IEEE P802.15
Wireless Personal Area Networks

Project	TG6 Body Area Networks
Title	NICT's MAC proposal to IEEE 802.15.6- document
Date Submitted	14/November/2009
Source	[Bin Zhen, Grace Sung, Huanbang Li, Ryuji Kohno] [NICT] [Yokosuka, Japan]	Voice: [+81-46-847-5445] Fax: [+81-46-847-5431] E-mail: [zhen.bin@nict.go.jp]
Re:	Response to IEEE 802.15.6 call for proposals
Abstract	This submission provides normative text for a MAC proposal presented in accompanying documents 802.15-09-0346-01-0006, 802.15-09-0161-00-006, and 802.15-09-0162-00-006.
Purpose	To submit a MAC proposal to IEEE 802.15.6
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 September be made publicly available by P802.15.

Table of contents

1. General MAC features

The MAC feature designed in this proposal is intended for (but not limited to) medical wireless body area networks. Delay latencies, network reliabilities, and device power consumptions hence are key criteria considered in the design. In particular, the MAC protocol must allow all possible PHY technologies (e.g. UWB systems, wearable narrowband systems at WMTS, WBAN, and ISM band, implanted systems at MICS band, and Human Body Communication systems) to run its full features. Some other considerations are coexistence, security, scalability and safety (SAR) etc. The major requirements for the MAC are as follows:

- Support medical and non-medical applications.
- To provide dependability and QoS guarantee for the most important life-critical message and majority real time traffic.
- Support multiple PHYs: UWB, MICS, WMTS, HBC.
- Support large range of data rate: from 10kbps to 10Mbps.
- Support large range of duty cycle: from <0.1% to ~30%.
- Support dynamic network size: from typical <6 nodes to >100 nodes per piconet.
- To provide power efficiency: >10 years life time.

1.2 A two-mode MAC

The network topology considered in this proposal is the star network as shown in Fig. 1. A BAN piconet consists of a central controller (namely the BAN coordinator) which initiates, terminates and manages the BAN piconet. For most BAN application scenarios, a single hop is enough. Transmissions within the network can hence be classified into coordinator-to-device (downlink) and device-to-coordinator (uplink). Note that the peer-to peer communication (device-to-device) is not considered here. The coordinator uses beacons command to identify and manage (such as create, maintain and terminate) a BAN piconet.
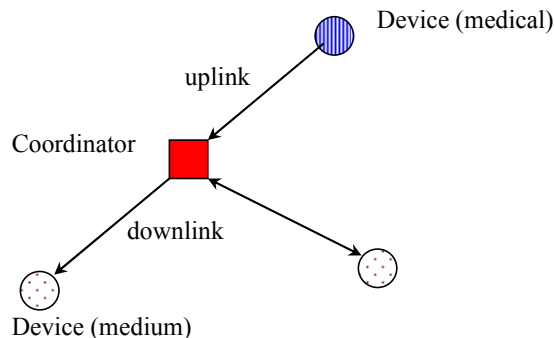

Fig.1   Start topology of BAN piconet

In order to sustain QoS oriented applications, this proposal supports the superframe structure to provide guaranteed channel access for traffic. For a BAN piconet which has the coordinator that regularly emits beacons, it is considered as operating in the beacon-mode. For simple BAN piconets, such as a simple MICS system with an implant sensor/actuator and an outside controller or medical systems sustaining lifetime more than 10 years, this proposal supports the non-beacon operating mode because these systems cannot or do not want to listen to the periodically transmitted beacon. The BAN piconet is said to operate in the non-beacon mode, if the coordinator does not regularly emit beacons. In contrast to the beacon mode, no time structure is defined and used for channel access in the non-beacon mode.

Note that, beacon command itself is not the key difference between the beacon mode and the non-beacon mode. Key differences are the regularity of beacon emissions and time structure. A BAN piconet can only operate in one mode. [1]

1.2 The BAN superframe structure

As shown in Fig. 2, the superframe structure defined in the beacon mode is bounded by regular beacons transmitted by the coordinator. The superframe structure is divided into an active portion and an inactive

---

[1] There is an exception for MICS systems in the case of emergency medical event. A medical implant event is allowed to transmit at any time to comply with the FCC MICS rule.

portion. In the inactive portion, the coordinator and devices may enter low power (sleep) mode for power conservation.   The BAN coordinator which is the control center of the BAN piconet is responsible for maintaining the timing of superframe structure.

In the active portion when data transmission occurs, the structure is further sequentially divided into the beacon, the priority access period (PAP), the contention access period (CAP), and the contention-free period (CFP). The CAP supports contention based channel access for one-time prompt traffic, such as association, bandwidth request, and some low duty cycle traffics. The CFP supports scheduled channel access for periodical traffics and QoS guaranteed traffics, such as medical waveforms and stream of audio and video. The PAP supports high priority communications for classified emergency or alarm traffic which is life critical over any other traffic.

The BAN superframe is divided into equal length time slots for easy computing of channel capability given a data rate. This reduces the required processing power for a device. The superframe structure can be configurable through beacon. Parameters to describe the superframe structure include:
- duration of a slot,
- number of slots in the active/inactive portion of superframe,
- present of PAP and CFP, and
- number of slot in the PAP, CAP and CFP of active portion of the superframe.
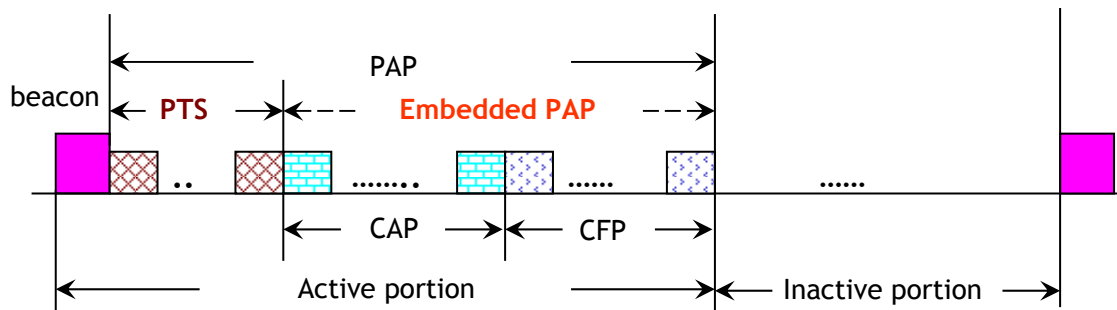

Fig.2 Structure of BAN superframe

1.3 Traffic classification

This TG6 was proposed by considering medical BANs as the main applications. Network reliabilities and packet latencies are therefore critical, especially for emergency life-threatening data. In order to ensure most instantaneous emergency data transmissions, traffics are classified into different categories before channel access in both the beacon mode and the non-beacon mode. As shown in Table I, each traffic category has different probabilities for getting a transmission chance (see section 2.1 and 2.4) during the CAP and different times for re-transmission. For example, voice traffic has higher probability of getting a communication window in CAP comparing to video traffic, and only the medical emergency data can be sent in the PAP. The traffic categories in Table I are from IEEE 802.1D. Table I lists two methods to contend the channel using ALOHA protocol
- To define an ALOHA window which consists of ALOHA slots. The length of the ALOHA window depends on the traffic category. The device randomly selects one of them to transmit.
- To define a transmit threshold for every ALOHA slot. The transmit threshold depends on the traffic category. The device generates random numbers between [0, 1] for all ALOHA slots in the CAP and selects the first one which is below the threshold to transmit.

