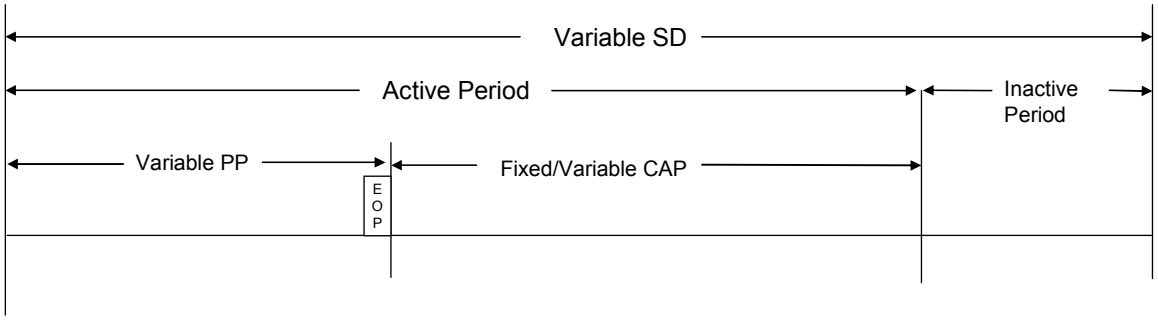


Figure 24 – Variable length superframe

6.1.2.4 No superframe

It is also possible that only variable PP is present in a superframe without CAP and Inactive period in this special case no superframe structure as such defined by the coordinator. Figure 25 shows the variable PP with no superframe structure. The coordinator may decide not to transmit the EOP periodically and it may transmit an equivalent broadcast message occasionally to facilitate certain network operations.

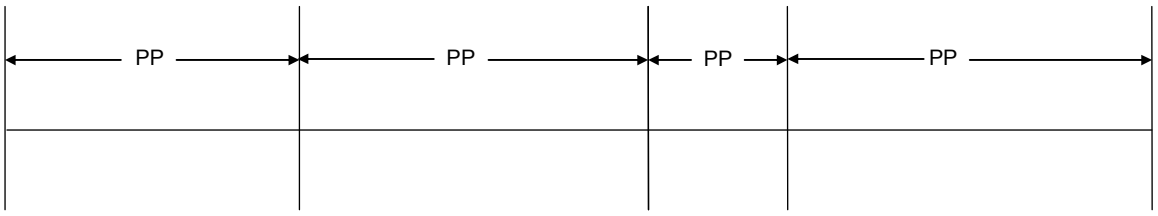


Figure 25 – Polling with no superframe structure

6.1.2.5 Channel time partitioning

The channel time unit is characterized by the symbol duration. The absolute value of symbol duration depends upon PHY. All the access mechanisms detailed above can be implemented

using both slotted and un-slotted system. In slotted system the time is partitioned into equal number of slots (multiple of symbol durations) and every frame transmission should commence at start of the slot boundary. On the other hand un-slotted system the channel time is not marked and frame transmission is allowed at any channel time.

6.1.2.6 Polling Mechanism

This section details out different polling based access mechanism and their applicability to the specific superframe structures. In order to grant channel access in the poll period (PP) of superframe, the coordinator sends POLL message to the devices. The coordinator transmits the POLL message to the devices at scheduled allocated time or with some delay to the allocated time or any time during the PP. The device may transmit no data packet, single data packet or multiple data packets on reception of the single POLL message. The number of packets a device can send after receiving a POLL message is conveyed through the POLL message itself by the coordinator. If the device does not have any data to send, the device may transmit NULL_DATA back to the coordinator in response to POLL message.

6.1.2.6.1 Scheduled Polled access

This mechanism is useful for medical (implant and nobody) devices with constant bit rate (CBR) or periodic traffic. The access method is supported by fixed superframe duration and fixed PP inside the superframe. Since the PP is fixed, the location of EoP message is also fixed. Each device is allocated a fixed time interval in PP. The devices are polled at the start of the allocated interval. The device need to wakeup (if sleeping) before its allocated interval in order to correctly receive the POLL message. An allocation interval can be used either for single or multiple data transmission. No frame transmission from or to the device shall commence beyond the allocated interval. The coordinator can move to the next device after the completion of allocated interval of the device. A device can be polled either every superframe or after multiple superframes based upon device application requirement. If a device needs to transmit data more than the allocated time, the device will communicate the requirement to the coordinator through ‘more bit’ in the data packet. If the device has communicated its additional requirement through the ‘more bit’ to the coordinator during the schedule allocation interval, the coordinator will poll the device again during the EPP period of the same superframe to provide channel access to the device. The device may go back to sleep after completion of allocation interval and can wakeup at the extended poll period (EPP) to send additional data. If the data transaction between coordinator and device is completed with in the allocation interval, the coordinator may send the NULL_POLL message to the device. The NULL_POLL message helps device to go to sleep mode when the transmission is completed before the completion of allocation interval.

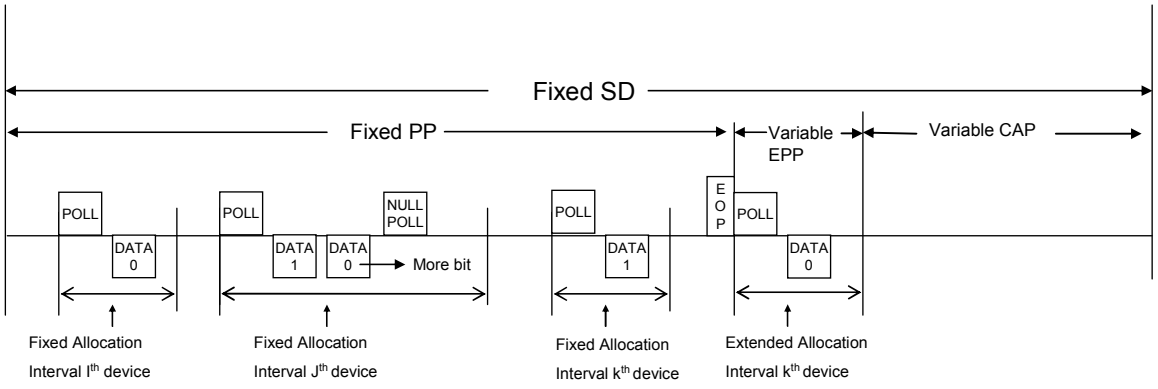


Figure 26 – Example of scheduled polling and use of extended poll period

6.1.2.6.2 Delayed Poll access

This mechanism is useful for on body non medical devices with constant bit rate (CBR) or periodic traffic. The access method is supported by fixed superframe duration with variable PP inside the superframe. Since the PP is variable the location of EoP message is not fixed. Each device is allocated a time interval in PP. The devices can be polled any time after the start of the allocated interval. The device need to wakeup (if sleeping) before its allocated interval in order to correctly receive the POLL message. An allocation interval can be used either for single or multiple data transmission. Frame transmission from or to the device can spill over to the adjacent allocated interval to handle the variability and retransmission. Since the retransmission and variability is handled by extending the allocated interval dynamically, therefore the extended poll period (EPP) is not required. The coordinator can decide to continue with the current device to handle the variability and retransmission due to packet losses. A device can be polled either every superframe or after multiple superframes based upon device application requirement. If the device has communicated its additional requirement through the 'more bit' to the coordinator at the schedule time interval, the coordinator will poll the device immediately in the current allocation interval. If 'more bit' in data frame received from the device is reset, the coordinator can switch to the next device at/after next device's allocated time interval. The NULL_POLL helps the device to go back to the sleep instead of waiting for further response from the coordinator.

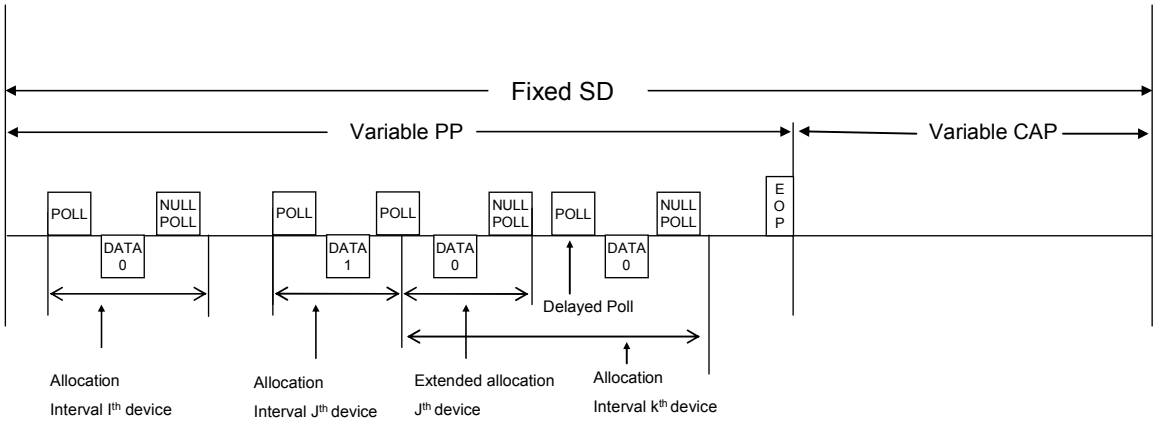


Figure 27 - Example of delayed polling

6.1.2.6.3 Unscheduled Polled access

This mechanism is primarily useful for on body non medical devices with variable bit rate (VBR) and burst traffic. The access method is applicable to variable superframe duration with variable PP inside the superframe. Since the PP is variable the location of EoP message is not fixed. The devices are not assigned any pre allocated time interval. The coordinator can poll a device any time during the poll period and the device needs to be in the ON state to correctly receive the POLL message. Once the device is polled it can either transmit single or multiple data. All variability and retransmissions are handled immediately. Since the retransmission and variability is handled by extending the allocated interval dynamically, therefore the extended poll period (EPP) is not required. A device can be polled either every superframe or after multiple superframes based upon device application requirement. If 'more bit' in data frame received from the device is reset, the coordinator can switch to the next device immediately. The transmission of NULL_POLL is not necessary.

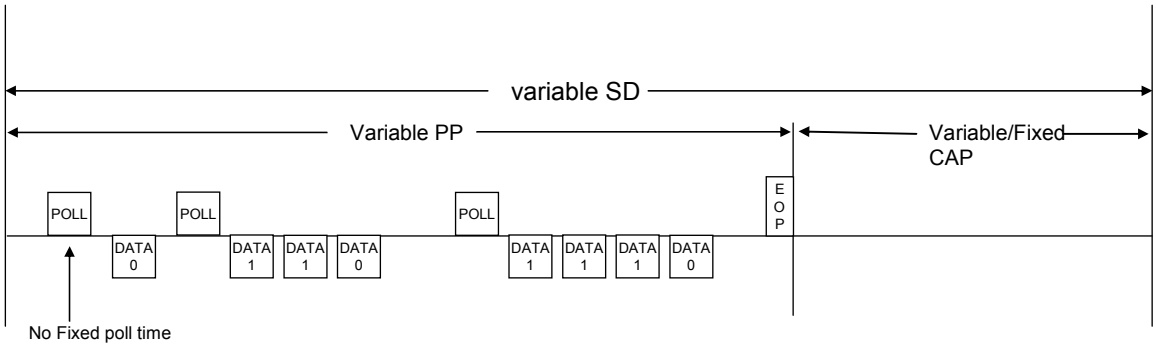


Figure 28 – Example of unscheduled polling

6.1.3 Polling Schemes

This section details out various polling schemes or MAC scheduling. The coordinator completes data transaction activity with every device one by one in a cyclic manner, defined as poll cycle. A session is defined between the coordinator and device for the duration the coordinator sends first POLL message to the device and switches to next device. In a session coordinator can send single

or multiple POLL messages to collect data from the device and move to the next device. Based on different conditions, coordinator can move to the next device. The different conditions include, when device has no more data to transmit, or when the allocated interval is over, or when the device has already transmitted its maximum allowed data frames as specified by the Polling scheme, or when maximum poll retry is exhausted, or when emergency event has occurred in another device.

In case of superframe structure, the devices can opt to be polled in every i^{th} ($i > 0$) superframe and coordinator need not have to POLL the device in every superframe.

The coordinator can collect required data packets from device either by sending single POLL message or multiple POLL messages. The number of packets a device can transmit upon receipt of a POLL is communicated through POLL message itself. How many packets a device can transmit in a session is defined by polling scheme employed for the device. Following are the supported polling schemes. Figure 29 shows poll based data transfer with different schemed.

6.1.3.1 Single data polling

In this polling scheme the coordinator need to collect single data in a session with the device. To collect the data from the device the coordinator sends a POLL message to the device. The device can transmit only a single data frame on receipt of this message. The *pktSeqnumber* in the message indicates that all previous data frames including frame with this sequence number has been received successfully at the coordinator. The transmitted data frame could be retransmission of previously transmitted packet or new packet transmission depends upon *pktSeqNumber* specified in the message. The error recovery mechanism associated with the poll based channel access is detailed in a later section. This polling scheme is particularly suitable for devices with deterministic packet generation and has low latency requirement. Since, only single data need to be collected this polling scheme is mainly suitable for scheduled and delayed polled access methods with fixed superframe structures.

6.1.3.2 Limited data polling

In this polling scheme the coordinator need to collect multiple but limited data in session with the device. To collect the data from the device the coordinator sends a POLL message to the device. The device can transmit data frames up to the number of packets stored in the buffer upon reception of this message. The *pktSeqNumber* in the message indicates that all previous data frames including frame with this sequence number has been received successfully at the coordinator. The transmitted data frame could be retransmission of previously transmitted packet or new packet transmission depends upon *pktSeqNumber* specified in the message. Since, deterministic number of multiple data needs to be collected, this polling scheme is mainly suitable for scheduled and delayed polled access methods with fixed superframe structures.

6.1.3.3 Exhausted data polling

In this polling scheme the coordinator can collect unlimited data in a session with a device. To collect the data from the device the coordinator sends POLL message to the device. The device can transmit multiple data frames as specified in the ‘window size’ field of the POLL message. The *pktSeqNumber* in the message indicates that all previous data frames including frame with this sequence number has been received successfully at the coordinator. The transmitted data frame could be retransmission of previously transmitted packet or new packet transmission

depends upon *pktSeqNumber* specified in the message. This polling scheme is particularly suitable for traffic with non deterministic and burst packet arrivals. Since, the number of packets a device can transmit in a session is non deterministic, this polling scheme is mainly suitable for unscheduled access methods with variable or no superframe structures. The polling scheme is also applicable with fixed superframe structure when devices with deterministic and non-deterministic traffic characteristics exist together.

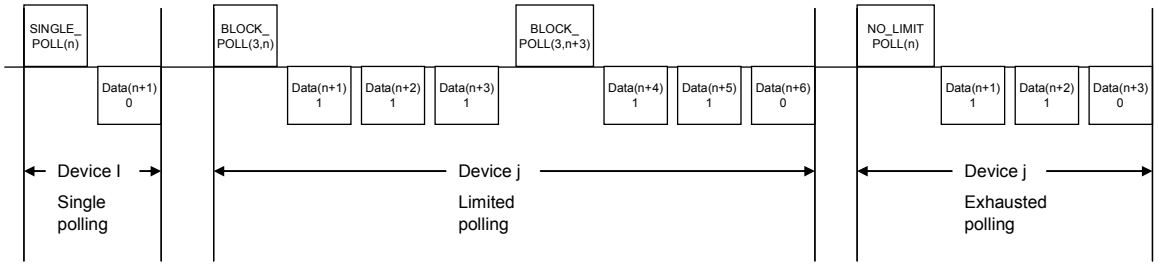


Figure 29 – different polling schemes

6.1.4 Random Access Mechanism

The random access mechanism shall run at the contention access period (CAP) of superframe structure defined by the coordinator. It will be primarily used for network management related protocol message exchange between device and coordinator and for non QoS applications. Since the carrier sensing is not reliable across all channel models and PHYs any variant of collision resolution other than carrier sense can be adopted.

6.1.5 Channel Time Partitioning

The channel time unit is characterized by the symbol duration. The absolute value of symbol duration depends upon PHY. All the access mechanisms detailed above can be implemented using both slotted and unslotted system. In slotted system the time is partitioned into equal number of slots (multiple of symbol durations) and every frame transmission should commence at the start of the slot boundary. On the other hand unslotted system the channel time is not marked and frame transmission is allowed at any channel time.

6.1.6 Device clock synchronization

The power constraint devices, especially medical devices try to sleep most of the time to save the power, when there is no data transaction going on with the coordinator. Such devices need to synchronize their sleep and wakeup schedule with coordinator in order to receive the POLL message sent by the coordinator. Since the device can only transmit data when polled in poll based access, no synchronization is required for data transmission. In addition the devices which do not need to save the power have no synchronization requirement at all. The synchronization requirement is applicable to fixed superframe only. In case of variable superframe, the next poll time is not fixed the devices has to be awake all the time. The polling rate for a device could be multiple of polling cycle established by the coordinator. An “on-time” bit in the POLL message is used to inform the devices the start of allocation interval. Additionally the POLL message may

contain a timestamp value, if not transmitted on time. The device can calculate the next POLL time to synchronize with the coordinator to receive the next POLL message correctly. The devices will not use received POLL message for synchronization if "on-time" bit is not set. The device has to wakeup before its next scheduled poll time to receive the next poll message. The duration before scheduled POLL time i.e. guard time a device need to wakeup depends upon maximum clock skew can occur at the device with respect to coordinator after reception of last POLL message with 'on time' bit set for synchronization. The duration between two on time POLL message is called synchronization duration. In case of downlink traffic, the coordinator can send a NULL_POLL message before actual data with "on-time" bit set, for device synchronization. The Figure 30 explains the device synchronization in a poll based access with fixed superframe structure.

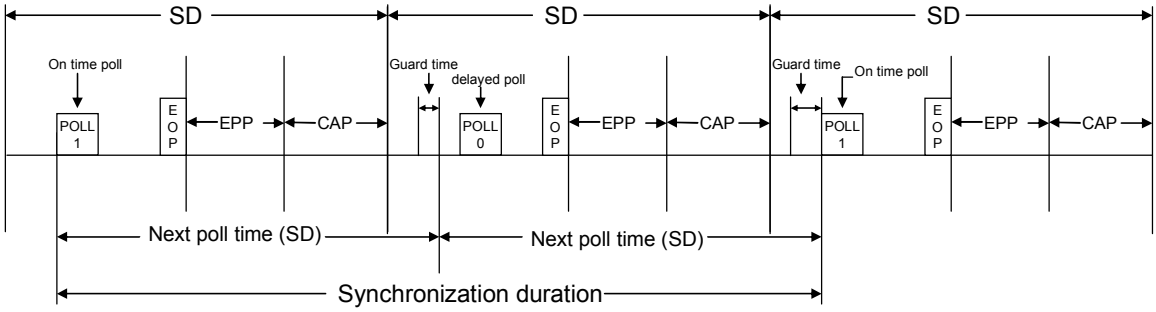


Figure 30 – The synchronization of sleep and wakeup schedule of device with the coordinator

6.1.7 Data aggregation

These data samples may be generated in frequently, say multiple samples per sec. In these cases, where multiple data units are already available for transmission, aggregation of data into one transmission unit would be advantages. If an implant device transmits each data unit separately, then each packet has its own MAC header whose length becomes considerable with respect to the actual data size. Also, the turn around time for the transmission of a frame and waiting for the inter frame time before the next transmission is high. Individual transmissions of small size packets lead to excessive power consumption and under utilization of bandwidth.

Data aggregation is a useful technique to avoid this kind of power and bandwidth wastages. In data aggregation, multiple MPDU of the same type (DATA) are aggregated into a single large data unit and sent through as a single packet. A new MAC type called AGR_DATA is defined for this purpose. The maximum number of octets in the frame body of the AGR_DATA PDU SHALL be determined by the Link MTU established during link activation procedure. If acknowledgement is expected for the data frames, then the number of frames that are aggregated is restricted to the receive window size of the receiver.

The use of aggregation frame reduces the ratio of power consumption spent in transmission of header bits to the power consumption in the transmission of actual data bits. Aggregation can be effectively used with poll based access and in contention based channel access and also with the different acknowledgement mechanisms. The sequence number of subsequent data frames can be found by incrementing the initial value found in the frame control. A single ACK frame is sufficient to acknowledge all the data frames in an AGR_DATA PDU.