Note that two methods are not equivalent. The first one make sure at least one transmit in an ALOHA window; while the transmission in every ALOHA slot in the second method is independent. There is always a probability that there is no transmit in a relative long time.

One more consideration of life-critical/alarm message is that the coming traffic has more stringent QoS and reliability requirements than those existing traffics. For example, a medical waveform for a patient in the ICU room is not considered as an Emergency/alarm message after its transmission is guaranteed by the CFP (defined in Section 2.3). However, when body temperature is detected to be over 40 degree, this is an Emergency/alarm message since treatment for such a high body temperature will decide the live or death of patient.

Table 1 Traffic classification

Priority	User priority	Traffic designation	ALOHA window		ALOHA threshold		Max. retransmit
			AWmin	AWmax	THmax	THmin	
Low	0	Background	16	64	0.125	0.0312	3
	1	Best effort	16	32	0.125	0.0625	3
	4	Video	4	16	0.25	0.0625	3
	5	Voice, medical waveform	4	8	0.25	0.125	3
	6	Network control	2	8	0.5	0.125	3
	7	Emergency/alarm message	1	4	1	0.25	5
High							

1.4 Acknowledge policy

The proposal supports four different types of acknowledgement schemes:
- No-ACK, which is that no ACK is required after data transmission.
- Immediate-ACK (Im-ACK), which the ACK being sent immediately after the packet transmission.
- Delayed-ACK (D-ACK), which the ACK being sent after multiple packet transmissions.
- Information piggybacked ACK (IP-ACK), which is to attach MAC command or message after the ACK packet.

No-ACK and D-ACK provides higher throughput when the channel condition is good. However, D-ACK may increase the complexity of device since it has to buffer all frames of transmitted data before they are confirmed. IP-ACK transmits an MAC command and a data packet to a device simultaneously for efficient channel resources managements. For example, an improvised slot in the CFP of the same superframe can be allocated by using IP-ACK to allow immediate re-transmission once error occurs. The IP-ACK can be combined with both Im-ACK and D-ACK.

2. Beacon mode

As mentioned above, the beacon mode is when the BAN coordinator regularly emits beacons to define the superframe structure for channel access. A superframe sequentially consists of the beacon, PAP, CAP and CFP. The superframe structure is bounded by beacons.

2.1 Beacon command

The beacon command is the first packet in a superframe. Beacon is a broadcast message to all devices in the BAN piconet. Functions of beacon are:
- BAN piconet identification
- Determining working mode of a BAN piconet (i.e. beacon mode or non-beacon mode)
- pending data or emergency/alarm messages to devices
- superframe management and status of slots in CFP
- clockwise and frame synchronization

The beacon may span 2 or 3 consecutive slots. For security concerns, the beacon can be transmitted with time or frequency hopping to avoid any potential eavesdropping or jamming. In order to comply with the FCC rule, for a network that operates in the MICS band, channel sensing by the coordinator is required before beacon transmissions.

Note that broadcasted beacons may be lost due to channel reasons. It is not necessary for a device to listen to every beacon in order to communicate in the beacon mode. In other words, a device can determine its beacon listening interval according to its own clock accuracy and application requirements. The selective beacon listening is shown in Fig. 3. This helps to reduce power consumption for beacon listening.
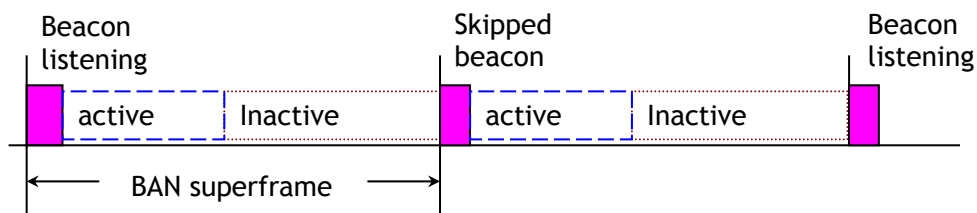

Fig.3 Selective beacon listening

During device associations, the coordinator configures the superframe format and also defines how frequent a device should listen to the beacon. The coordinator may also change the configuration of superframe

during communications. But the new configuration must be repeated multiple times to make sure that all devices know the changes before it takes effect.

2.2 Contention access period (CAP)

The CAP starts immediately following the PAP and shall complete before the beginning of the CFP on a superframe slot boundary. The CAP length is configurable. However, its length shall not be zero. The minimum length is 7 slots.

2.2.1 Why not CSMA?

The CAP is used for uplink traffic only. In the CAP, devices that wish to transmit will compete for channel access using slotted ALOHA mechanism. The ALOHA, instead of CSMA mechanism which depends on clear channel assessment (CCA) operation, was chosen because of the underlying PHY features. As shown in Fig. 4

- The impulse UWB signals are hard to be detected due to its weak, transient and carrier-less features, and harsh channel condition.
- Fast attenuation of in-body MICS signals (< 300mm propagation distance)
- Deep fadings of on-body narrow band signals in the case of Non-line of sight (NLOS)
- High noise floor of HBC systems
- Fast and deep fading of on-body system due to human movements

The above channel conditions make it unreliable for CCA operation. An unreliable CCA results in the well known 'hidden node' issue in the CSMA. Consequently, the CSMA deteriorates to pure ALOHA channel access, which is of worse performance than the slotted ALOHA.
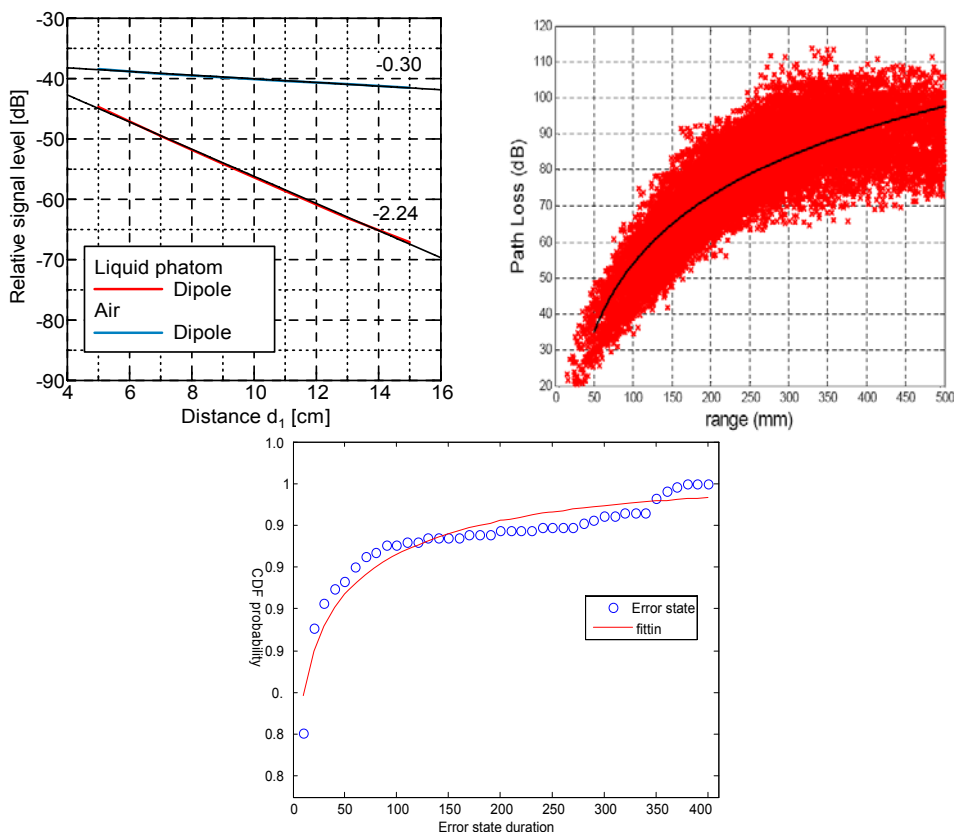

Fig. 4 Measured path-loss of MICS signal in 08-0416-03 (a), simulated path-loss of MICS signal in 08-0519-01 (b), and measured fading period due to movement in the UWB band (c)

2.2.2 Slotted ALOHA channel access

In the slotted ALOHA, a packet must finish its transmission in a slot. This, however, results in the well known upper limitation of capacity of the slotted ALOHA. The CAP is mainly designed for one-time prompt traffics

and some low duty cycle traffics. For these kinds of traffic, a large amount of payload is not expected.[2] To increase the capacity of CAP, each contention slot (a CAP slot and a PTS slot in Section 2.3) is further divided into two ALOHA slots, as shown in Fig. 5. Communications and acknowledgements shall be completed within the ALOHA slot. This means less packet collision during channel contention. As a result, the CAP capacity is doubled.
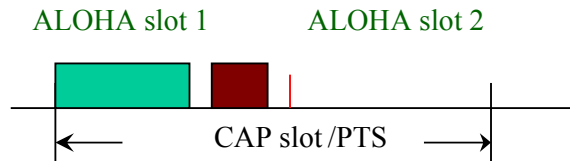
ALOHA slot 1   ALOHA slot 2

CAP slot /PTS

Fig.5 two ALOHA slots in a CAP/PTS slot [3]

Note that the two ALOHA slots in a CAP slot are a tradeoff between collision probability and net throughput which is the throughput of packet payload. Although more ALOHA slots can further reduce collision probability, fewer octets of payload can be carried by a frame packet on considering a fixed length of preamble is needed for any frame. To be more flexible, the duration of ALOHA slot is configuration to adapt to the CAP slot, data rate, and traffic load.

As shown in Table I, all traffics are classified into different categories before channel access. For communications in CAP, each category of traffic has different transmit probability in a communication window. If the communication fails in the first trial, the device shall back-off a certain period of time and try again. The back-off period is exponential based, and its unit is the communication window. The device repeats the above steps with a new transmit probability until the maximal number of re-transmission or the end of CAP. The detail procedure for slotted ALOHA is described in Fig. 6.

----
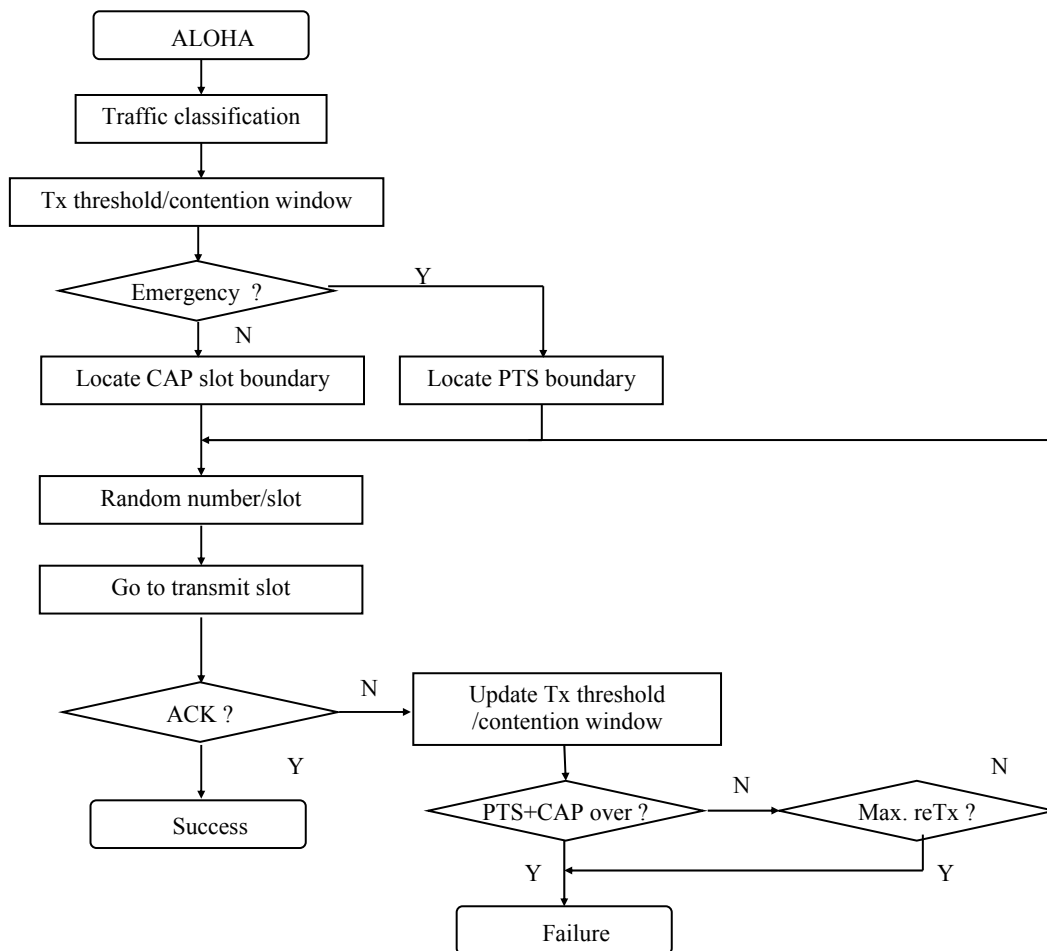
[2] In other words, it is suggested to use CFP for bulk data communications.
[3] The same structure of ALOHA window was designed in CAP slot and PTS. This can decrease the complexity of device and protocol.

Fig.6 Slotted ALOHA based channel access in the beacon mode

2.3 Contention free period (CFP)

The CFP is immediately after the CAP and shall complete before the next beacon. The CFP consists of multiple guaranteed time slot (GTS). The CFP length is configurable with minimum length equal to zero.