But, the data aggregation is not always applicable. Some applications require data units to be delivered within a certain time bound. So, in such applications, the MAC implementation should not wait to do data aggregation which could delay the delivery of data units and result in exceeding their delay bound. Therefore the devices can optionally use the data aggregation until the delay bound is met as per application requirement. Another concern is that the probability, of packet loss is higher for large size packets.

6.1.8 Data fragmentation

This proposal supports data fragmentation, so that large data frames can be transmitted with smaller MTU size supported by the underlying PHY. The fragmentation and reassembly feature is an optional feature of the MAC protocols. The support for fragmentation and also the maximum number of fragments that can be supported are agreed during device association. The MAC frame header provides the frame control, provides the fields to indicate that fragmentation is used and *fragment number, fragment* length and an indication that this is the last fragment. These fields are used by the receiver to reassemble of data frames before giving the complete frame to the upper layer. A BAN MAC supporting the fragmentation and reassembly has to reassemble all the fragments in a data frame and then pass it to the higher protocol layer

6.2 Error Recovery

In order to provide reliable packet transmission the standard supports two kind of error recovery mechanism: poll based error recovery (coordinator driven) applicable only to upstream traffic with poll based channel access and Automatic Repeat Request (sender driven) which is applicable to both upstream and down stream traffic. Since the ARQ based error recovery is not power and bandwidth efficient because of additional transmission of acknowledge of packet, the poll based error recovery is provided to for highly power constraint devices. Additionally, ARQ mechanism requires retransmission of data packet once data packet or Acknowledgement is lost. The poll based access does not allow retransmission of packet without any response received from the coordinator otherwise it can lead to the collision of retransmitted packet with poll message. The situation is shown in Figure 31.

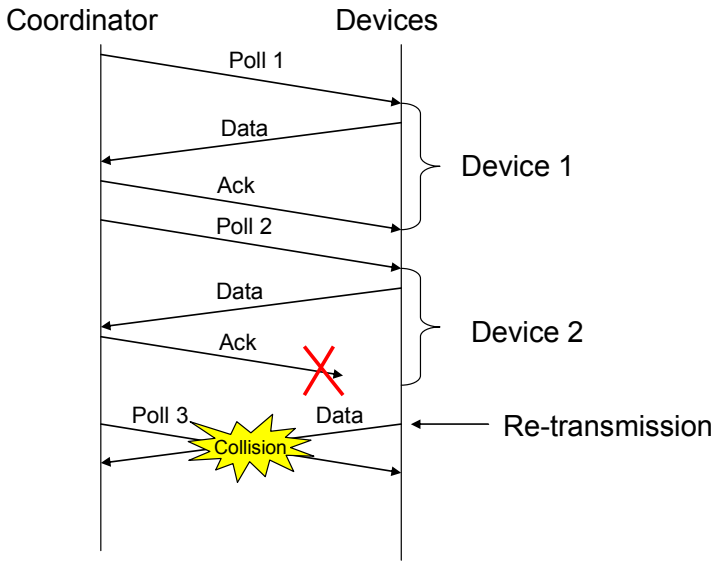


Figure 31 - Data retransmission can lead to poll and data collision

6.2.1 Poll based error recovery

The poll based error recovery mechanism is integrated part of poll based channel access mechanism and does not require separate acknowledgement to be sent by the coordinator in response to receipt of a packet from the device. This error recovery is coordinator driven and only applicable to upstream traffic. Following sections detail the poll based error recovery in case of single and block data transfer respectively.

6.2.1.1 Error recovery with single data transfer

Following details the error recovery to handle different kind of packet losses in single data transfer. The Figure 32 - Figure 33 demonstrate the poll based error recovery for single and block data transmission.

6.2.1.1.1 SINGLE_POLL message transmission, reception and retransmission

- The coordinator sends SINGLE_POLL message to the device with 'pktSeqNum' number asking device to send packet with sequence number next to 'pktSeqNum'
- On receipt of SINGLE_POLL message the device transmits a single data with sequence number next to the specified "pktSeqNumber" in the SINGLE_POLL message.
- The device can drop all the transmitted packets from its buffer up to sequence number specified in the SINGLE_POLL message.
- In case the coordinator does not detect any transmission from the polled device or the received data is corrupted, the coordinator will retransmit the SINGLE_POLL message with the following exceptions.

- Data transaction can be completed within the remaining allocated interval in case of scheduled access otherwise the SINGLE_POLL with same 'pktSeqNum' will be sent in next poll cycle.

- Re-transmission of SINGLE_POLL messages is not reached to that *maxPollreTransmission* value.

- The poll period is not extended inside the superframe so the only minCAP is left.

6.2.1.1.2 BLOCK_POLL transmission, reception and retransmission

- The coordinator sends BLOCK_POLL message to the device with 'pktSeqNum' number and 'window size' asking device to send multiple packet specified by window size with starting sequence number next to the 'pktSeqNum'.

- On receipt of BLOCK_POLL message the device transmits number of data as specified in window size field of the message with sequence number next to the specified "pktSeqNum".

- The device can drop all the transmitted packets from its buffer up to sequence number specified in the BLOCK_POLL message.

- In case the coordinator does not detect any transmission from the polled device the coordinator will retransmit the BLOCK_POLL message with same or reduced window size only if:

    - Data transaction for multiple packets can be completed within the remaining allocated interval in case of scheduled access. Otherwise the BLOCK_POLL with same 'pktSeqNum' number will be sent to the device in next poll cycle.

    - Re-transmission of POLL messages is not reached to that *maxPollreTransmission* value.

    - The poll period is not extended inside the superframe so the only minCAP is left.

6.2.1.1.3 BITMAP_POLL transmission and retransmission

- The coordinator will send BITMAP_POLL to the device only if it receives partial number of packets from the device in response to the BLOCK_POLL message and the last packet received from the device is not received with 'more bit' reset. The message specifies 'pktSeqNum', 'window_ size' and bitmap of packets to be retransmitted.

- In case the coordinator does not detect any transmission from the polled device the coordinator will retransmit the BITMAP_POLL message with same or reduced window size only if:

    - Data transaction for multiple packets can be completed within the remaining allocated interval in case of scheduled access. Otherwise the BITMAP_POLL with same 'pktSeqNum' number will be sent to the device in next poll cycle.

- Re-transmission of POLL messages is not reached to that *maxPollreTransmission* value.
- The poll period is not extended inside the superframe so the only minCAP is left.

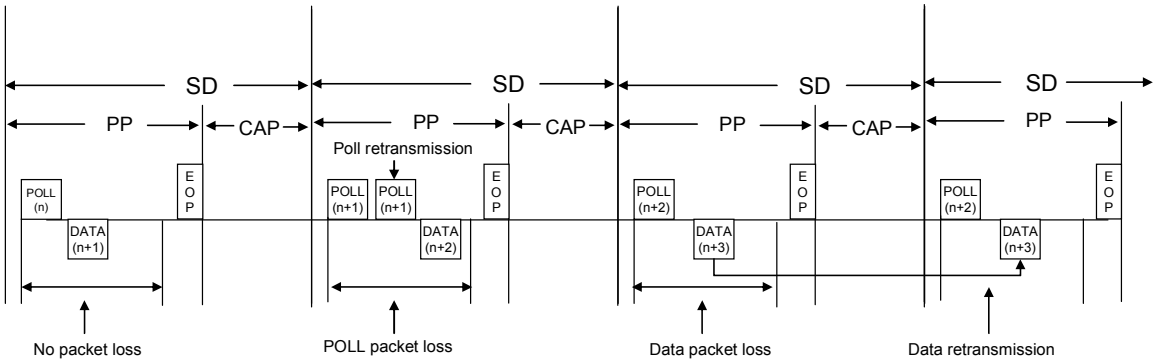


Figure 32 – Poll based error recovery for single data transfer

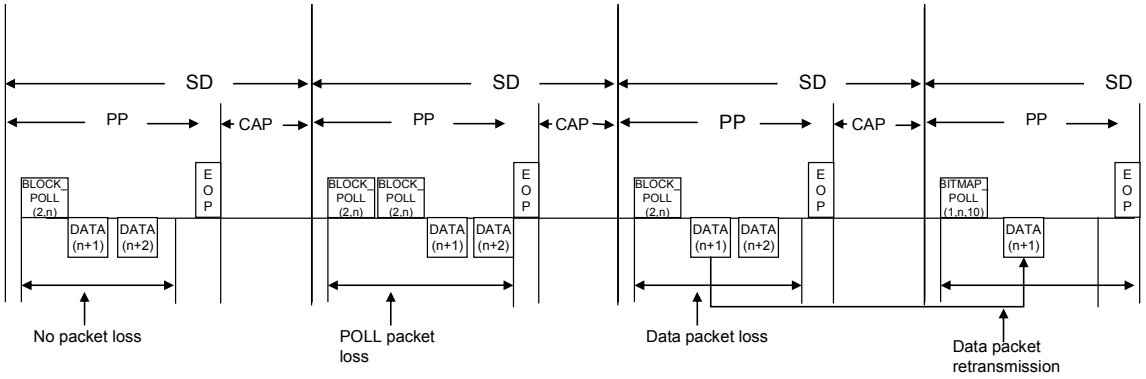


Figure 33 - – Poll based error recovery for block data transfer

6.2.2 Automatic Repeat Request (ARQ) based error recovery

The ARQ based error recovery is applicable to both upstream and down stream traffic. Stop and wait ARQ mechanism shall be used for single data transfer with immediate acknowledgement and selective repeat ARQ shall be used for block data transfer with delayed acknowledgement specifying the bitmap of successful transmission.

6.3 Power Management

6.3.1 Sleep and wakeup across superframe(s)

The scheduled and delayed polling channel access mechanisms facilitate device to sleep between their consecutive polls. The length of the time a device can sleep depends upon it poll rate. The device need not have to wakeup at every superframe if it is being polled after multiples superframes. Once the device is awake in PP it can go back to sleep as early as possible with different power saving options.

6.3.2 Power saving options

The power saving options provides the flexibility to the device to save the power. Different level of power save options facilitates the device to go back to sleep as early as possible after completion of data transaction with the coordinator. There are four different levels of and each level defines how early the device can go back to sleep after data transmission requested by the coordinator through the poll message.

6.3.3 Level 1

Device can directly go to sleep after transmitting requested number of data packets by the coordinator if “sleep” bit in the received POLL message is set.

6.3.4 Level 2

If “sleep” bit is not set in the received POLL message the device can wait for NULL_POLL from the coordinator to go back to sleep after transmitting requested number of data packets by the coordinator.

6.3.5 Level 3

Device can go back to sleep after completion of scheduled access interval if no NULL_POLL is received, in case of scheduled access.

6.3.6 Level 4:

Device can go back to sleep on reception POLL message for the next device in case of delayed poll access

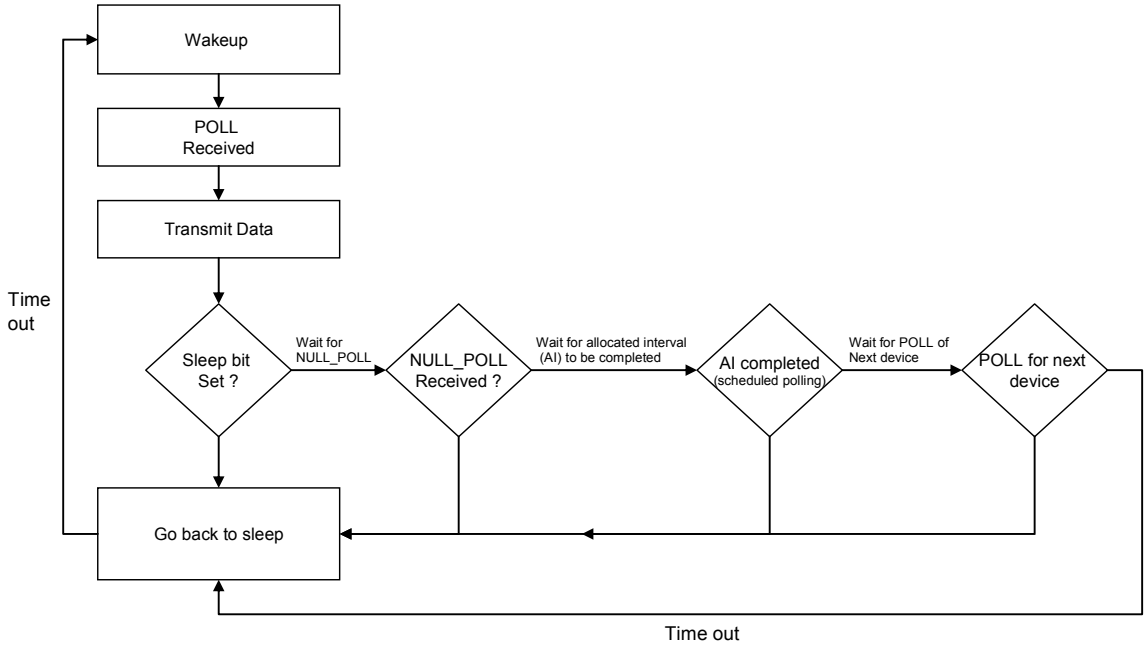


Figure 34 – Flow diagram for microscopic power saving

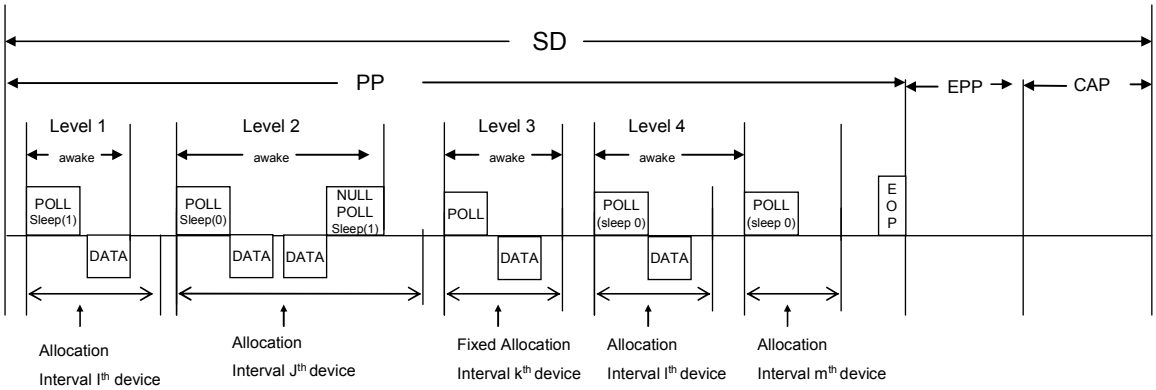


Figure 35 – Example power saving options

6.4 Implant specific mechanisms

6.4.1 Wakeup mechanism

Figure 36 shows the in general sequence of operations performed by the coordinator to accomplish a data communication session with the implant device(s). To start a network, the coordinator has to select an interference free channel by performing listen before talk (LBT) and ensuring that no other implant network or primary user (the licensed user of allocated spectrum) is already present in the channel. If no free channel available, then it tries to coexist with other networks using suitable co-existence mechanism.

The implantable devices are resource constraint especially in terms of power. The lifetime of implantable device could vary from several hours to few years. Once the device is implanted the

battery can not be changed during its lifetime. This constraint mandates the implant device to sleep most of the time when there is no communication required between implant device and external programmer. In this case whenever external programmer/data collector wants to set some parameter of the implant device or collect some data from the implant device, it has to first wakeup the device and then establishes a communication session.

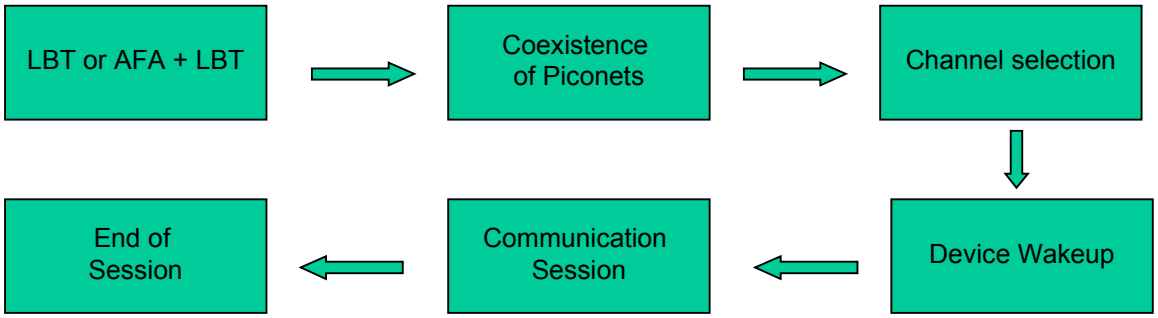


Figure 36 – Implant medical communication

6.4.1.1 In band wakeup mechanism

The in band wakeup mechanism uses operating channels available for data and control transmission to wakeup the sleeping implant device by the external coordinator. This mechanism does not require extra wakeup radio along with regular transceiver. The coordinator uses the regular transmitter to send the wakeup signal and implant device receives the wakeup signal through regular receiver only. The coordinators can either wakeup a single device or multiple devices for a single communication session using respective mechanisms. The Fig. shows the different states for implant device and transition between them.

6.4.1.1.1 State Diagram

An implant device could be in one of the following states. The switching between the states depend upon type of event occurred.

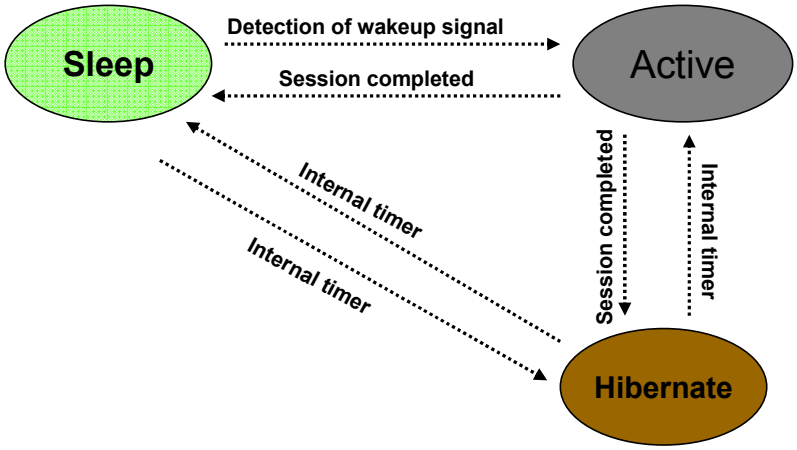


Figure 37 – Implant device state diagram

6.4.1.1.1.1 Active

In this state the device is awake and does not require externally to be waked up by the coordinator. The device may or may not be part of active communication session. A device is considered to be in '**Active'** state if sleeps between consecutive polls to save the power during a communication session. The device can go to sleep state or Hibernate state upon completion of a data session from this state.

6.4.1.1.1.2 Sleep

In this state device is duty cycling at all available channels in a low power mode (most of the receiver circuit is switched off except energy detector) to receive the wakeup signal sent by the coordinator. The device can go to active state on reception of a wakeup signal or Hibernate state when internal timer timed out from this state.

6.4.1.1.1.3 Hibernate

In this state the transceiver of the implant device is completely switched off (along with energy detector) and only the internal timer at the device is running to facilitate self wakeup before next scheduled time pre established with the coordinator.

6.4.1.1.2 Device duty cycling

The channel for wakeup is not fixed. The implant device duty cycles at all available frequency channels one by one in a periodic manner as shown in Figure 38. The actual ratio of Rx_ON and Rx_OFF time while duty cycling, depends upon latency, reliability and power consumption requirements of the system. Increase in the ratio of Rx_ON to the Rx_OFF reduces wakeup latency and increases reliability and power consumption. When a device receives wakeup signal intended for the device from the coordinator, it acknowledges the receipt of wakeup signal and switch its state from sleeping to active. Once the device is active it waits for next instruction from the coordinator and is assumed to be awake.