2.3.1 Guaranteed time slot (GTS)

Communications in the CFP is reservation based. The allocation of GTS is controlled by the coordinator. This guarantees the required QoS and reliability for specific traffics. The device informs the coordinator its QoS requirement during association. Multiple contiguous GTS can be granted to one device. The GTS can also be used for poll command. The communication shall start only at the beginning of the GTS allocation. And it must complete before the end of the last allocated GTS. The allocation of GTS to a device is attached with an attribute tag with

- lifetime attribute, which is the lifetime of the allocation, and
- traffic attribute, which is either general allocation or exclusive allocation.

The lifetime of a GTS allocation can span one superframe (i.e. for one times re-transmission), multiple superframes (i.e. for a session of best-effort traffic), or infinite superframes (i.e. for periodical traffic). For all non-medical traffics, the GTS allocation is general allocation. This is contrast to the GTS allocation to medical traffic, which is exclusive. The difference is that, when there are not enough GTSs to be allocated, the coordinator can withdraw general GTS allocations even before their expiration and grant the GTS to new medical traffics. This provides high priority for medical traffics over the non-medical traffics. The withdrawal of general GTS allocations shall be known by the device.

The CFP can be used by both uplink and downlink traffic. For allocated uplink GTS, the device shall directly transmit and the coordinators enter reception state. It is vice versa for downlink GTSs.

The access of GTS for a device can be periodic or on-demand. The periodic GTS access means the device is grated the same GTS allocation in every M ($1 \le M < \infty$) superframes. It is designed for scheduled traffics, like medical waveforms and voices which occur periodically. After the GTS reservation is granted, the device can always use them until the reservation expires. The on-demand GTS access means a one time GTS allocation, which can be in the same superframe or the next superframe. It is designed for unscheduled traffic, like network managements, re-transmissions or low duty cycle events.

2.3.2 Poll command in CFP[4]

This MAC proposal supports poll command in the unoccupied GTSs which have not allocated to any device. A particular reason for having poll command is the MICS system. According to the FCC's MICS rule, the implant device works in a reactive manner for except medical events. This implies that implant devices must be inquired first, and then answer the inquiry. It is, therefore, in the grey area whether the beacon is an 'inquiry' or not. Although beacon is generally considered as a broadcast message, it does have mandatory CAP to allow devices to transmit. The poll command bypasses the grey area by specifying a two-way transmission session. The biggest difference between poll and beacon is that the poll is specified with a destination address, while the beacon is not. In other words, the poll command particularly enquires if particular devices have data to send. Therefore using the poll complies with the FCC regulation for MICS systems.

The poll command can address to

- a single device by a unique address, or
- any device by the public address

The former allows an improvised access of GTS for a device. This can be used for re-transmission or additional traffics beyond the capacity of allocated GTS. The latter shall only be used in the non-beacon mode for implant network association.

The poll command carries information for network associations and superframe structure in the beacon mode. It also defined a communication period. As illustrated in Fig. 7, the communication period can be

- immediately after the poll command, or
- after a while of the poll command.

---

[4] The poll command can be used in non-beacon mode, too.

The channel access for public addressed poll command is based on the slotted ALOHA. The channel access procedure is the same as those described in Fig. 6.

As illustrated in Fig. 7, an explicit poll command is used to enquire pending data. The explicit poll may emit regularly from the coordinator in un-allocated GTSs based on a pre-defined parameter. The poll command can also occur implicitly, usually together with the IP-ACK sent to a device. The implicit poll may indicate transmission corruptions, and requesting a re-transmission. In such a case, it is referred as the on-demand poll.
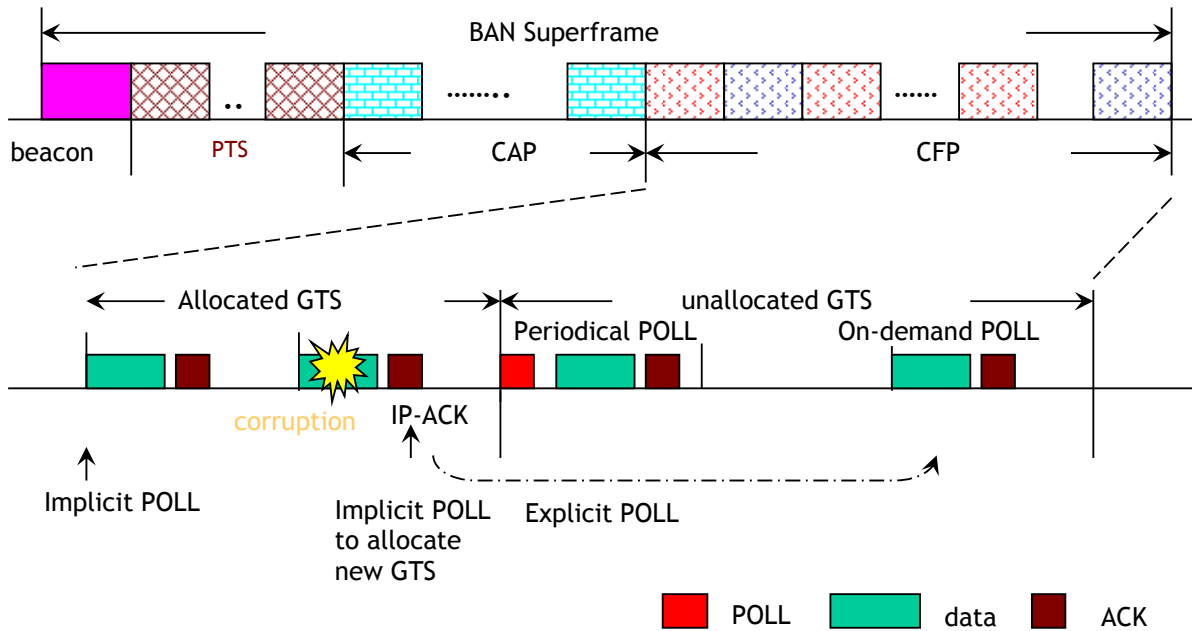

Fig.7 Poll command in CFP

2.4 Priority access period

The priority access period (PAP) is immediately after the beacon in the superframe. The PAP is dedicated for the emergency/alarm message. Any other categories of traffics shall not take the PAP. The PAP is comprised by
- Priority time slot (PTS), which is a physical time period immediately after the beacon, and
- embedded PAP, which are the unoccupied slots in both CAP and CFP.

The emergency/alarm message can be either uplink or downlink. Although emergency/alarm messages are typically low duty cycle, more than one medical sensor may simultaneously detect abnormal signals in the life-critical situation.

Once the emergency traffic occurs, devices shall listen to the beacon to know the configuration of current superframe. If a GTS has been allocated in the current superframe, the device can transmit the emergency traffic in both PAP and the allocated GTSs.

The channel access in PAP is contention based because it is in-efficient to allocate fixed radio resources to the low duty cycle nature of the emergency traffic.

2.4.1 Priority time slot (PTS)

The duration of PTS is configurable. For medical applications, it usually span for 2~3 slots. For non-medical applications, it can be set to 0. The PTS in the superframe provides guaranteed channel access for emergency traffic, which is required by the FCC.