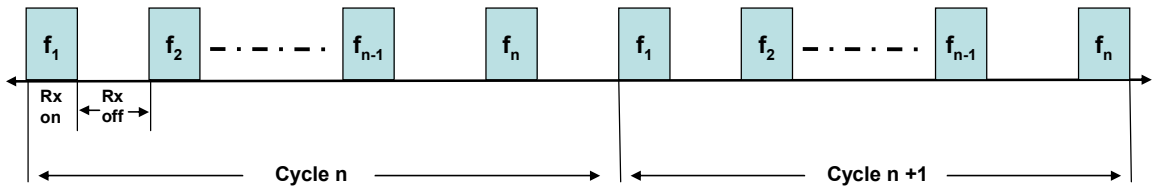


Figure 38 – Implant device duty cycling

While duty cycling, an implant device may receive interference from other operational implant networks or wakeup signal from its own coordinator but not the intended one to be waked up. This would lead to overhearing at the implant device and thus higher power consumption. To avoid this, if an implant device receives any potential interference from neighborhood implant networks or from its own network in a particular channel, the device excludes that channel from the available channels list and stops duty cycling on that channel for a specified duration. An example is shown in Figure 39. While duty cycling in channel '2', device receives a wakeup signal which is not intended for it and stops duty cycling in channel '2'. In this manner when the coordinator starts a communication session with implant device(s) all other devices which are not part of active session stops duty cycling on that channel in which communication session is established and avoid overhearing due to regular data communication. Similarly if a device receives interference due to data communication of its own network while it is not part of active session, it stops duty cycling on the operation channel for specified duration.

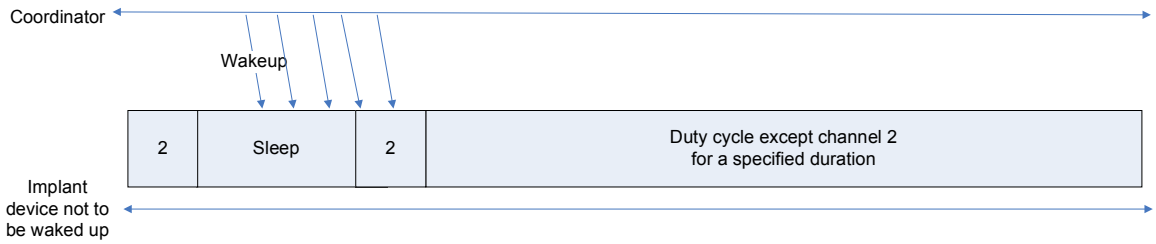


Figure 39 – The device stops duty cycling at channel to avoid interference

6.4.1.1.3 Single device wakeup

In order to wakeup a device the coordinator starts sending wakeup signals in the selected channel with target implant device id as destination address and more bit set to 0, till it receives ACK from the implant device as shown in the Figure 40. 'M' bit facilitates other non intended devices to stop duty cycling on the channel to avoid overhearing. After reception of ACK the coordinator assumes that device is awake and communication session is established. At the end of the communication session the coordinator may instruct the device to go back to sleep/hibernate state. The session is assumed to be closed by the implant device if there is no communication from coordinator for a specified duration and it goes to sleep mode automatically.

Sometimes it may be possible that already a data communication session is active with other devices when coordinator wants to wakeup an implant device. To avoid overhearing due to interference the devices stop duty cycling in the channel in which active session is operational. In this case the coordinator can not send wakeup signal on the same channel to wakeup the device. Furthermore if the coordinator uses the same channel in which active session is operating for wakeup, this will lead to overhearing of wakeup signals for the devices which are part of active session. To avoid this problem coordinator selects a new interference free qualified (according to

FCC regulations) channel and performs wakeup in newly selected channel. In this way the devices which are already part of active session do not receive the wakeup signal sent by coordinator, thus avoid overhearing.

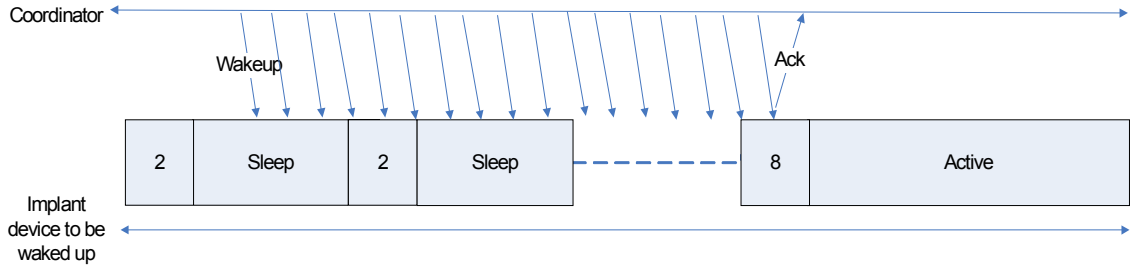


Figure 40 – Single device wakeup

6.4.1.1.4 Multiple device wakeup

The one by one wakeup procedure leads to higher wakeup latency and signal overhead. This section describes a two phase wakeup mechanism for simultaneous wakeup of multiple devices.

6.4.1.1.4.1 Lockup Phase

As shown in the Figure 41, the coordinator transmits lockup signal in the selected channel for a specified duration of time ensuring that all implant devices should have received at least one lockup signal in this duration. The LOCK_UP signal is sent with the list of address for all the devices to be waked up. If a group of devices needs to be waked up their GROUP_ID can be used as destination address instead of individual addresses. Similarly in case all devices need to be waked of broadcast address (0xFF) can be used. In this phase the devices those are intended to be waked up stop duty cycling and lock themselves in the channel in which lockup signal has been received and wait for WAKE_UP signal. The devices do not send ACK on reception of LOCK_UP signal. On the other hand all unintended devices stop duty cycling in the channel on reception of LOCK_UP signal. The LOCK_UP signal is send at least for the duration in which implant device completes its one cycle while duty cycling.

6.4.1.1.4.2 Wakeup Phase

Once the lockup phase is over, all intended devices are waked up but yet not acknowledged. In this phase, coordinator sends wakeup signal individually to confirm that device is really awake. Since the devices has already been locked in the selected channel and their receiver is ON (not duty cycling), only one wakeup (or few in case of wakeup drops) signal is required to receive the acknowledgement. The Figure 41. shows the multiple wakeup procedure

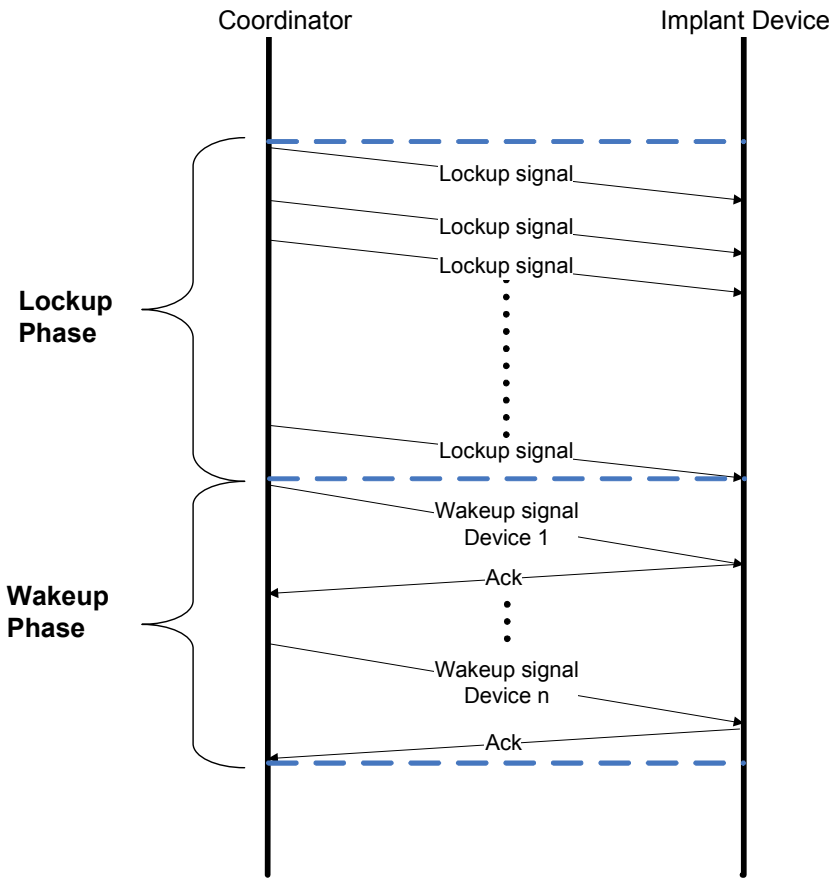


Figure 41 – Multiple device wakeup

6.4.1.2 Out band wakeup mechanism

For non-MICS band wake up, when an IMD is in deep sleep mode, non-MICS RX will keep listening for wakeup signal from coordinator in a non-MICS channel, which has least interference. When a signal is detected by energy detector on the channel, sync detector module verifies if it is a BAN wake up signal. If continuously 2 or 3 non-BAN signals are detected on the channel, 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.

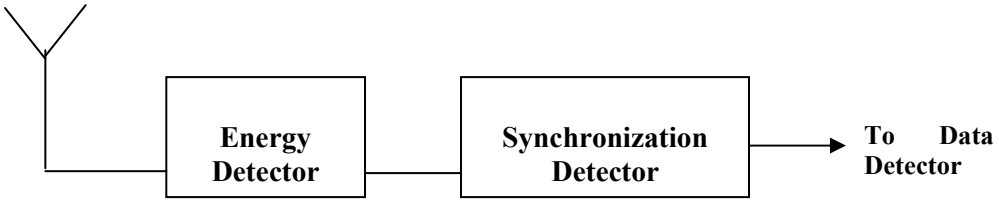


Figure 42: Non-MICS receiver at IMD device for wakeup mechanism

An example below shows where IMD locks on f_3 as it is found to be less interference channel. IMD's non-MICS energy detector, in order to conserve energy, duty cycles and therefore scans for wakeup signal only for a fraction of time as shown in the Figure 43.

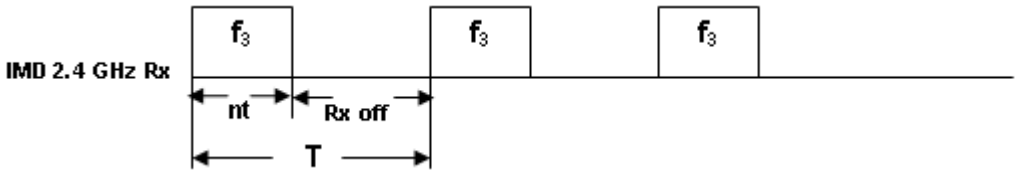


Figure 43: IMD non-MICS Rx energy detector duty cycle

Where t is time required 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.

Out of band (non-MICS band) wake up mechanism is proposed here. One of the non-MICS bands that can be used for wakeup mechanism is 2.4 GHz band (or 5.7 GHz as another 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.

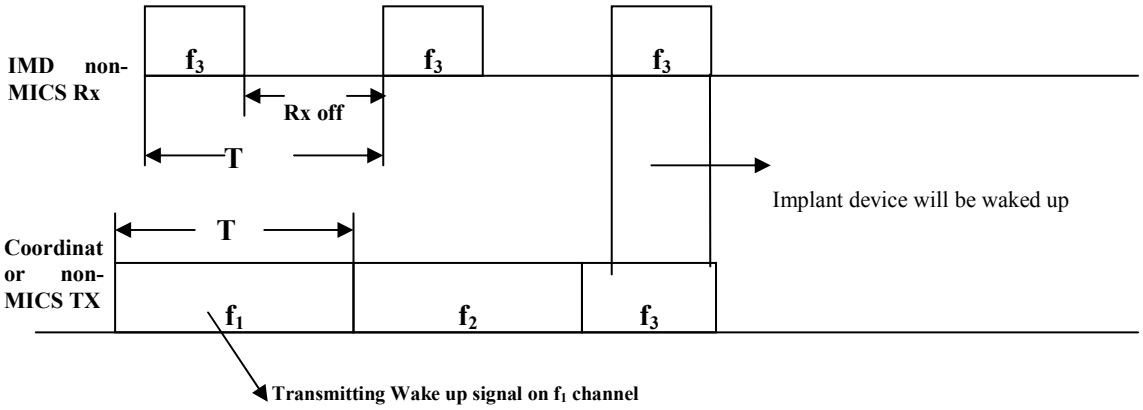


Figure 44: Wakeup mechanism for IMDs

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

6.4.1.2.1 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.

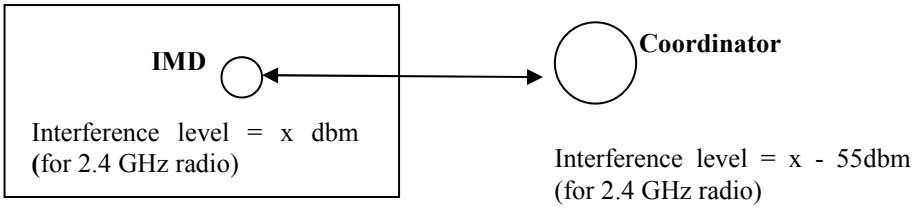


Figure 45: Different interference level for IMD and coordinator

6.4.1.2.2 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-radi o command is sufficient to allow IMD to transmit
- Method 2: When polling is required on MICS channel in order to allow a transmission

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

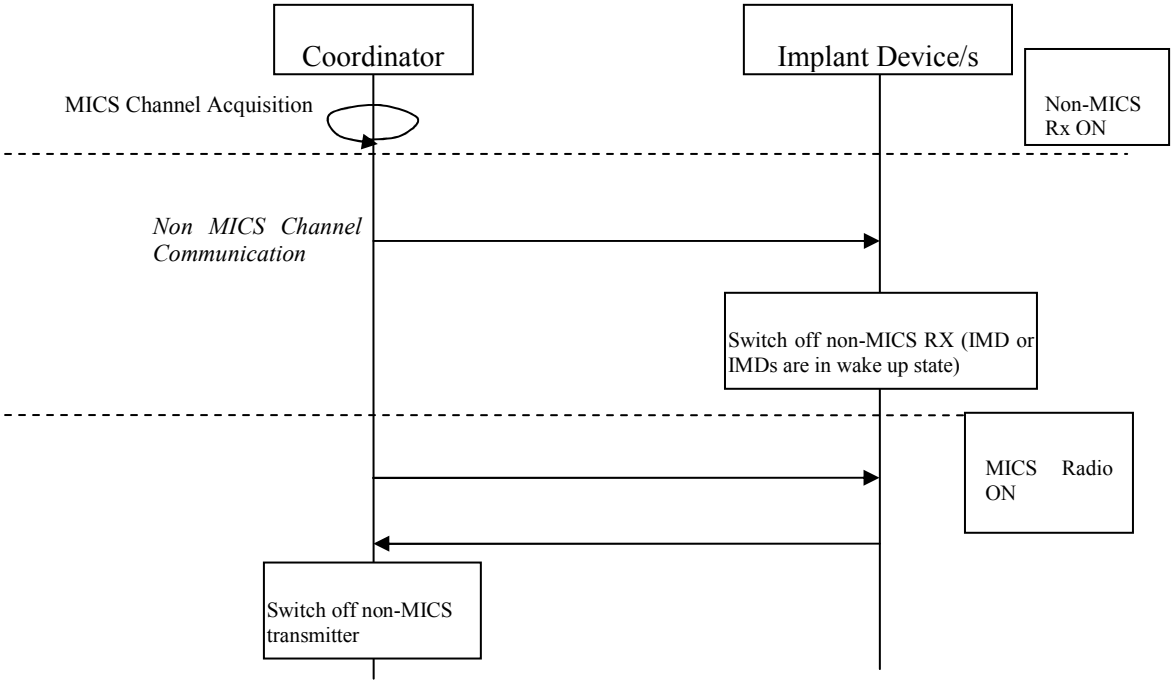


Figure 46: Wakeup process handshake

6.4.1.2.3 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 si ngle wakeup signal command.
- Wake up signal is sent to one IMD and then complete association with that IMD. After th is 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.

6.4.2 Emergency handling

Emergency handling is one of the most crucial requirements in any telemedicine systems. However, emergency messages have highly erratic nature; it has to be sent as soon as possible. The emergency data should not be delayed or denied due to dynamic availability of network resources. This section provides the detail of handling emergency events in implant communication. When the emergency occurs network may be operational (coordinator is busy with other nodes in data transfer) or non operational. When network is not operational the coordinator keeps only its detector ON instead of complete receiver circuit. For further power optimization duty cycling of energy detector is also allowed ensuring that the emergency messages can be detected with required reliability. There is no dedicated channel allocated to handle emergency data transmission. The coordinator always tries to duty cycle on channel with highest priority (the prioritization of channels is discussed later). The emergency situation can be detected either by implant device or by the coordinator and communicated to each other.

6.4.2.1 Emergency at device:

When emergency event detected at the implant device, the network and the event device (device with emergency message) may be in one of the following states.

6.4.2.1.1 Network is not operational

Network coordinator is inactive and not having data session with any implant device. This also implies that event device was inactive when the emergency event occurred at the device.

6.4.2.1.1.1 The sequence of operation performed by the device

1. Select the highest priority (the channel prioritization is set selected by the coordinator and communicated to the device at the time of association) channel for transmission of emergency alarm message by following the prioritization order.

2. Transmit ALARM messages in the selected channel to the coordinator to indicate the occurrence of an emergency event.

3. Wait for an acknowledgement from the coordinator after transmitting alarm messages.

4. If ACK message is received from the coordinator, follow the instruction of the coordinator conveyed through ACK message (e.g. wait for the next message from the coordinator or immediately send the emergency data).

5. No ACK received, repeat transmission of alarm messages for specified number of time till an acknowledgement is received from the coordinator in the selected channel.

6. If not a single acknowledgement is received from the coordinator in the previous channel, wait for random time and select a new channel following the prioritization order. Repeat steps 2 to 6 for the newly selected channel.

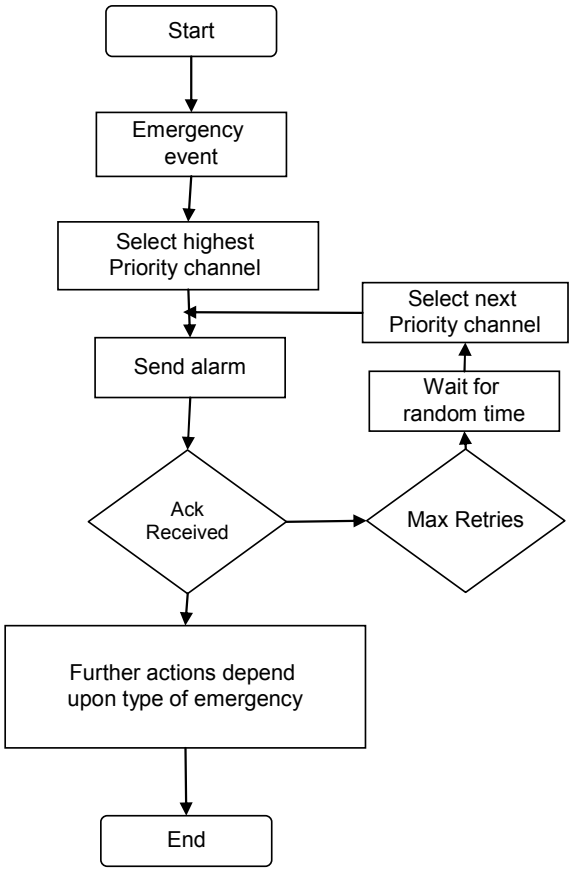


Figure 47 - Flow chart emergency handling at device: network non operational

6.4.2.1.1.2 The sequence of operation performed by coordinator

1. Duties cycling on highest priority interference-free channel to correctly receive the alarm message transmitted by the device.

2. If energy detected due to interference (primary or secondary), perform clear channel assessment/ listen before talk (LBT) to select the higher priority interference-free channel for duty cycling.

3. If emergency alarm message received, send acknowledgement to the sensor node and handle emergency. Coordinator shall resume the duty cycling on a higher priority interference-free channel after the completion of emergency data transfer.

4. If internal timer timed out, look for higher priority interference free channel (following the prioritization order) than the current channel and start duty cycling if available. Otherwise, continue duty cycling with the current channel.