The same a CAP slot shown in Fig. 5, each PTS slot is divided into two ALOHA windows. This allows tow chances of channel access which doubles the PTS capacity. Another reason is that the emergency traffic is usually not very long (with limited payload). The emergency traffic and its ACK shall be completed within the ALOHA window.

The PTS supports both uplink and downlink emergency communications. As shown in Fig. 8, the beacon shall indicate the direction of each communication window. For downlink emergency traffics, the coordinator shall also indicate the addressed device in the beacon. It shall transmit the emergency traffic in the scheduled communication window, and wait for the ACK from the device. For uplink emergency traffics, the slotted ALOHA procedure described in Fig. 6 is adopted. If a data transmission failed, the device shall make transmission attempts later in the embedded PAP. Although the channel access for uplink emergency traffic is contention cased, high probability of packet collision is not expected due to the low duty cycle nature of emergency traffics.
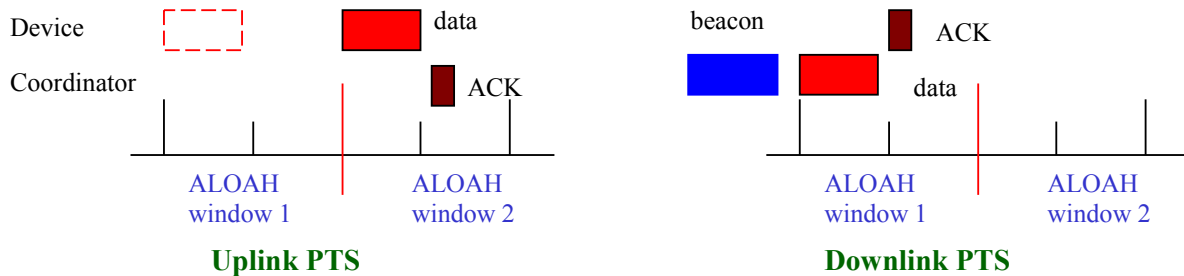
Fig. 8 Priority time slots (PTS)

2.4.2 Embedded PAP

Although the PTS in the superframe provides the guaranteed channel access for emergency traffic, it is wasteful in bandwidth as the emergency priority traffic is usually low duty cycle. The embedded PAP corresponds to the un-occupied slots in both CAP and CFP. In other words, the embedded PAP partially overlaps with the CAP and the CFP. It provides a second opportunity for emergency traffics which failed to be transmitted in the PTS.

Figure 9 illustrate three types of the embedded PAP which correspond to three different scenarios:
   1) CAP slots: All CAP slots are unoccupied per its definition. The emergency traffic contends the channel with other traffics using slotted ALOHA mechanism with, however, different parameters shown in Table I, (i.e. transmit probability and backoff steps).
   2) Free GTSs in CFP: The device knows free GTSs by listening to the beacon. The free GTS is accessed in the same way as PTS. To support this, the coordinator shall enter reception state in all free GTSs.
   3) Free period in allocated GTSs: A device may not use the full duration of allocated GTSs. It is possible to utilize the remaining free period to complete the emergency transmit and its ACK. However, this requires a more complicated operation. At the coordinator, it requires to emit a buzz signal to indicate the completion of the assigned data transmission for those PHYs which cannot conduct reliable channel sensing. At the device end, it shall actively detect the channel by channel sensing or listening to the buzz signal to know the channel status.

The PTS and embedded PAP together enable an efficient way to provide multiple opportunities for emergency traffics. By having multiple transmit opportunities, simultaneous alarming from multiple sensors can be reliably delivered.
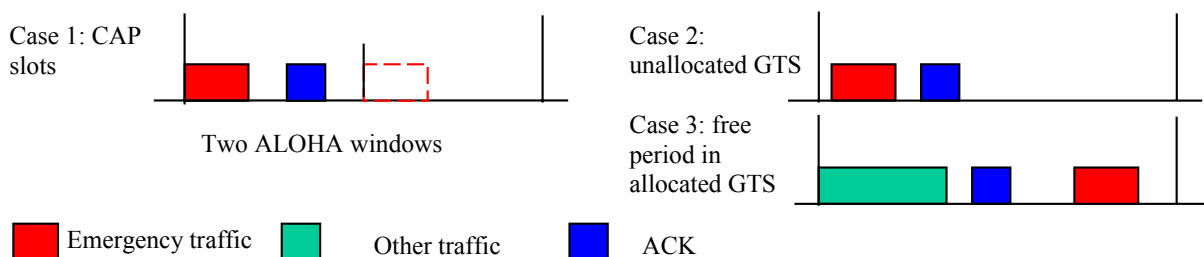
Fig.9 Three scenarios for embedded PAP

2.5 BAN group superframe

Some medical applications, such as EEG and ECG, have real time traffic from a large amount of sensors to a data collector. There are two methods to support more devices in a BAN piconet

- More slots in a superframe up to 256
- Ground BAN superframe which consists of N superframes

The first method has some drawbacks on considering the frame design. For example, one of functions of the beacon is to broadcast the GTS allocation in current superframe. Per IEEE 802.15.4 superframe where there are 7 GTSs, the payload is 35 bytes. However, for a superframe with 256 GTSs, the payload will be 1070 bytes. The payload is too much on considering the fading rate of a dynamic BNA channel (shown in Fig. 4(c)) and low data rate (<100kbps) of some narrow band PHYs. Besides, long superframe may lead to large clock offset to be considered. As a result, a large guard time is need because the guard time should cover the worst case.

For the above analyses, the proposal thus provide group BAN superframe as shown in Fig. 10. Each superframe consists of the configurable active portion and inactive portion, as shown in Fig. 2. The beacon only covers a limited number of GTS in current superframe. Each GTS is labeled by a superframe ID and GTS ID. The BAN group superframe also enables a flexible configuration to adapt GTS allocation per dynamic range of duty cycle.
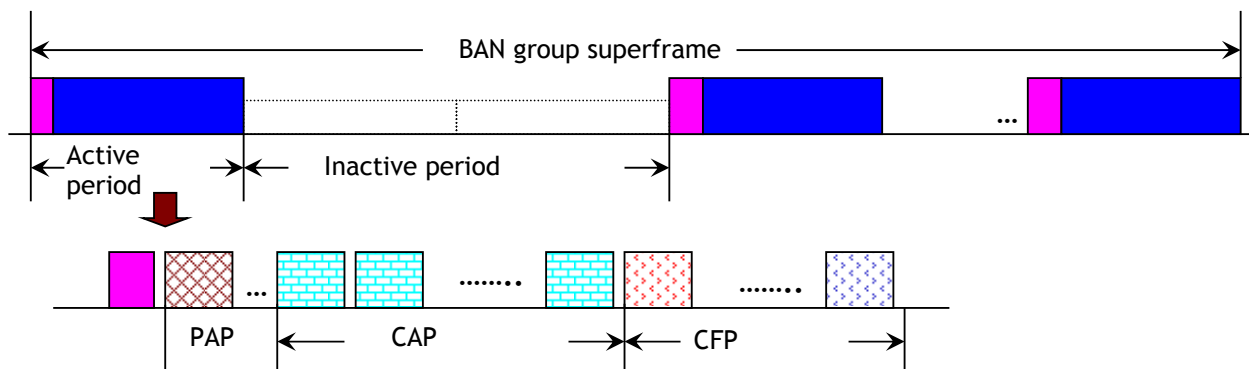
Fig.10 BAN group superframe

3. Non-beacon mode

When the BAN coordinator does not regularly emit beacons, the BAN piconet is said to operate under the non-beacon mode. This is a power saving operating mode for devices which cannot or do not want to listen to beacons. For the very low duty cycle applications, periodical wakeup and listening to the beacon for synchronization may consumes more power than what that used for traffic payload. The non-beacon mode can also be used for very simple networks. For example, most implant applications consist of only a few (1 or 2) implant devices. The beacon mode is overloaded for such applications.