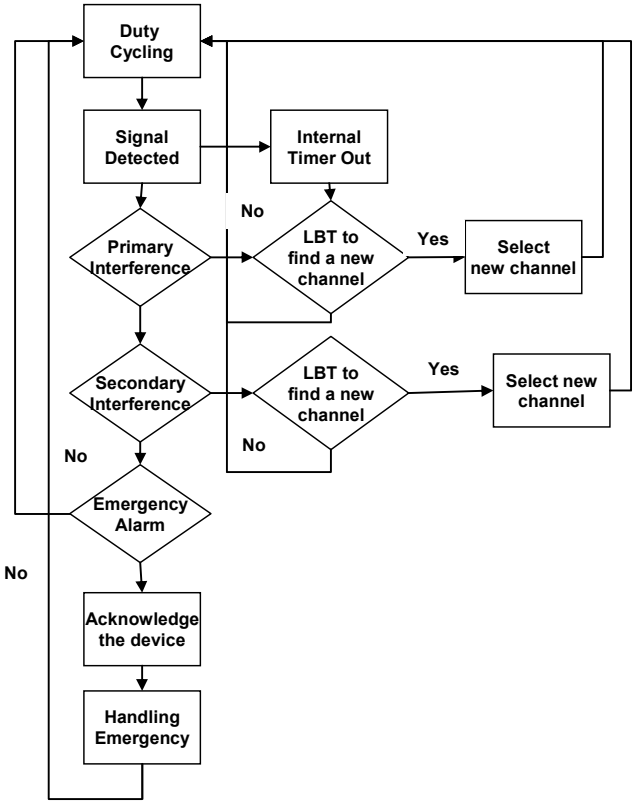


Figure 48 –Flow chart emergency handling at coordinator: network non operational

Figure 49 shows exemplary transmission of emergency alarm message by the implant device and reception of the same at the coordinator in case network is not operational.

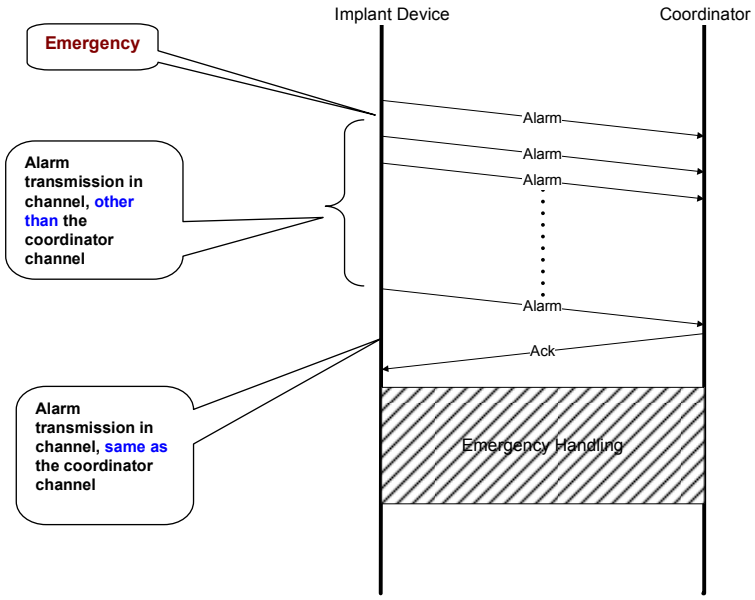


Figure 49 – Emergency Handling – Network non operational

6.4.2.1.2 Network is operational and device is non-operational

Network controller is active and running an active session with implant devices but not with event device. Event device was inactive when the emergency event occurred.

6.4.2.1.2.1 The sequence of operation performed by the device

Event device was inactive when emergency event occurred therefore it does not know the network status: operational or non operational. The sequence of operations performed by event device in case network in operational are same as when network is non operational.

6.4.2.1.2.2 The sequence of operation performed by coordinator

1. The superframe consist of busy and idle period

2. On occurrence of emergency event, the event device transmits multiple alarm messages to the controller. This may lead to two possible outcomes at the coordinator.

3. If the alarm message is transmitted during the idle period, the alarm message will be successfully received by the coordinator. The coordinator will acknowledge the event device and will handle the emergency data transfer from the event device.

4. If the alarm message is transmitted during the busy portion, the transmission of alarm message may collide with the packets transmitted during the data session.

5. The continuous transmission of alarm messages from the event device will collide with data packets and management packets causing forced collision which triggers an emergency notification event at the coordinator side

6. Upon the detection of emergency notification event, the coordinator suspends its normal operation and waits for the possible alarm message from the device.

7. If the coordinator receives any alarm message within a specific period of time it acknowledges back to the event device otherwise performs necessary actions as specified by the MAC protocol or resumes its normal operation.

Figure 50-Figure 51 shows exemplary transmission of emergency alarm message by the implant device and reception of the same at the coordinator in case network is operational and transmission of alarm messages at inactive and active portion of superframe respectively.

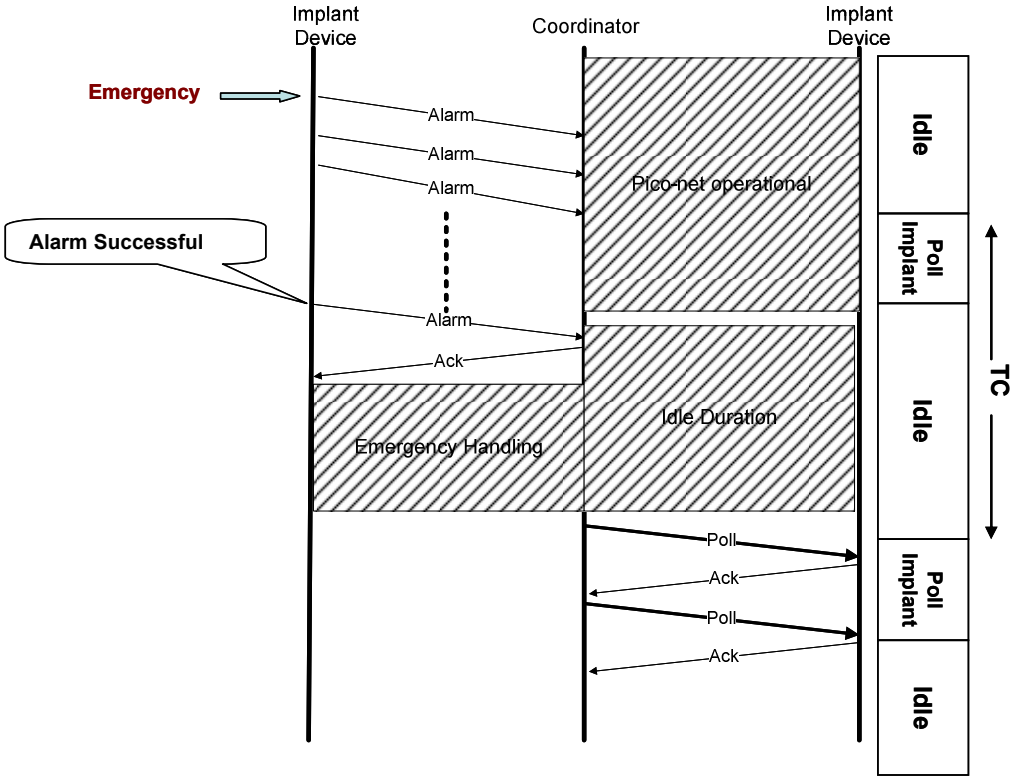


Figure 50 – Emergency Handling: Transmission of alarm message at inactive portion of superframe

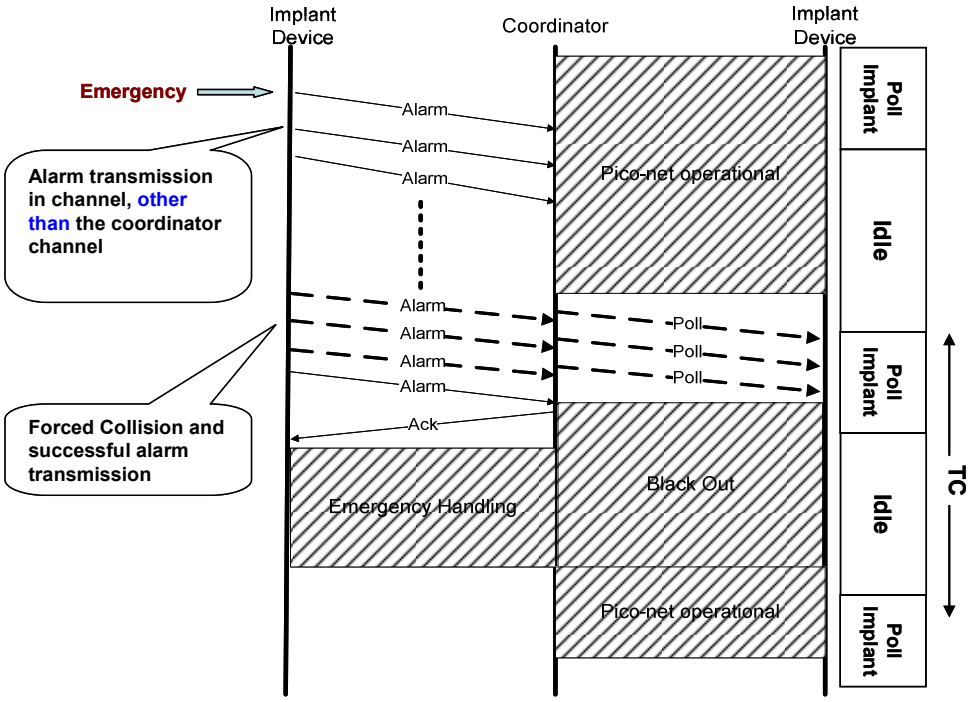


Figure 51 - – Emergency Handling: Transmission of alarm message at active portion of superframe

6.4.2.1.3 Network is operational and device is operational:

Network controller is active and event device is part of the access schedule. In this case device can either use its allocated channel time to transmit the data, inactive period of superframe or it can use forced collision as described in the previous section to transmit alarm messages in the active period of superframe. The coordinator operation is similar to the previous section.

6.4.2.2 Emergency at coordinator

Sometimes it may be required for a coordinator to change some parameters of the implant device due to either emergency detected at some other implant device or at coordinator itself. In this case coordinator can use wakeup the device first using wakeup mechanism detailed in previous section if device is sleeping or use allocated time interval to convey the emergency event by sending POLL message with data as payload.

6.5 Single MAC for Multiple PHY

Sometimes implant medical applications may coexist with on-body medical applications. In other words, a single external coordinator may be capable of communicating with implant as well as on body devices through dual PHY interfaces. In this case the MAC has to support implant and on body communication simultaneously in a transparent manner. To support simultaneous operation of multiple PHY, the MAC uses time sharing between two PHYs. The Figure 52 shows the time partitioning between implant and on body to support both the application simultaneously. The implant devices are given higher priority than the on body device. The on body device utilize the idle period of implant frame cycle.

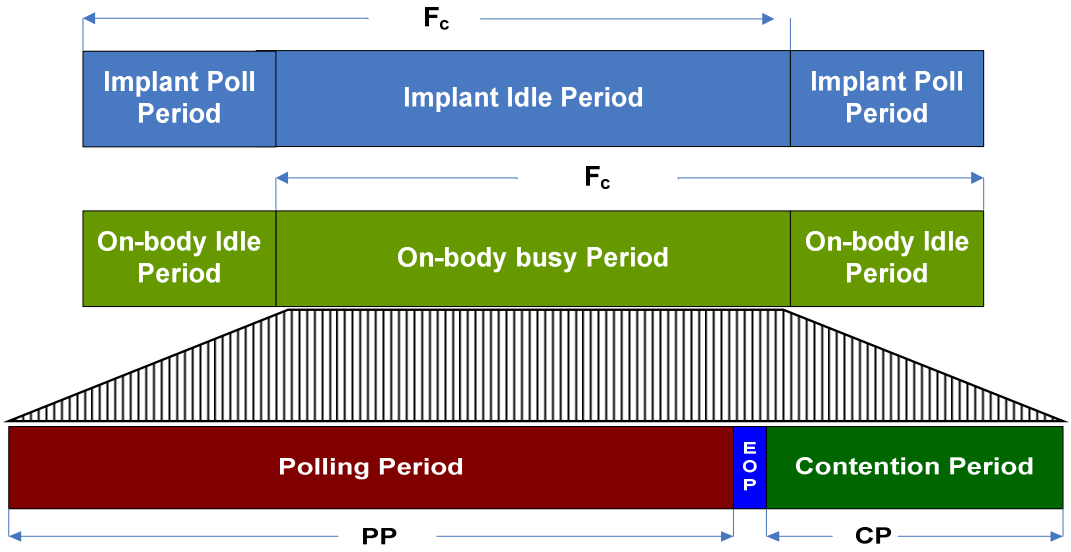


Figure 52 – Time sharing between implant and on –body PHY

7 Network Management

7.1 Device Association and Disassociation

This section contains association process for implant and on-body devices.

7.1.1 Piconet join process for Implant applications

The diagram below shows message exchanges for piconet joining procedure.

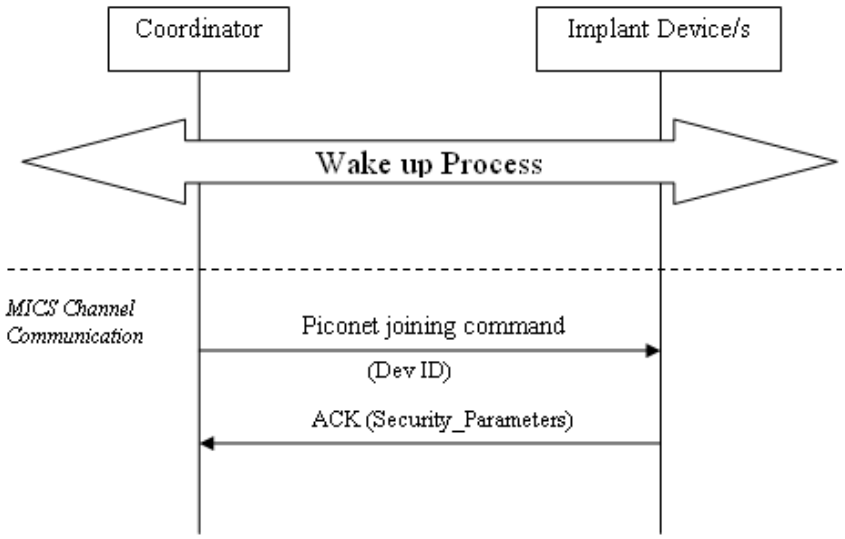


Figure 53 - : Piconet joining handshakes

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

Piconet joining command would be followed by ACK from IMD device, thereby completing pico net joining procedure. Piconet joining can be part of wakeup mechanism.

7.1.2 Piconet join process for on-body applications

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

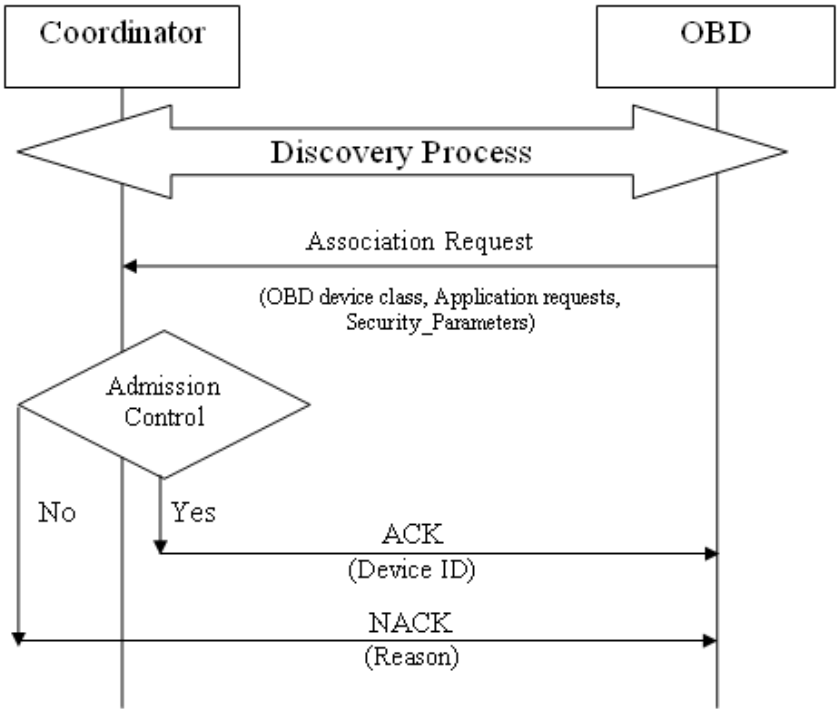


Figure 54 - Message sequence for Piconet join process

An OBD sends piconet joining request to discovered coordinator which contains following param eters 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 (A CK) in response to piconet join request. ACK response will contain Device ID for the piconet. Fo r 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.

7.1.3 Group Association

There are applications in Body Area Network like EEG, ECG, EMG, and Gaming etc which com prises 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 effici ent 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 f rom 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 in formation (it could be representative node's IEEE MAC address).
4. The representative device is responsible for network joining, that is, associating to a coor dinator.

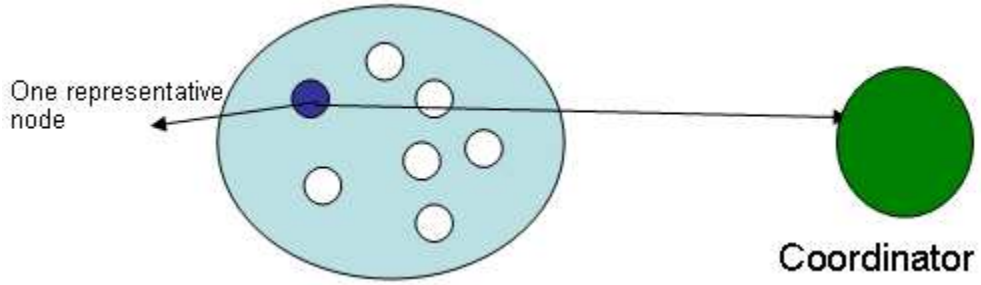


Figure 55 - A group application is represented by one node for association and disassociation process

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 equivale nt 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 p ools 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 adde d to EOP message.
10. All the device of a group application should keep on scanning for EOP message which co ntains 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 i ts 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 shoul d start listening for its poll message and enter to polling cycle.
13. A coordinator can remove the pool information along with representative information fro m its EOP message, when all the devices start responding to their respective poll comman

ds.

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 devi ce ID pool and representative information. The respective device can also be freed.

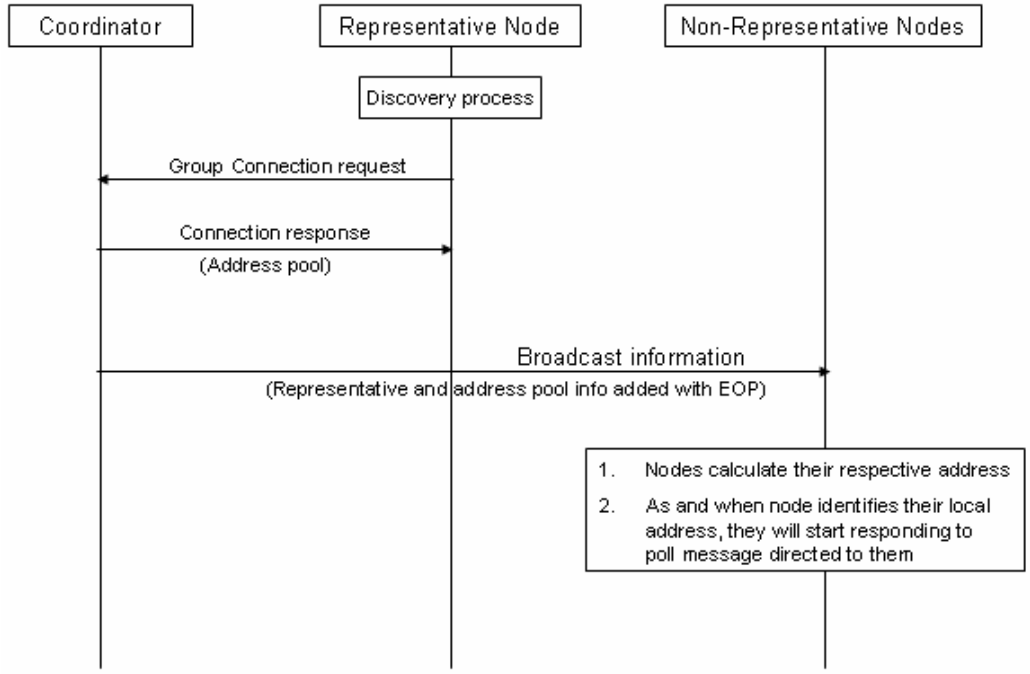


Figure 56 - Message sequence for group association

Multiple representatives

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

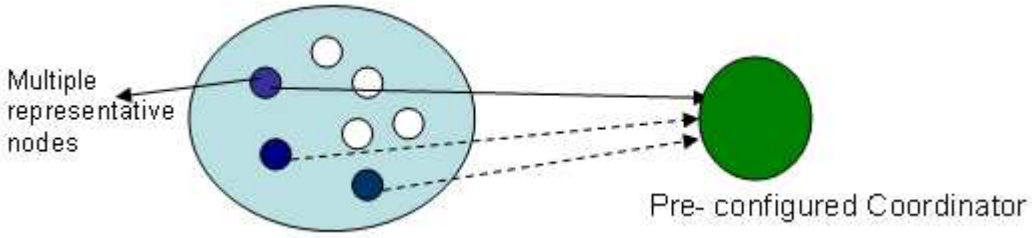


Figure 57 - A group application is represented by multiple nodes for association and disassociation process

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 privat e 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 succee ds 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.

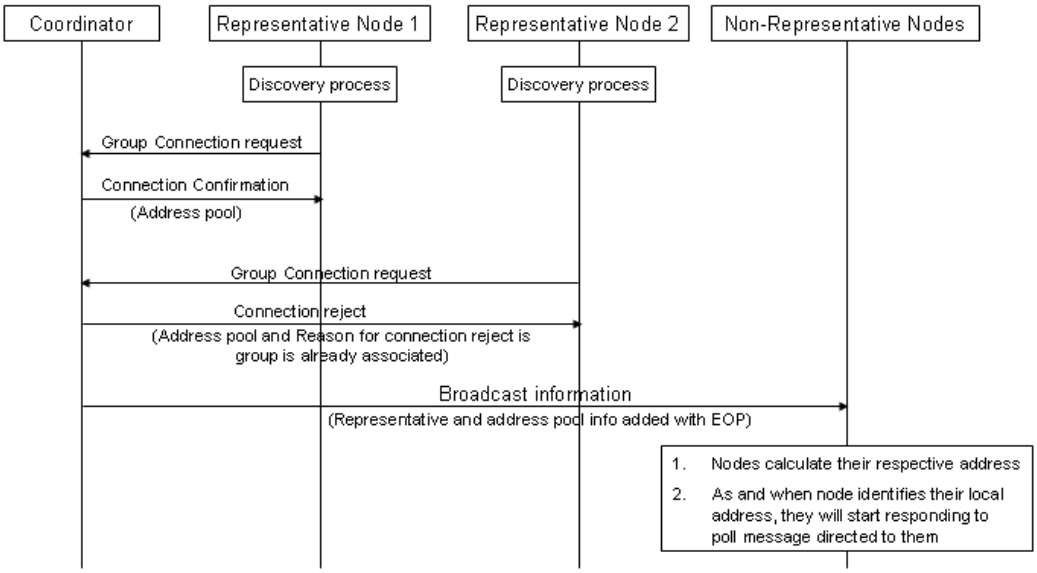


Figure 58 - Message sequence for group association when there are multiple representatives

7.2 Network Coexistence

As per IEEE technical requirement for Body Area Network (BAN), at least 10 networks should be able to coexist within a limited 6X6X6 meter cubic space. There are multiple ways to solve the coexistence problem: Dynamic frequency selection, collision avoidance and bandwidth sharing among the networks. Sometimes it may be possible the no channel is available due to the presence of other BAN networks or other technology network. It becomes necessary for two or more BAN networks coexist in a single channel in time shared basis. The flow chart

Figure 79 shows the sequence of operations performed by a coordinator of a network to coexist with the other networks when it starts as well as while running. The provided solution covers different scenarios of BAN with respect to mobility model of BAN nodes.

- **Static:** No topological changes for long duration. The BAN nodes move from one place to other very infrequently. Bed side patient monitoring is one of the BAN example of this category. The coordinator is situated out side of the body. This restricts movement of body within a range of 3 m.

- **Semi Dynamic:** Infrequent topological changes. Random way point mobility model with large considerably moderate duration of stay in a station between two movements. Multiple BANS in an elevator could be the example of this category. This is the example of dense network when all network coordinators are within each others communication

range. A waiting hall. This is the example of non dense network of this category when all network coordinators may not be within each others communication range.

- **Highly Dynamic:** frequent topological changes. Random way point mobility model with very short duration of stay in a station between two movements. BAN inside vehicles.

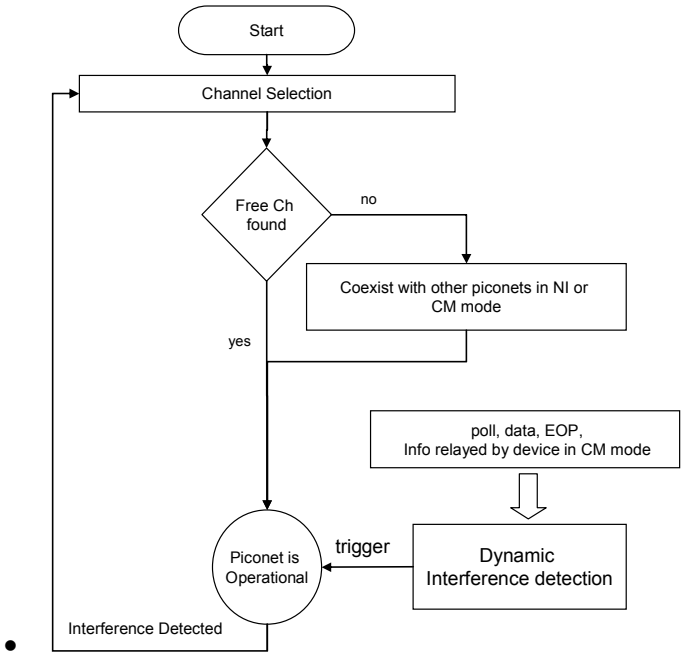


Figure 59 – Flow chart for coexistence

7.2.1 On-body co-existence

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.

7.2.1.1 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 or independent decisions for the time resource (option 1) or by using an offset Piconet synchronization method (option 2). These options are discussed in more details later. This mode is useful for static and semi dynamic scenarios.

7.2.1.2 Coexistence interference mitigation (CM) 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. This mode is useful for dynamic scenario.

The Figure 60 shows the flow chart to decide different modes of coexistence when the coordinator starts a network.

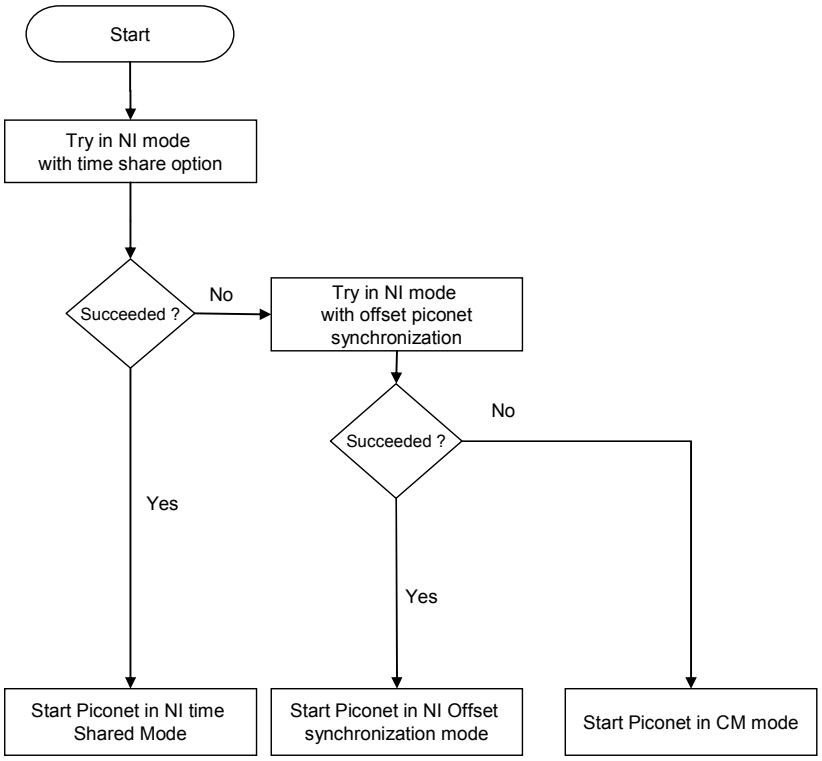


Figure 60 – The selection of different mode of coexistence

7.2.1.3 Channel description:

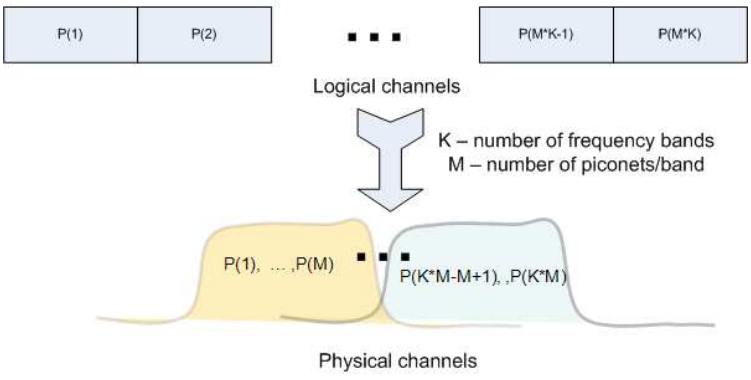


Figure 61: Logical to Physical Channel mapping

Figure 62 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.

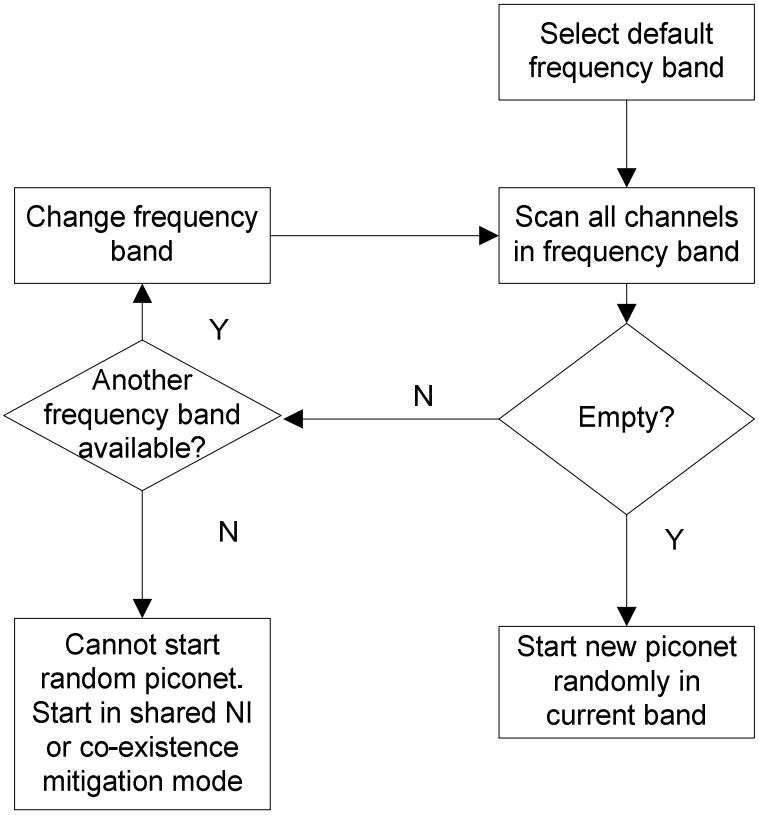


Figure 62: Piconet formation (Listen before talk)

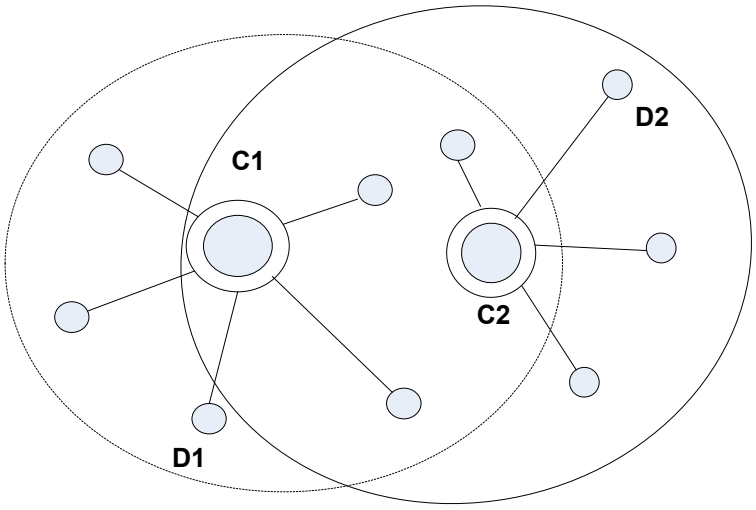


Figure 63: C1-C2 can/will talk to each other

Figure 63 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 64 shows the sequence of operations between C1 and C2 in the time resource sharing NI mode and Figure 65 shows the method to achieve the message exchange in a superframe using contention based access.

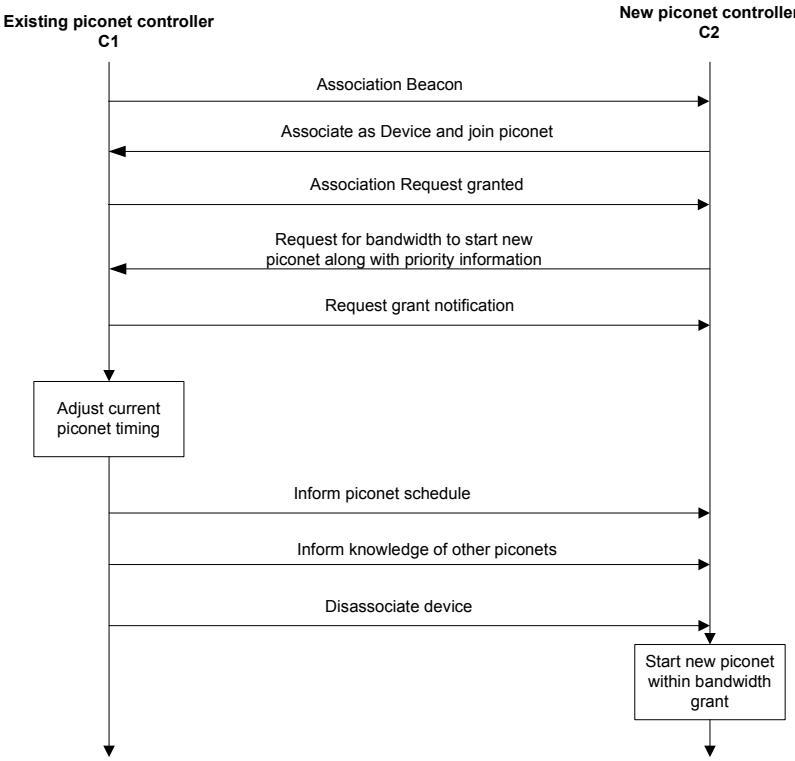


Figure 64: NI time resource sharing mode

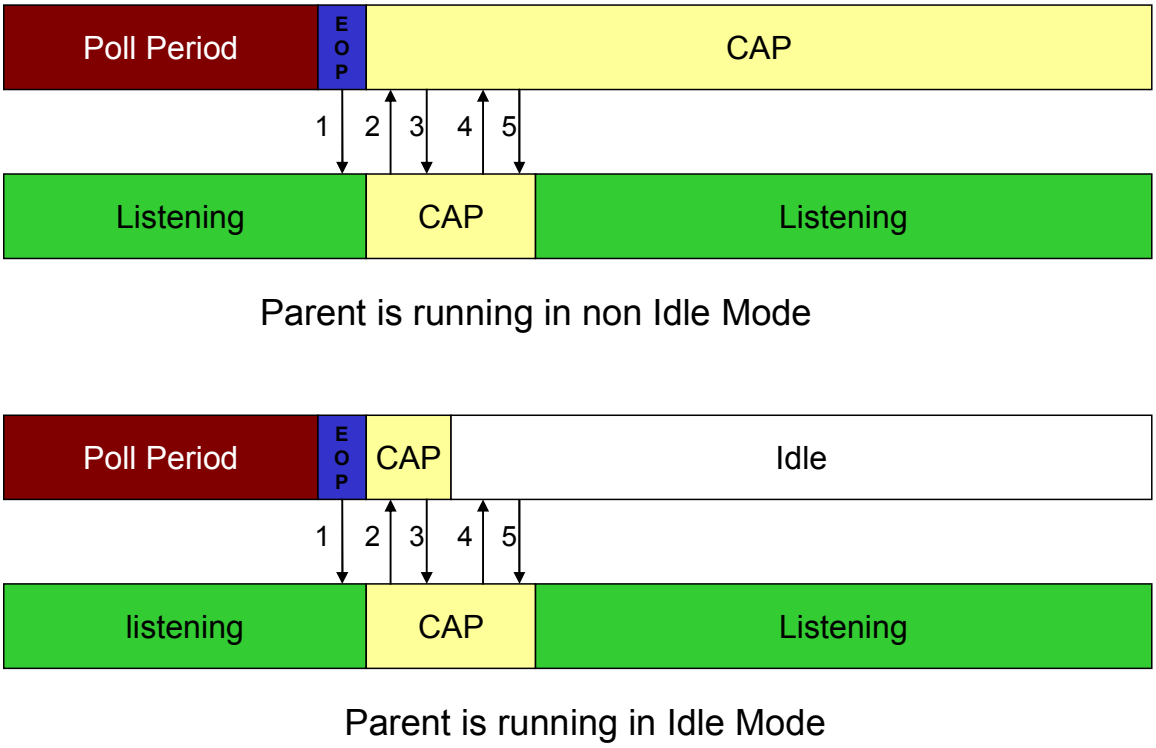


Figure 65 – Transmission of message for coexistence in NI mode

Figure 66 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.

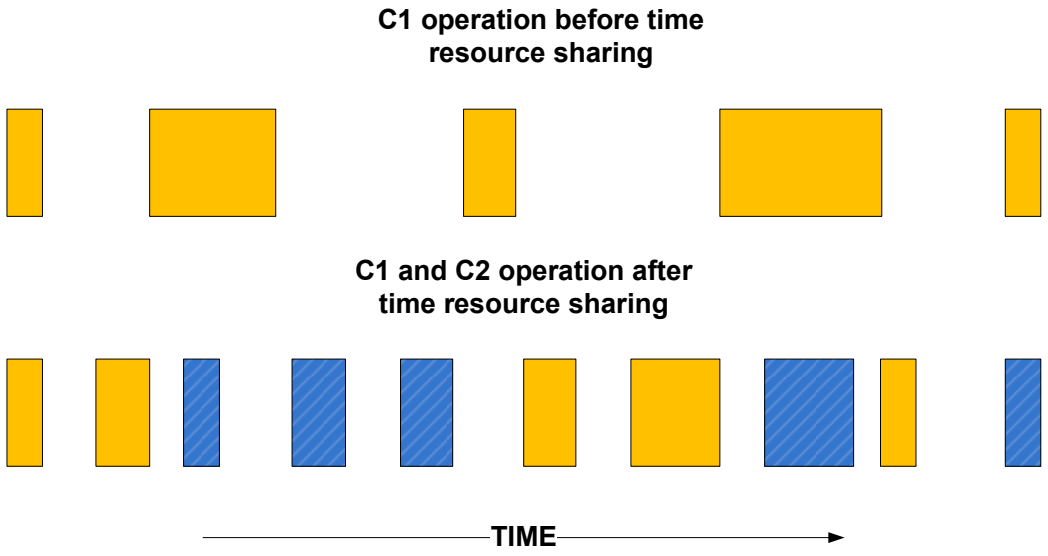


Figure 66: NI time resource sharing mode timing

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 67. 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.

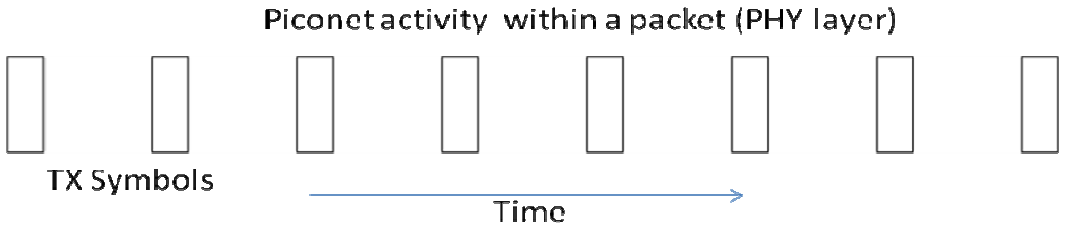


Figure 67: Tx activity within a packet in PHY mode with low duty cycle

The sequence of communication between C1 and C2 is shown in Figure 68. 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.