In the non-beacon mode, there is no concept of superframe structure. Communications in the non-beacon mode are divided into handshake session and communication session with fixed durations. The handshake session consists of ALOHA slots. The poll command is used in the handshake session to confirm that the counterpart is ready for reception. The devices and the coordinator shall wake up at the rendezvous time and start the handover session. The deviation of the clocks may be very large after long time of sleeping. Comparing with the data frame, the poll command is short and therefore will not consume too much power even is lost. The coordinator or device may also start the handover session by using wakeup radio. The communication session is uniquely occupied by one device which have successful handshake. The time reference is the star of first received poll.

As shown in Fig. 11, either the coordinator or the device can initiate the handshake. They are used for downlink traffics and downlink traffics, respectively. The only difference is who speak first.

For the coordinator initiated handshake, the device shall enter reception state and wait for polls from the coordinator. Upon receiving a poll command with a unique address, the device shall reply an ACK to indicate it is ready for communications. Then both the coordinator and the device enter the communication session for traffic. If the handshake session failed, which could be due to bad channel conditions, clock offsets or packet collisions (from other BAN piconets), the coordinator and devices shall exercise an exponential back-off, and make another attempt after the back-off period. If the handshake session expired, there shall be no communication session. For MICS systems, implants should try to listen to different channels for poll command since they have no knowledge on which channel the coordinator will select. The

poll command with a public address is used by MICS systems for piconet association. Upon receiving a poll command, the implant shall generate a random number to decide whether to response in the ALOHA slot. Similar mechanism can be found in Fig.6.

For the device initiated handshake, the device will shall send polls first. Different from the coordinator initiated handshake, multiple devices may wakeup simultaneously. The channel access mechanism is based on pure ALOAH for the same reasons described in Section 2.2.2. The packet collision contributes another reason for the handshake failure. If the handshake session failed, exponential back-off shall be conducted for the next opportunity.
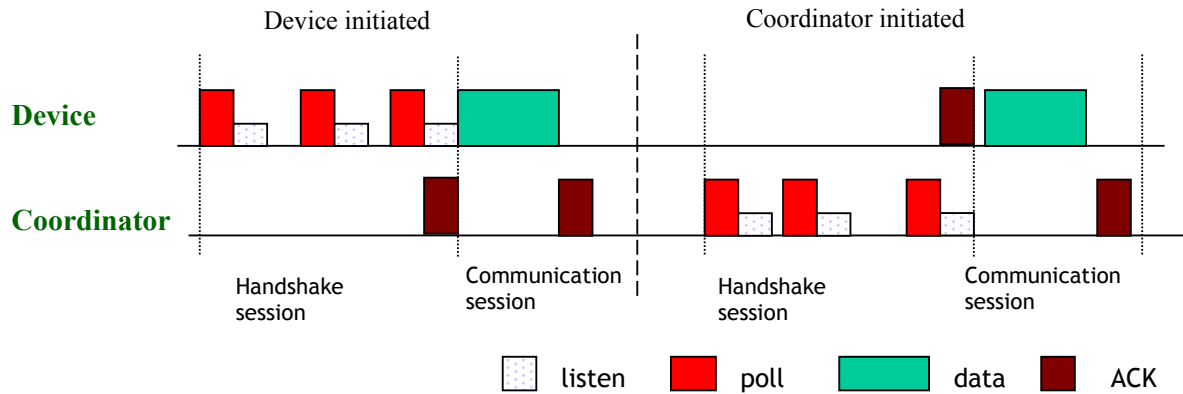

Fig. 11 Communications in the non-beacon mode

4. Low power consumption

Low power consumption is important to medical applications. Even in the beacon mode, to save battery is needed. As shown in Fig. 2, devices can enter sleep state during the inactive period of the superframe. In addition, as shown in Fig. 3, the selective beacon listening allows the devices to skip some superframes as long as the clock accuracy and QoS requirements are satisfied.

4.1 B-E beacon transmit

One of the important functions of beacon in the beacon mode is to allow synchronizations between devices and the coordinator and to align all transmissions to start from the slot boundary.

In order to overcome the potential clock offset between the coordinator and devices after long time sleeping, the conventional practice (as defined in IEEE 802.15.4) is to have devices being ready prior to the beacon emission by a certain amount of time, which equals to the maximum possible clock offset. For a given time, T and clock offset $\pm \delta$, the device must wake up at T-2δ to wait for the beacon. This method is referred as B-B in Fig. 12. After wakeup per its own clock, the coordinator emits beacon. By being ready for reception before the beacon, the devices can easily define the slot boundary which is at the beginning of the beacon frame. However, more power is consumed at devices since it is the device's duty to compensate the clock offset.

Instead of having the devices to counteract the potential clock offset, this proposal supports an alternative method termed B-E, by which the coordinator is responsible for compensating the potential clock offset. As shown in Fig. 12, the coordinator now emits the beacon earlier and with a longer preamble at T-2δ. Therefore, when the devices wake up, the beacon is always available. Although the coordinator pay more power for clock offset compensation, the power consumption at devices is reduced. The B-E method matches the fact that the BAN coordinator is usually richer in battery budget in comparison with devices.