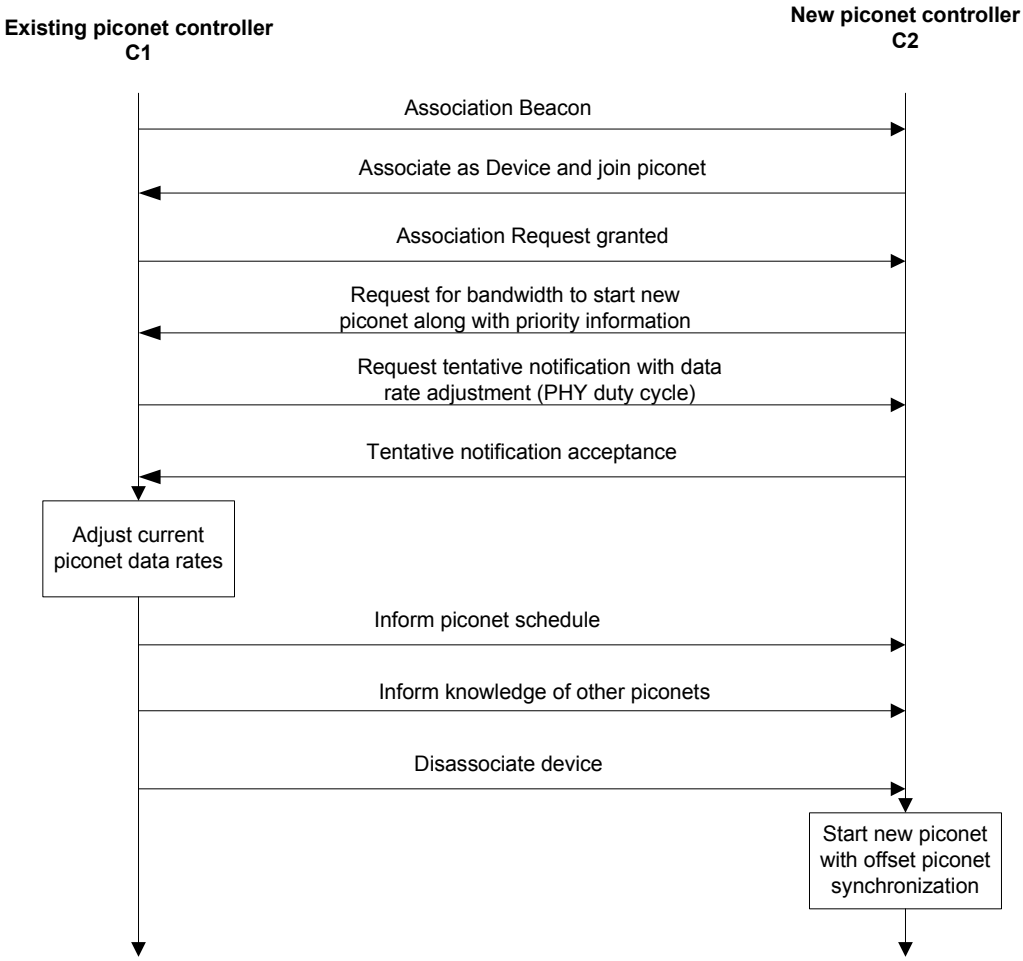


Figure 68: NI offset piconet synchronization

Figure 68 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 70.

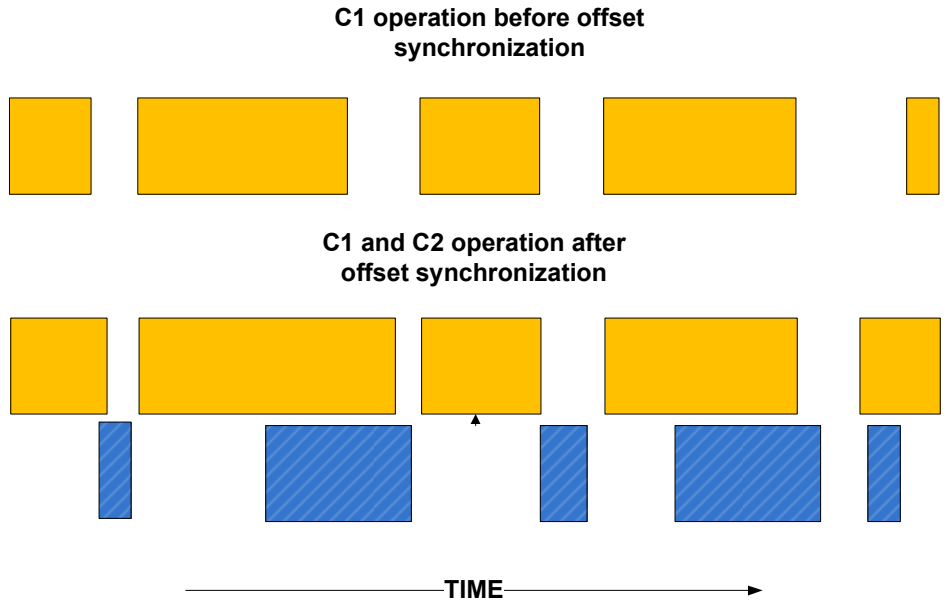


Figure 69: Offset Piconet synchronization frame level

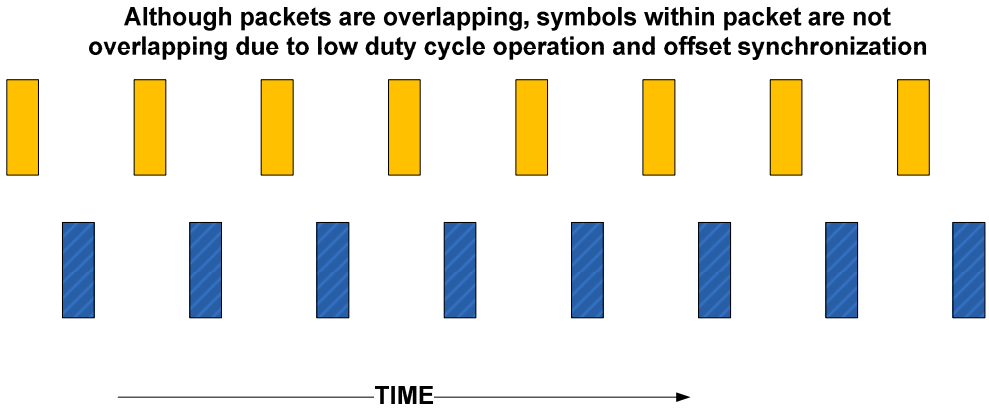


Figure 70: Offset Piconet synchronization (symbol level)

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 69 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.

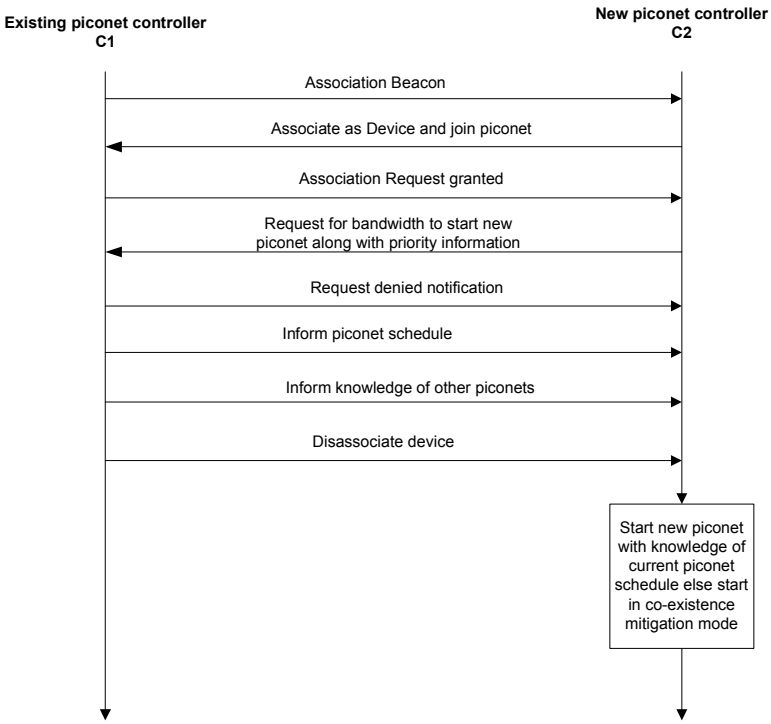


Figure 71: Denied time resource mode

Figure 72 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.

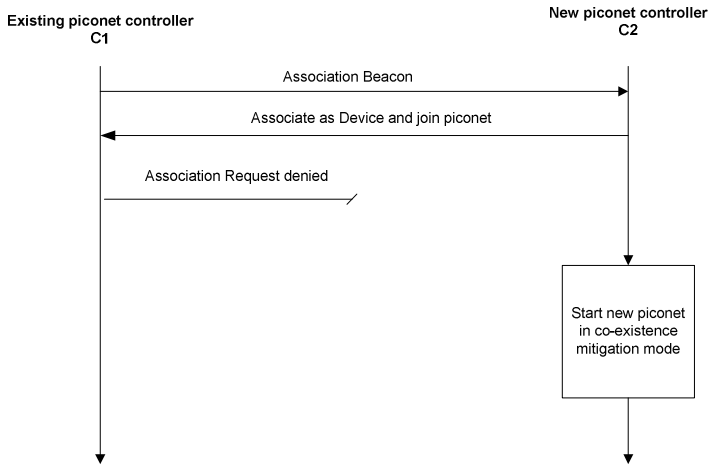


Figure 72: Denied Association mode

Coexistence 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 73 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.

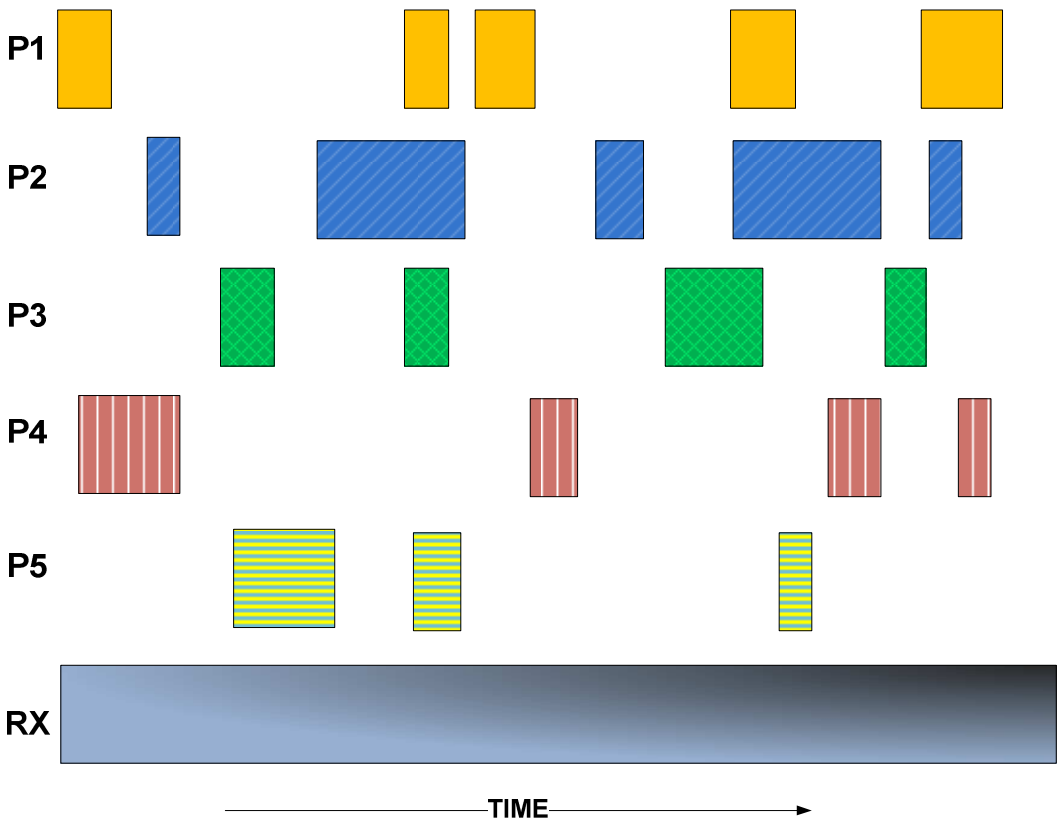


Figure 73: Co-existence of 5 simultaneously operating Piconets in CM mode

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

TBD 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:

- **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.

- **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
- **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.
- **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 74.

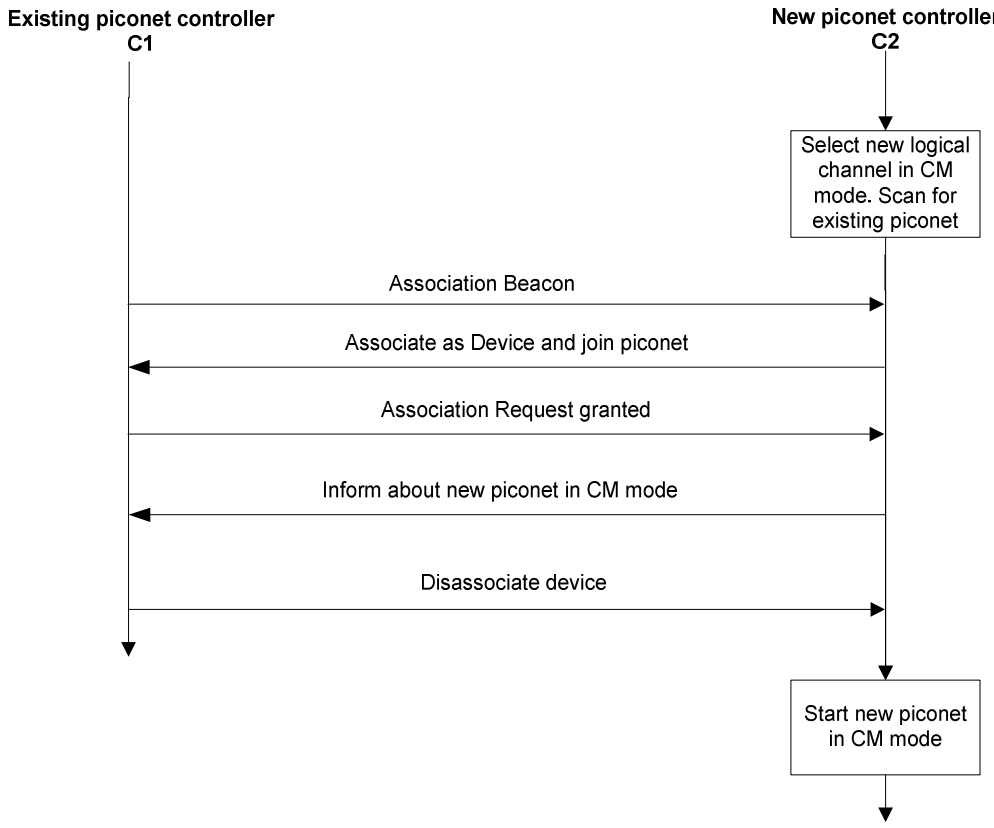


Figure 74: Notification in CM mode

7.2.1.4 Occasional collision detection and avoidance during slot allocation

If there is a case for piconet coordinators not to be able to talk each other, exchanging information for piconet coexistence is difficult. When two piconets get close and slot allocation of each piconet is serviced, there may be a possibility of collision between coexistence related message and data slots. So we propose a collision avoidance method by collision detection. Collision detection may be channel sensing or serial packet error detection. In case 1 of fig. 75, proposed resloving process is described by channel sensing at the start of active frame duration. If piconet 2 coordinator senses interference, it stops beaconing or polling and waits advertise message from neighbor piconet 2 coordinator. Piconet 2 coordinator receives advertise message, and reply its own advertise message by broadcasting. Then Piconet 1 coordinator receives advertise message from piconet 2 coordinator. There is time offset information and timing information of slot allocation in advertise message to avoid next expected collision.

If Piconet 1 sends advertise message intermittently, Piconet 2 may not receives the expected message. So, Piconet 2 sends advertise message instantly with no more waiting when no advertise message has been received during the specific duration after energy of receiver had gone down.

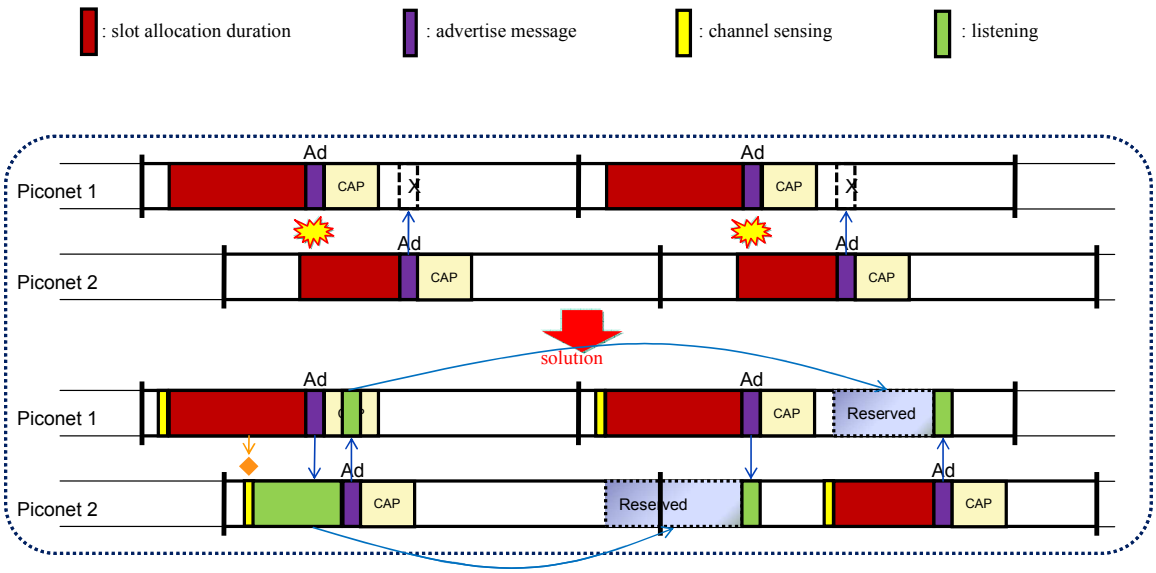


Figure 75 - piconet collision case 1 when two piconets get close

In Case2 of Figure 76, operation is nearly same as case 1 except channel sensing is performed at the end of active frame duration. This is designed to guard CAP from collision. Consequently, channel sensing or collision detection at the start of active frame or at the end of active frame helps detect piconet collision, and piconet coordinator exchanges coexistence related information by advertise message. And then piconet collision can be avoided.

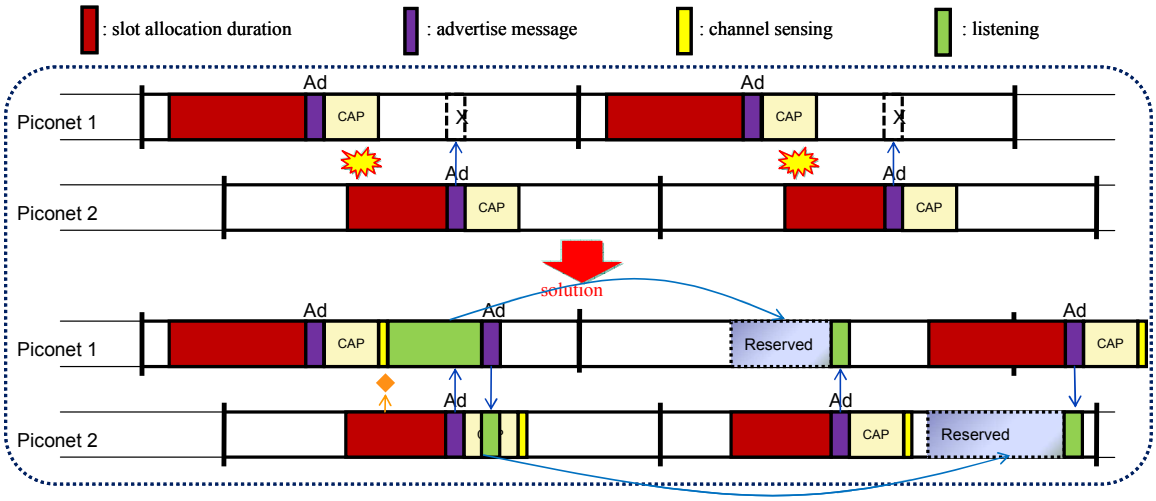
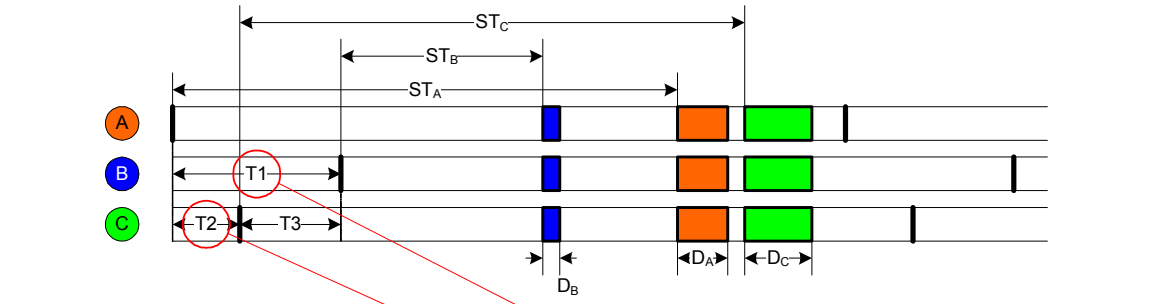


Figure 76 - piconet collision case 2 when two piconets get close



TDMA Schedule Advertisement Message

Addr	# hop	Slot Start	Slot Dur	Seqno

TDMA schedule Table A

Addr	# hop	Offset	Slot Start	Slot Dur	Seqno
A	0	0	ST_A	D_A	SN_A
B	1	T1	ST_B + T1	D_B	SN_B
C	1	T2	ST_C + T2	D_C	SN_C

TDMA schedule Table B

Addr	# hop	Offset	Slot Start	Slot Dur	Seqno
A	1	? T1	ST_A ? T1	D_A	SN_A
B	0	0	ST_B	D_B	SN_B
C	1	? T3	ST_C ? T3	D_C	SN_C

TDMA schedule Table C

Addr	# hop	Offset	Slot Start	Slot Dur	Seqno
A	1	? T2	ST_A ? T2	D_A	SN_A
B	1	T3	ST_B + T3	D_B	SN_B
C	0	0	ST_C	D_C	SN_C

Figure 77 - time offset calculation

When this process is done once, piconet coordinator can know timing of next advertisement message in advance by information such as time offset between transmission time difference of advertise messages. Figure 78 shows this process is available when polling access is used and EOP or advertise message slides. Time offset calculation and knowing process for slot duration of neighboring piconet is described in Figure 77.

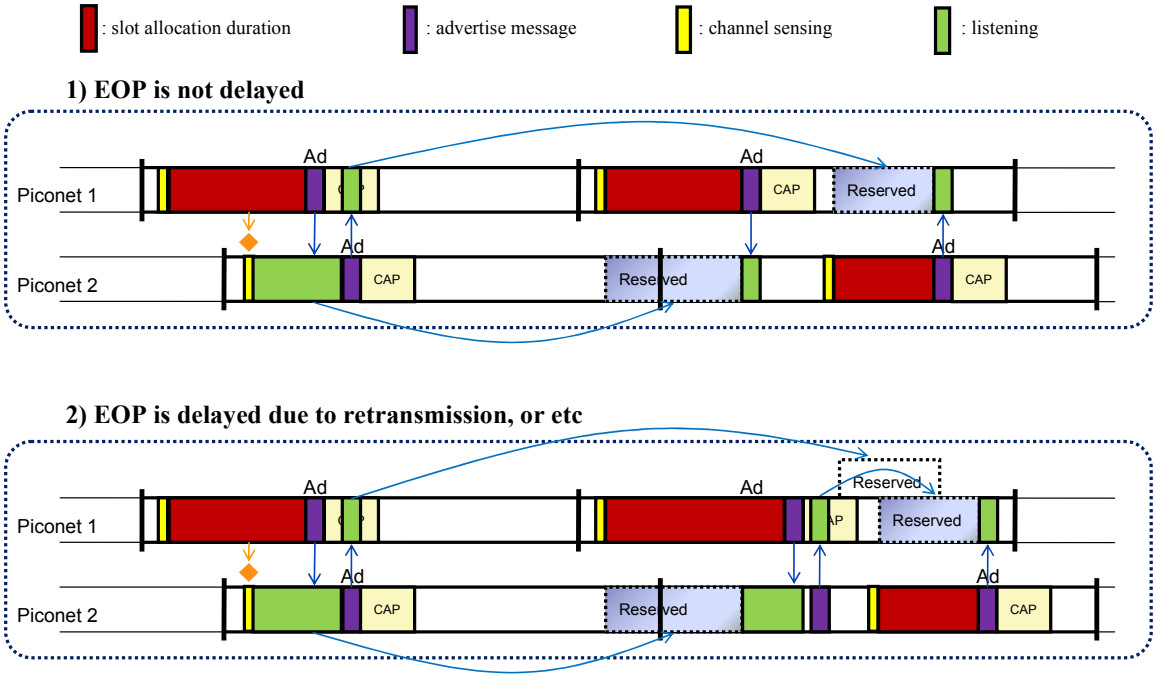


Figure 78 - piconet collision case 1 when two piconets get close

7.2.2 Implant co-existence

This section details the mechanism to support coexistence of multiple piconets in the same channel. Efficiency of proposed mechanism depends upon topological changes and per piconet load. Following are the operations performed by an external controller to start a piconet and try to coexist with other networks. The flow chart of the protocol is shown in

Figure 79.

- Select a channel
- Perform Listen Before Talk (LBT) for the time as specified by FCC rules
- If the channel is found busy, select another channel and repeat the operation otherwise send an enquiry message to confirm the presence of another piconet.
- If no response received, start the piconet on the selected channel otherwise select a new channel.
- If all channels are exhausted and no free channel is available try to coexist with other existing piconets.

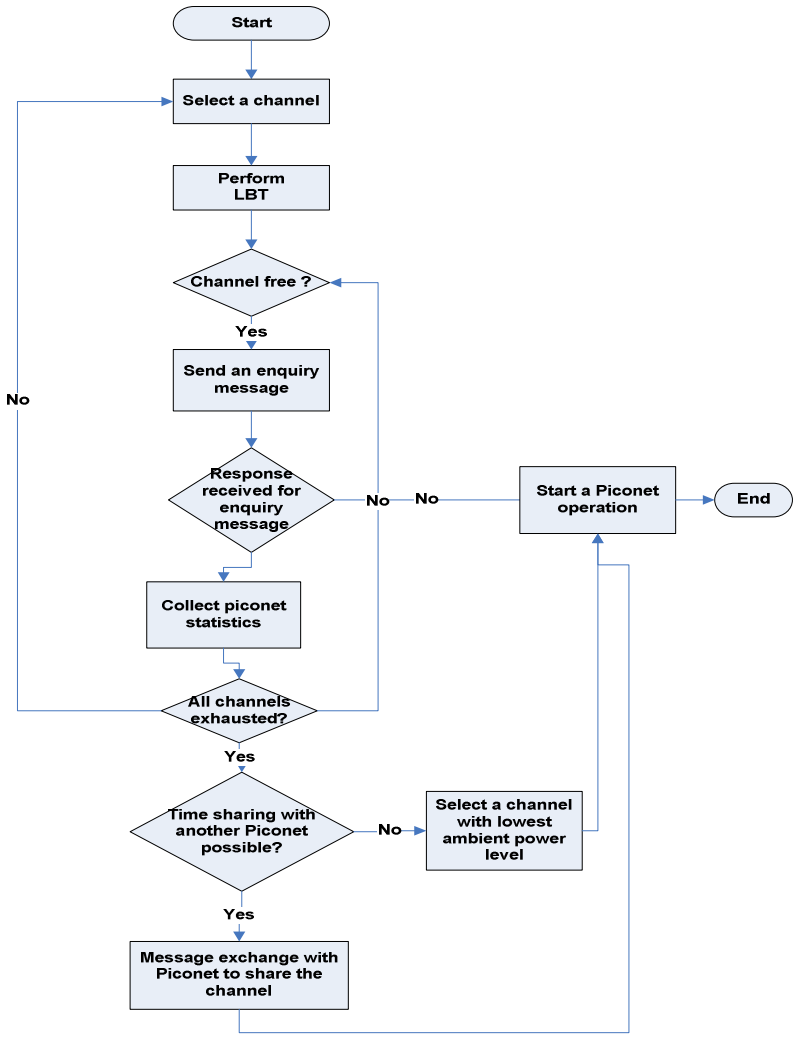


Figure 79 – flow diagram for implant coexistence

8 Security

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

8.1 Security Parameters

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 proposed security method is a highly flexible method for choosing multiple levels of security protection. A control field called **Security_Control_field** is exchanged between the BAN devices. 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, many of the BAN device communication typically consisting of short sessions, such devices can choose to have the same security level all the data and control exchange in a session. However, flexible security mechanisms are provided such that other applications that have large data transfer in long sessions can select the security level on a per frame basis.

Security level is represented in the Security Control field using one byte bitmap. Each bit is used to indicate the support of the security features as follows:

I. Bit 0 – Authentication
II. Bit 1 – Integrity protection
III. Bit 2 – Encryption/Decryption
IV. Bit 3 – Replay protection using frame counters
V. Bits 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 in a single byte field, that carries a hex value indicating the security algorithm that will be used by the security mechanism. Only standard security algorithms will be used. Proprietary security algorithms will not identified using this field. The algorithm used for the security mechanism can also mentioned as a parameter that is exchanged along with the Security_Control_Field. Default Algorithm used is - AES.

The client device submits the security parameters to the BAN coordinator during association. If the security support indicated by the client are acceptable to the coordinator then it can proceed with the network join procedure or the coordinator can fail the association of the device with a negative acknowledgement.

The following capabilities are expected in a coordinator and BAN device (client) for implementation of the security mechanism.

1. A coordinator would be preconfigured with following details
    - The minimum Security mode that a coordinator expects a BAN devices to suppor t.
    - A Security Table is stored in non-volatile memory of coordinator consisting of t he following fields
        - Shared keys for each client device (multiple keys identified by an identif

ier, called Master Key ID- MKID)

- Type of device/Service provided by the clients

2. A BAN device would also be preconfigured with security keys and the corresponding M KID as in the coordinator.
3. A device (client) and coordinator should have the capability to store temporal keys and fr ame counters until the keys are renegotiated in a later session.

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 saved at the coordinator and client. A subsequent session can choose to continue counting from the frame counter stored from the previous session or restart with a new random frame counter.

8.2 Authentication Procedure

After a BAN device successfully joins the piconet, if authentication is supported, the coordinator initiates the authentication procedure. Authentication uses a 4-way handshake procedure which validate that the peer device shares the same master key.

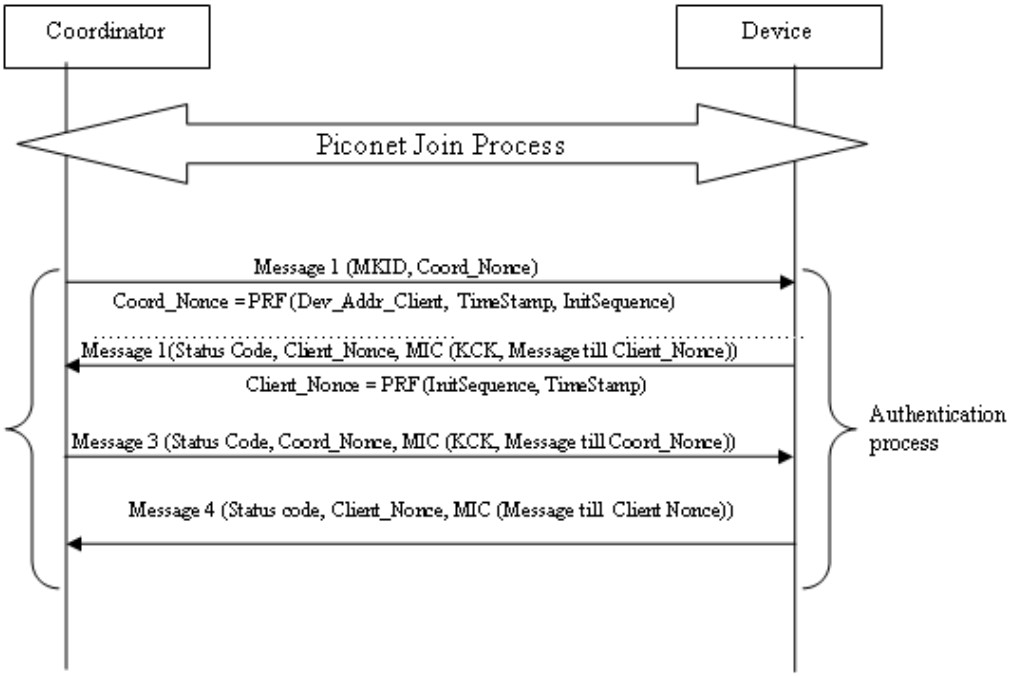


Figure 80 - Message sequence for Authentication process

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 du ring the previous session will be used.
- After, authentication and identifying a new set of temporal keys , Freshness or replay prot ection counter is reset to 0.

8.2.1 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.

8.2.2 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.

8.2.3 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 in stalled by out of band mechanism not covered in this protocol.
- After association, only the representative node does the authentication procedure (as expl ained in section 7.2.3).
- The coordinator and the representative node will broadcast the Master Key Id, Coord-No nce and Client-nonce(chosen by the representative node) used for the key generation in th e 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, r esponse sequence to verify that the devices have the same keys and then data communicat ion begins.
- This common key can be used for broadcast or group communication also. A coordinator can send a broadcast message secured using this group key.
- However, if there is a unique requirement in the application for each group device to gene rate a unique key, then the device Client-Nonce can be appended with the Device_ID to g enerate different keys for each device. The coordinator has the task of generating an inde pendent key for each device of the group.

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 can be selectively used in the frames that are sent from the BAN device and the coordinator. Standard frames like (poll or other control frames) sent from the coordinator need not be encrypted or integrity protected. Since, this could make brute force attack possible, since the format and size of the control frames are small and with predictable values.

8.3 MAC frame format for Secure Frames

The security header field is the key field that indicates the security selection. This is the key field that indicates which of the following fields will be present in any secure frame.

This field is to be coded as a bitmap indicating the following values:

All bits 0 0x00 – No security feature is used for this frame

Bit 0 – set to 1 indicates Encryption and Decryption is used

Bit 1 – set to 1 indicates Partial frame Encryption and Decryption is used, ie. The Encryption Offset field is present

Bit 2 – set to 1 indicates replay protection is used.

Bit 3 – set to 1 indicates Integrity protection is used.

Bit 4 – 32 bit keys are used

Bit 5 – 64 bit keys are used

Bit 6 – 128 bit keys are used

Bit 7 - RFU

1 byte	2 bytes	1 byte	N bytes	4 bytes
Security Header	Encryption Offset	Security replay counter	Secure Payload	MIC

Figure 81 - The Security Header and payload for secure frame

8.4 Upper layer interface to support the Security for Frames

The choice of the security header field in the above figure is to be driven the application or the characteristic of the BAN device and the services provided by the device at this session. A preset table listing the BAN services, devices and their respective security needs can be maintained either in the BAN

or the logical link control layer above the MAC that can automatically set the values for the security header field based on certain inputs from the application. This is important to guide per frame security support.

9 Appendix A: IEEE 802.15 TG6 MAC Technical Requirements

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

10 Appendix B: BAN traffic type and requirements

The Table 2 demonstrates the categorization of various BAN traffic types and the recommended channel access mechanism to can be used to achieve their power and Quality of Service (QoS) requirements.

Table 2 – Traffic types and their recommended channel access

Class	Description	Performance Requirements	Example	Recommended Channel access
T_1	CBR low data rate traffic	• Highly power constraint devices • Packet delay • Support of large number of devices	• Patient Monitoring • ECG • Fitness Applications • Interactive Gaming	Scheduled polling
T_2	CBR high data rate traffic	• power constraint but less than T1 • Packet delay	• EMG • Un compressed audio	Scheduled, Delayed polling
T_2	VBR traffic	• Delay and Packet Delay Variation • Optimized bandwidth utilization • Power efficiency is optional	• Real time multimedia streaming	Unscheduled polling

11 Appendix B: Simulation Results

The simulations have been performed in C++ framework for different application scenarios to evaluate the performance of channel access mechanism with respect to following metrics.

Delay: Queuing delay + Channel access delay + Transmission delay

Power consumption: Total power consumption in term of time spent by radio at different states (transmitting, receiving, idle)

Packet delay variation: Deviation to the reference value. Mean packet delay is taken as reference value.

11.1 Simulation 1: Application class T1

Table 3 – Application specific details for T1 simulation

Application	**Arrival rate/devices**	**Number of devices**	**Allocated slot time (S_i) per device (ms)**
ECG	4 Kbps	20	0.582
Vital Signal Monitoring	4 Kbps	20	0.582
EEG	8 Kbps	20	0.164
Interactive Gaming	4 Kbps	40	0.582
Fitness	4 Kbps	20	0.582

Table 4 – Global simulation parameters for T1 simulation

Simulation Run	100 sec
Data rate	1.5 Mbps
PER @256 Bytes	10 %
Total load	560 kbps
Frame cycle	115 ms
IFS	15 µs
Poll size	15 bytes
ACK size	15 bytes

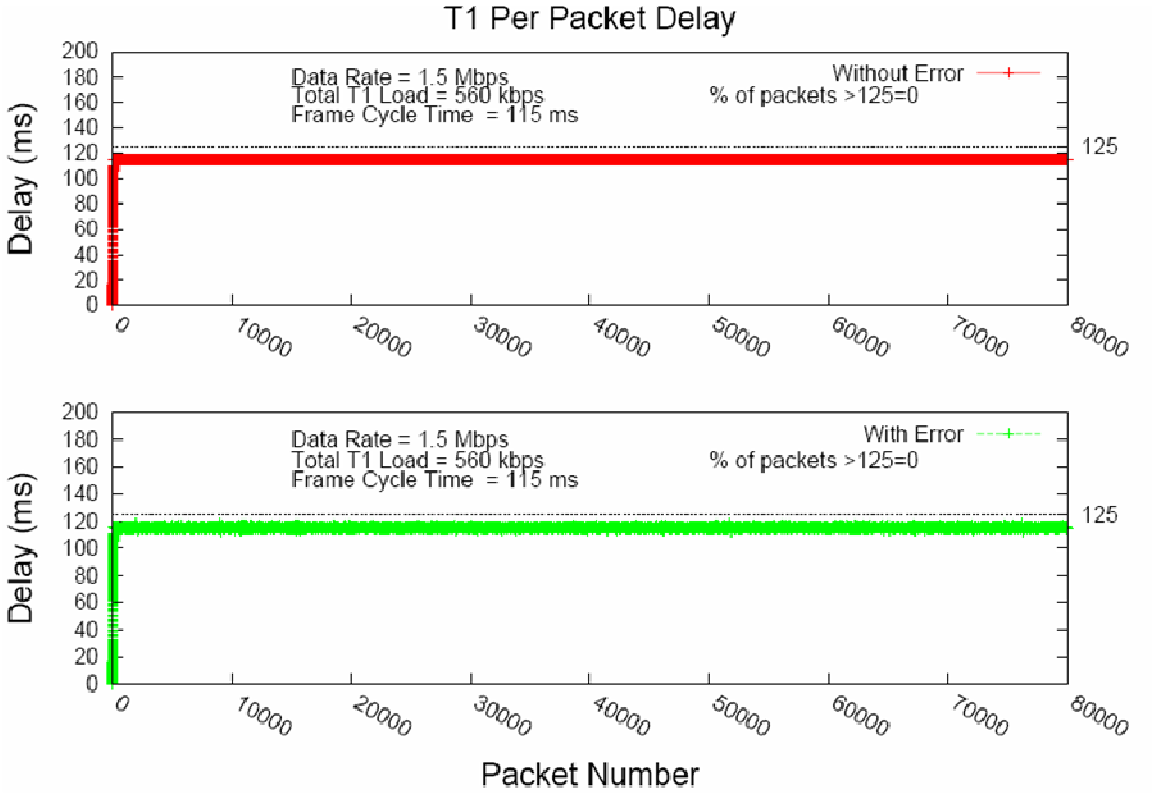


Figure 82 - Delay results for T1

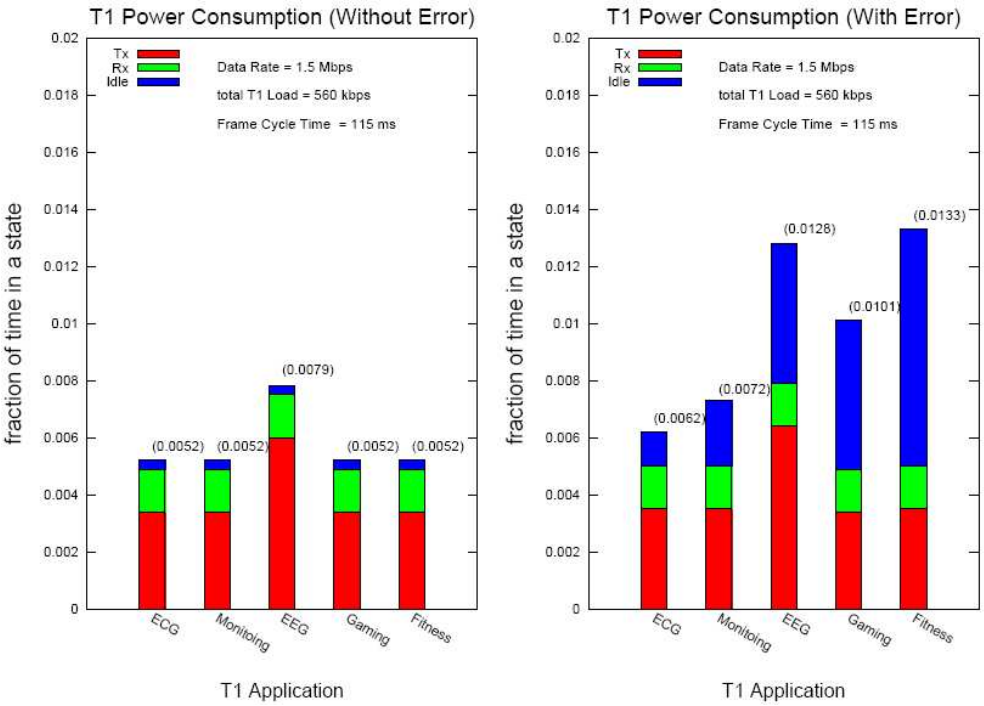


Figure 83 -- Power results for T1

11.2 Simulation 2: Application class T2

Table 5 – Application specific details for T2 simulation

Application	Arrival rate/devices	Number of devices	Allocated slot time (Si) per device (ms)
EMG	96 Kbps	12	4.8
Audio (CBR)	64 Kbps	10	2.73