In the B-E scenario, the slot boundary is now defined at the end of the prolonged preamble by the delimiter. The frame delimiter can be set directly at the slot boundary or a constant offset to the slot boundary. This B-E beacon broadcasting strategy is considered to be more efficient for BAN, because the coordinator usually has more power capacity than the device. Especially batteries for the coordinator could be rechargeable or easier to replace comparing to batteries for BAN devices. Table III compares the two beacon broadcasting methods.
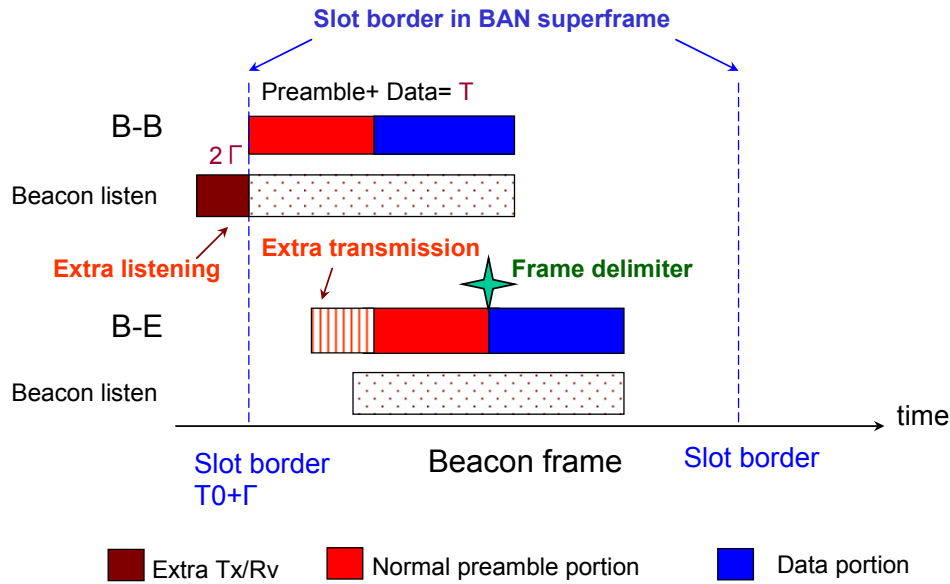
Fig. 12 Power efficient beacon

Table III Beacon broadcast comparison

	B-B	B-E
Beacon preamble	Constant preamble length	Variable preamble length
Listen of beacon preamble	Wakeup before the beacon	Wakeup during the beacon preamble
Slot boundary	At the beginning of beacon	At the frame delimiter or with a constant delay
Maximal device sleeping time	No limitation	Be limited by slot duration, frame delimiter and clock accuracy
Beacon payload	No limitation	No limitation
Power	More power to listen at device	More power to transmit at coordinator

4.2 Wakeup radio assisted BAN

Wakeup radio is useful for very low duty cycle applications and emergency communications. Typically the wakeup radio works in a different frequency band from the main radio. And the operation power, particularly the reception power of wankup radio, is much lower than that of the main radio. The wakeup radio can be used for a device to wake up its counterpart from the inactive state to normal active state. It can also be used to configure the main radio, e.g. working channel, modulation, data rate etc. This feature is particular useful for MICS systems, which require to scan and work on a clean channel for every communication session. Wakeup radio can be used in both beacon mode and non-beacon mode. In the beacon mode, wakeup radio is to wakeup device to listen to the beacon

As shown in Fig. 13, the communication consists of wakeup session and communication in the wakeup radio assisted systems. The wakeup session can be initiated by the coordinator or the device by setting a timer, or any medical event, etc in the application layer. Fig. 14 lists a frame structure for wakeup radio. The preamble is for amplitude estimation and bit synchronization. The address code is Manchester encoded for improved robustness. The packet can address a single device or a group of devices for broadcast and multicast. An OOK modulation is preferred since the receivers do not need to maintain a clock for reception, which can greatly reduce the power consumption. Fig. 15 shows the protocol how the wakeup radio works in the non-beacon mode.
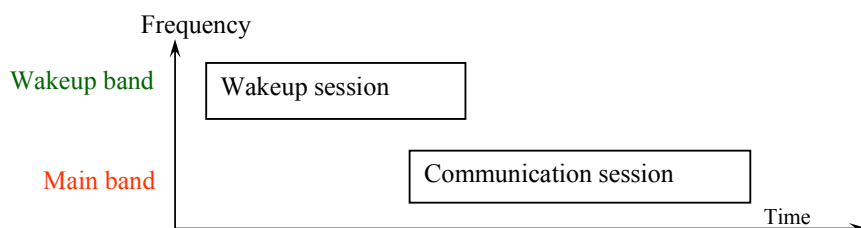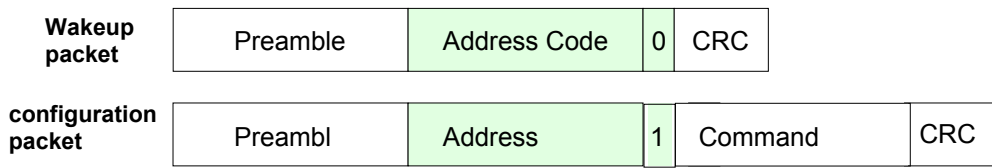
Fig. 13 Wakeup radio assisted system

Wakeup packet	Preamble	Address Code	0	CRC	

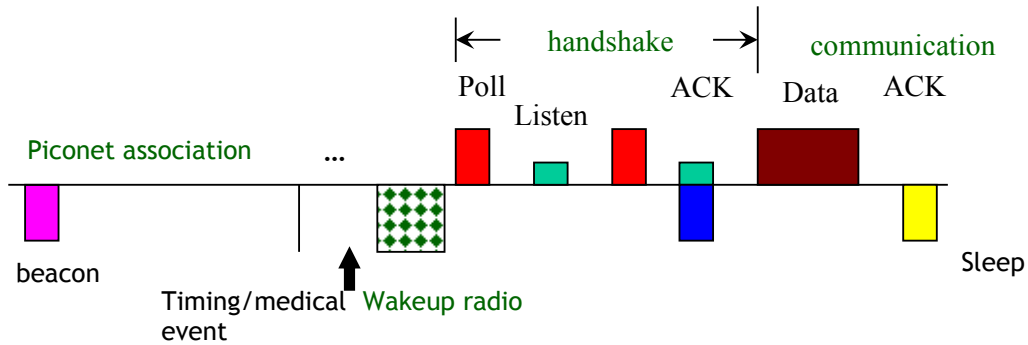| configuration packet	Preambl	Address	1	Command	CRC

Fig. 14 Frame format for wakeup radio

Fig. 15 Wakeup radio assisted BAN in the non-beacon mode

5 Interference and coexistence

There are two coexistence issues in the TG6
- coexistence between medical applications and non-medical applications in a BAN piconet
- coexistence among BAN piconets

The first issue is solved by the central control MAC protocol because both medical traffics and non-medical traffics are in the same piconet. The coordinator can control the allocated GTSs in CFP to medical traffics and to non-medical traffics. Alternatively, the coordinator could also create a medical superframe and a non-medical superframe for each application.

The solution to the second issue depends on whether different BAN piconet can cooperate with each other. In the cooperative manner, different BAN picnets are synchronized with a clock.[5] Then all BAN piconets can arrange the active portion of the superframe in the inactive period of the other superframe. If they cannot cooperate with each other, each BAN piconet can perform random time hopping (TH) and frequency hopping (FH) to avoid the worst case of interference. However, on considering the complexity and power consumption, the hopping is at the superframe level. This is shown in Fig. 16.
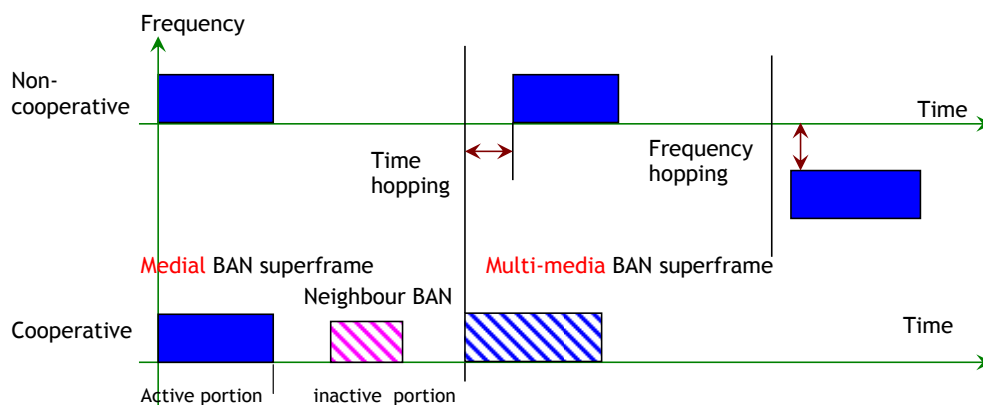

Fig. 16 Coexistence consideration

---

[5] How to get the synchronized clock is another story. The BAN piconet may exchange clock information periodically. Or they may be equipped with another radio to be synchronized.

6. Example system parameters

Example parameters for BAN system are given in Table IV.

Table IV Typical value and range for the system parameters

System parameters		Default value	Range
BAN superframe	Slots	16	16 or 32
	CAP slots	8	8~15
	CFP slots	0	0~7
	Priority slots	1	1 or 2
	ALOHA slot duration	1 ms	1 ~ 8 ms
	Slot duration	2 ms	1~256ms
Max. packet payload			256 or 512 bytes
Beacon duration		1 slot	1~3 slots
Max retries	Category 1 ~ 6	3	3
	Category 7	unlimited	5 ~ unlimited
GTS life time (superframe)		unlimited	2^N (N=0~4), N=7 means unlimited
	Superframe	16	16~256 BAN superframe
	Superframe duty cycle	25% (1:4)	6.66% ~ 100% (1:16)
	Beacon listening	4	0.1% ~ 100%
Non-beacon mode	Poll (non-MICS)	3	2 ~ 10
	Poll (MICS)	20	10 ~ 50

7. Protocol simulation

We have simulated the performance of the proposed beacon mode. BAN system parameters for the simulation are listed in Table V and Table VI. The traffic parameters are in Table VII. A star topology network with 50% superframe duty cycle was considered. The simulation results are given in Fig. 17.

Table V Parameters for MAC protocol

Parameters	Value
Data rate	250 kbps
Slots in BAN superframe	16 , 32
Slot duration	240 symbols
Symbol time	16 µs
PHY Symbols per Octet	2
SIFS	12 symbols
LIFS	40 symbols
Turnaround time	12 symbols
CAP Retries	3
GTS Request command	11 Octets
ACK wait duration (max.)	54 symbols
ACK command	5 Octets
MAC Header	9 Octets
PHY Header	6 Octets

Table VI Parameters for power consumptions

Parameters	Value
Tx power consumption	36.5 mW
Rx power consumption	41.4 mW
Sleep power consumption	42 µW

Table VII Traffic parameters for simulations

Applications	Leads/ Sensors	Traffic load	Payload (bytes)
ECG	2,4,6,8,10,12	4.352 kbps/lead,	68

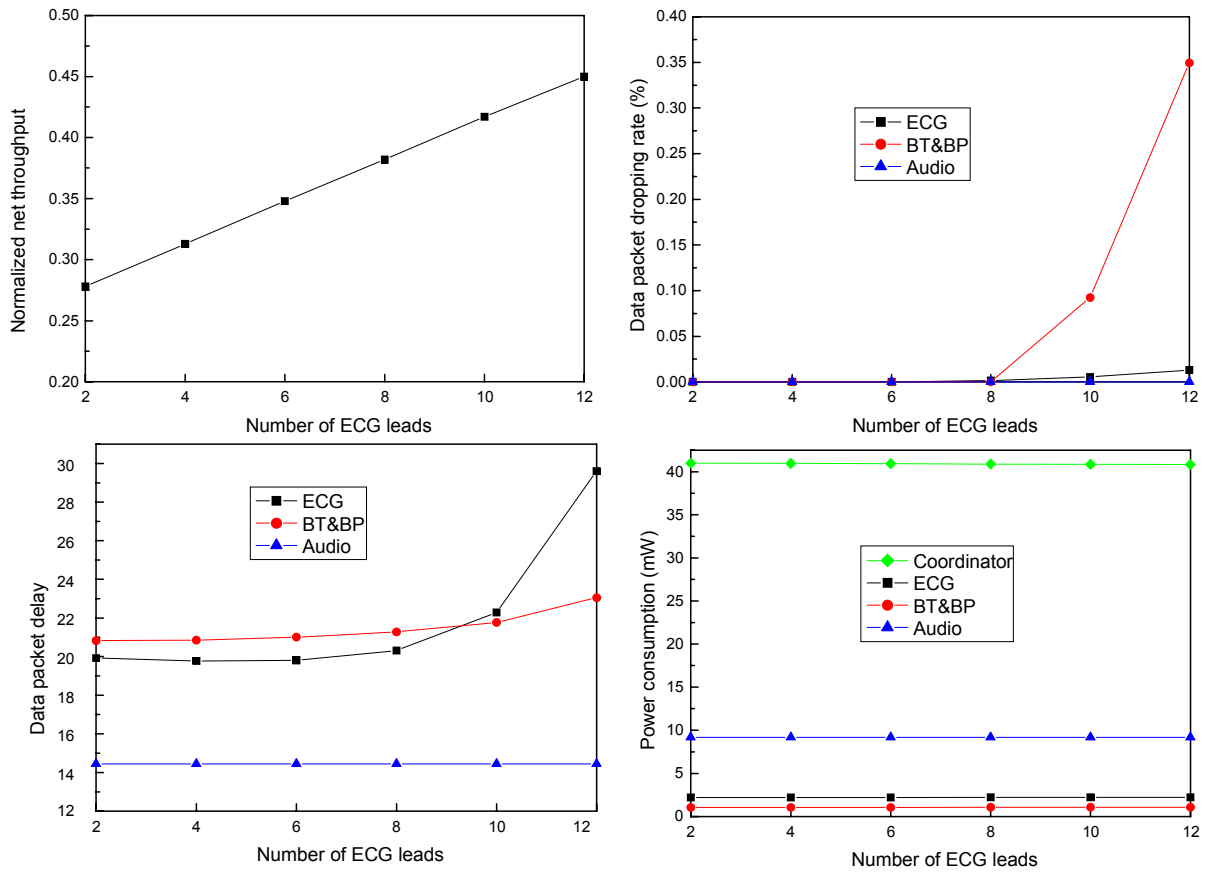|		8 packets/s/lead	
Body temperature (BT)	1	1.6bps, 1packet/5s	1
Blood pressure (BP)	1	3.2bps, 1packet/5s	2
Audio	2	30kbps each	68

Fig. 17 Simulated system performance: normalized net throughput,(a), packet drop rate (b), packet delay (c), and power consumption (d)