Table 6 – Global simulation parameters for T2 simulation

Simulation Run	100 sec

Data rate	3 Mbps
PER @256 Bytes	10 %
Total load	1792 kbps
Frame cycle	115 ms
IFS	15 µs
Poll size	15 bytes
ACK size	15 bytes

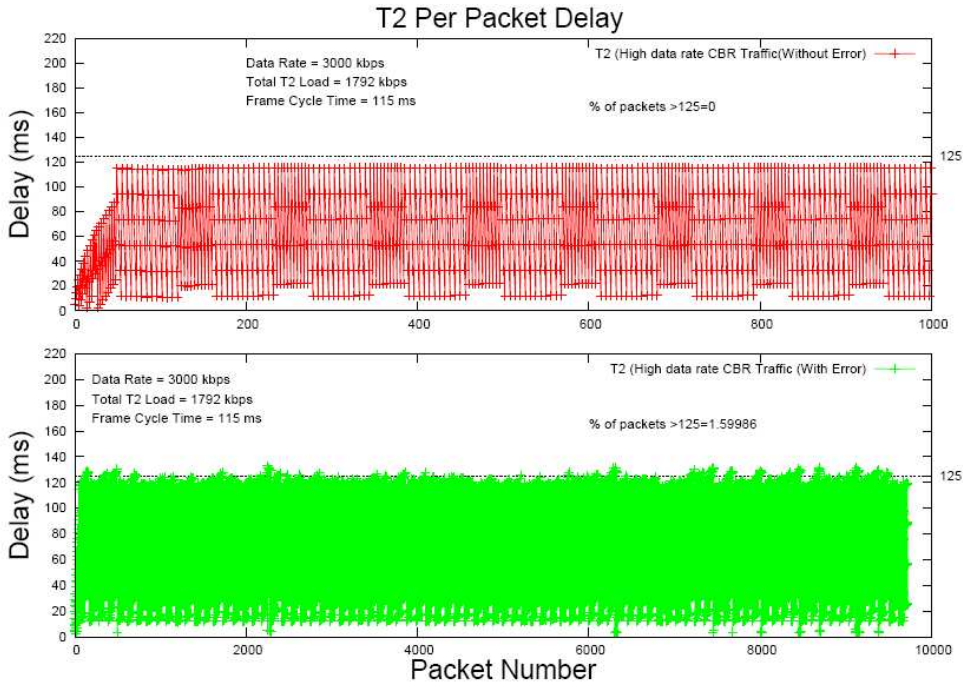


Figure 84 - delay results for T2

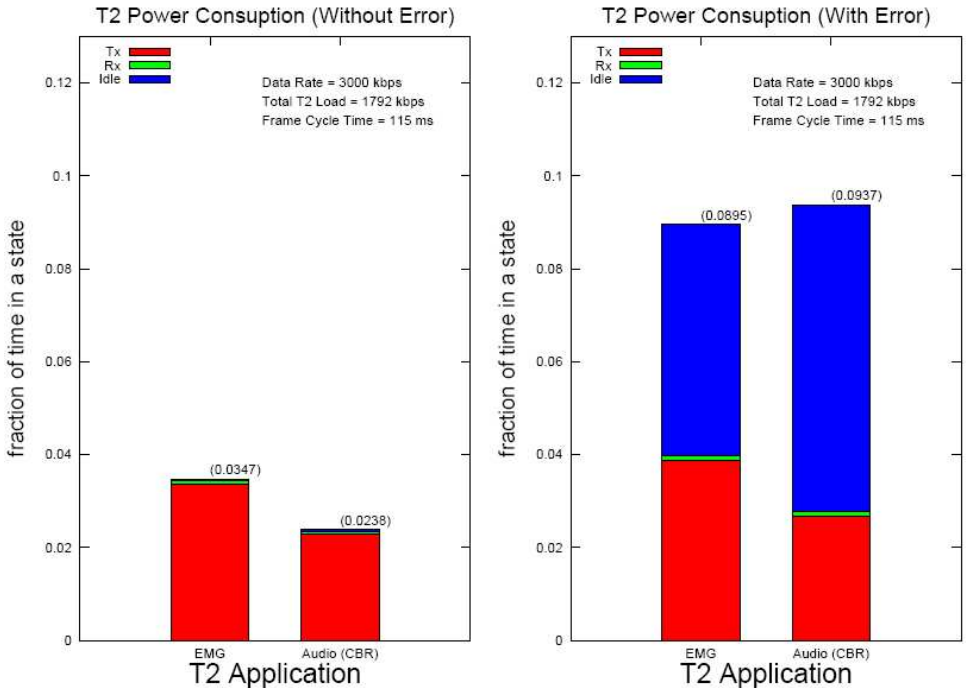


Figure 85 - power results for T2

11.3 Simulation 3: Application class T2

Table 7 – Application specific details for T3 simulation

Movie Name	Compression ratio	Mean frame size (bytes)	Peak/Mean (Packet size)	Mean (Kbps)	Peak/Mean (Data rate)
Star Wars	27.62	1400	6.81	280	1.9
Star Trek	23.11	1600	7.59	330	2.5
Silence of the Lambs	13.22	2900	7.73	580	4.4
Mr. Bean	13.06	2900	5.24	580	3.1

Table 8– Global simulation parameters for T3 simulation

Data rate	10 Mbps
PER @ 256 Bytes	10 %

Frame cycle	115 ms
IFS	15 µs
Poll size	15 bytes
ACK size	15 bytes

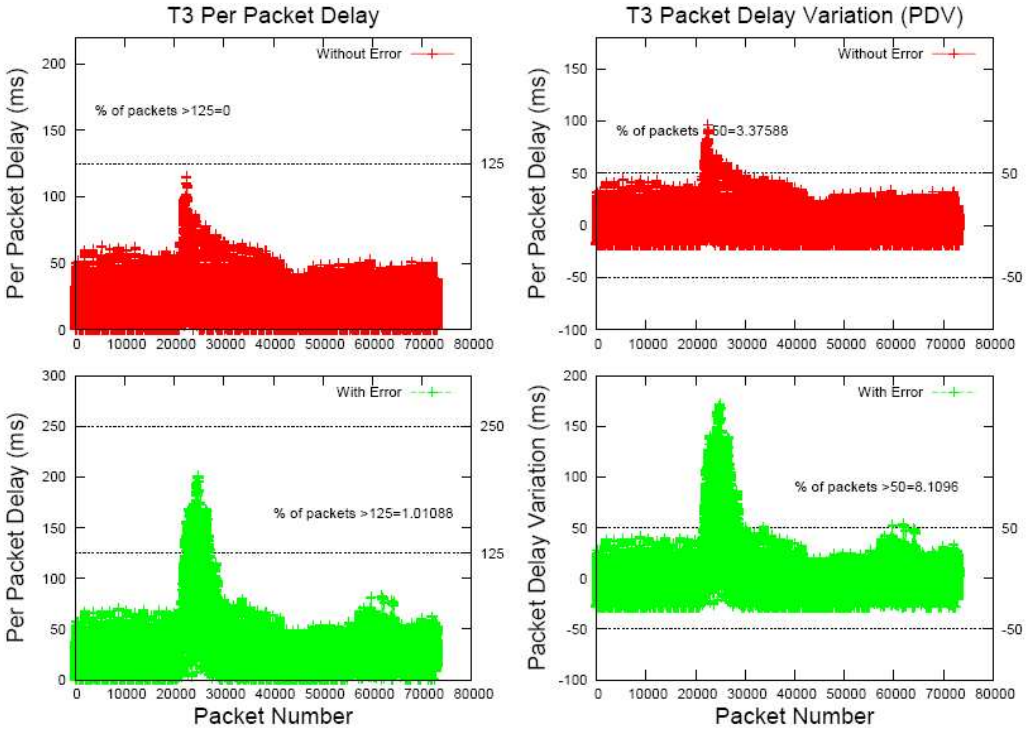


Figure 86 - Delay and packet delay variation results for T3 simulation

11.4 Simulation 4: Variable poll rate

Table 8 – Traffic detail of variable poll rate simulation

Application	Arrival rate/devices	Number of devices	Allocated slot time (Si) per device (ms)
App 1	4 Kbps	3	1.53
App 2	2 Kbps	3	1.53
App 3	1 Kbps	4	1.53

Table 9 – Global simulation parameters for variable poll rate simulation

Data rate	300 Kbps
Total load	22 Kbps
Frame cycle	50 ms
IFS	196 µs
Poll size	15 bytes
ACK size	15 bytes

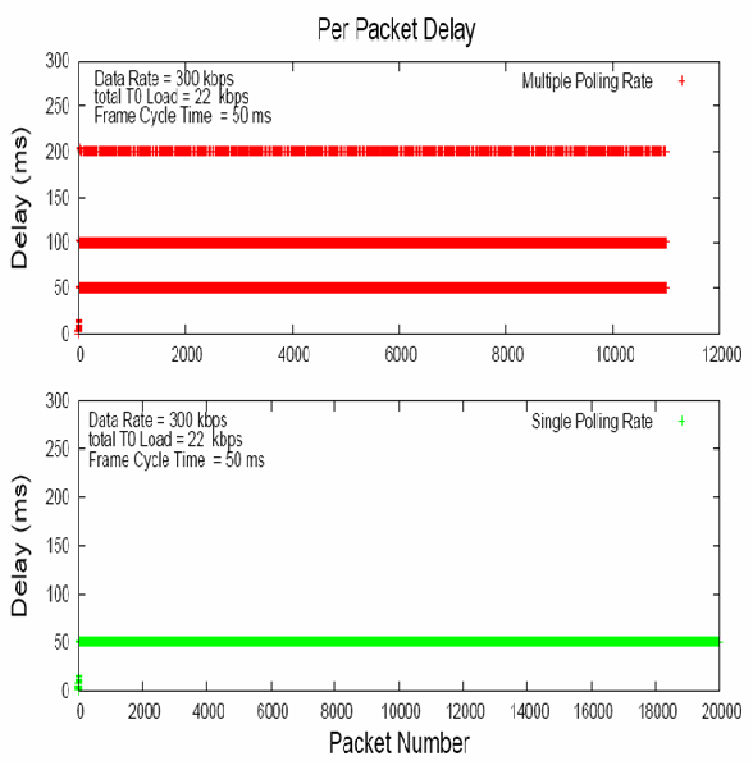


Figure 87 - delay results for variable poll rate

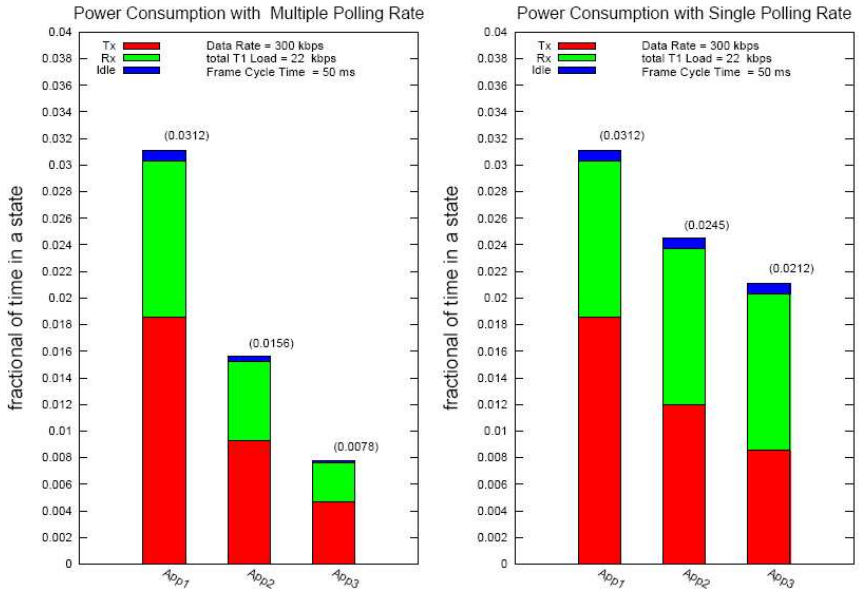


Figure 88 - power results for variable poll rate

11.5 Simulation 5: Emergency Latency

The simulation is performed to measure the latency of emergency handling with the following parameters

- An emergency is scheduled randomly in a simulation run
- Number of simulation run = 10000
- Duration of a simulation run = 1000sec
- 10 implant data sessions in a simulation run with each session duration of 10sec
- Duty cycle of coordinator = 10%
- One channel transmission time 100ms

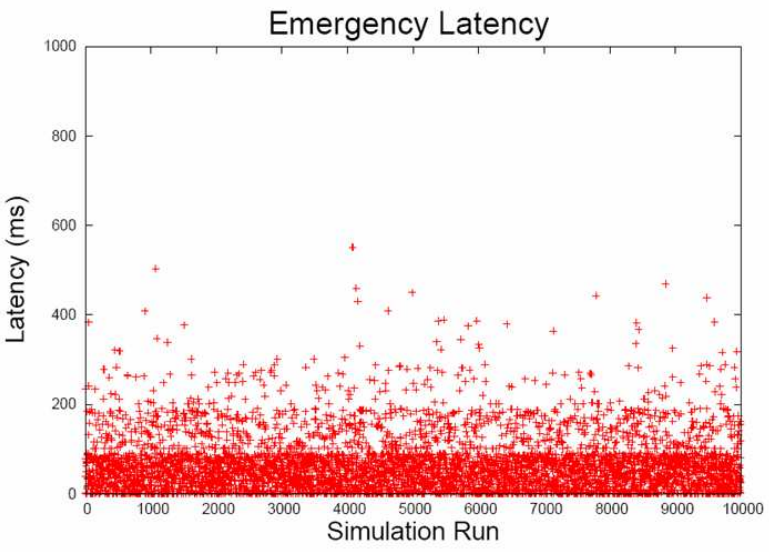


Figure 89 - latency result for emergency handling

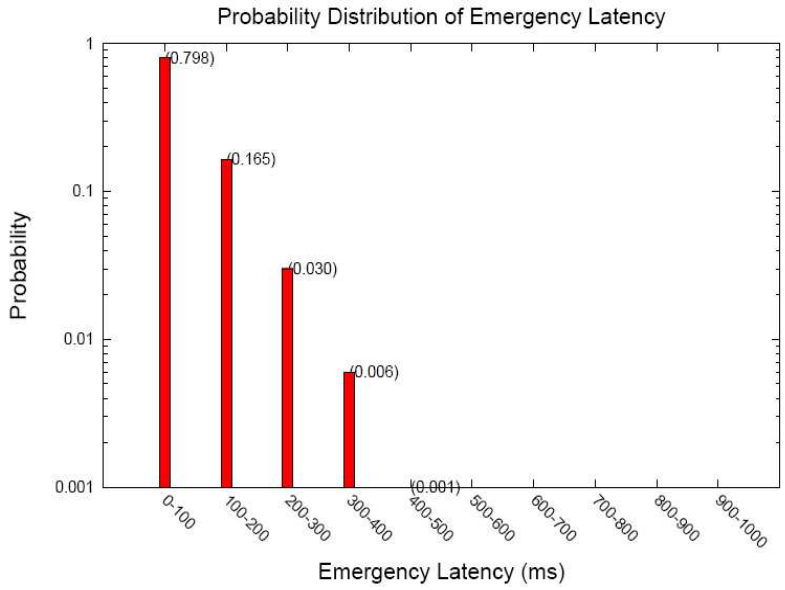


Figure 90 - PDF for latency of emergency handling

11.6 Simulation 6: The effect of frame cycle on delay and power

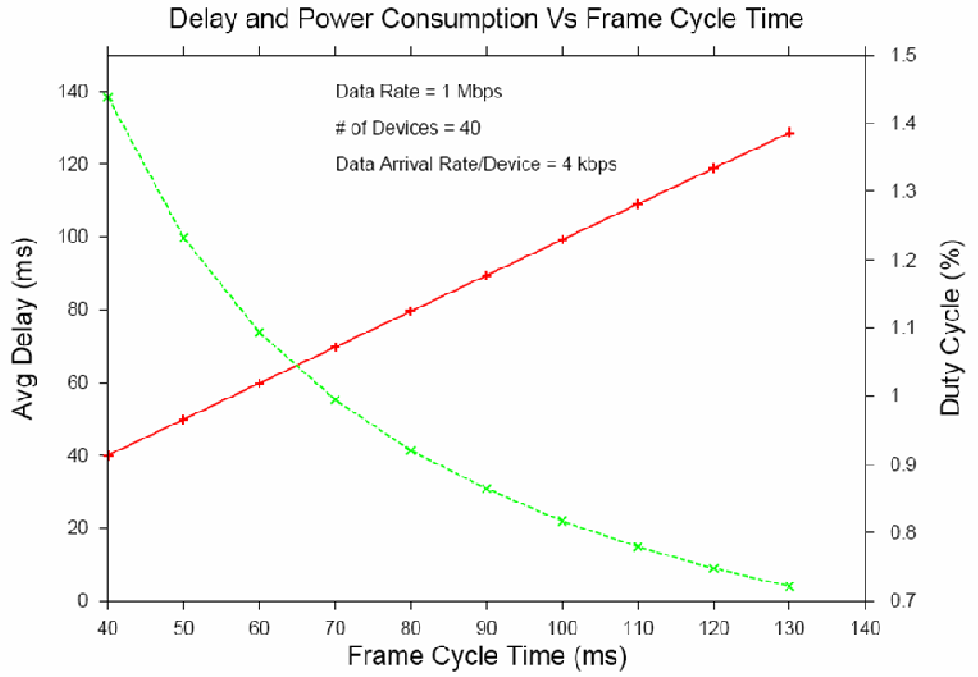


Figure 91 - Delay and power consumption Vs frame cycle

12 Appendix C: Guideline to select superframe length

The length of superframe is constraint by the following conditions.

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

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

- If the superframe 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 superframe length should be large enough such that it can support data arrival at n.

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

Where,

Pi = Poll size for ith device
Si = Allocated transmission duration for ith device
R = Data rate of the physical channel
IFS = Inter Frame Space duration