4. IEEE 802.15.6のアクセス機構

第一回講座を開設（March/2019）してからからもう1年半以上が経過してしまいました。その間，第二回（May/2019），第三回(Dec./2019)とデータ伝送技術の基本的知識や近年のIP環境での利便性を改善するためのQoSクラスの導入などに関する知見を取得する講座が続きましたが前回までの講座で漸くBANネットワークアクセスについての基本的な知見を得られるところまで到達出来たと感じています。ただ，今回の講座の後半部をよりよく理解するためには物理層の基本技術（具体的にはワイヤレスディジタル変復調技術）やnetwork securityの基本である暗号化に関する知見が必要となりますので読んでくださる方々全員に分かり易い記述とは云えない箇所もあることを了解ください。

それにしてもCOVID-19のパンデミック以来，長期間に渡る様々なリアルな活動が制限され、更に稀に見る酷暑の中で著者も原稿作成の気力を何となく削がれて第四回講座開講がこれほど遅れてしまったことを心苦しく感じています。講座に目を通してくださる技術者の皆様もそれこそ ”Health Care”-firstでお過ごしください。

4.1 ランダム・アクセス手順

4.1.1　slotted ALOHA

slotted　ALOHAプロトコルでは（チャネルアクセスを試みる）ノードは前もって割り当てられているユーザ優先度（User Priorities：UPs）に従ってアクセスを試みます（優先度を規定する表　Table-2　参照：優先度の設定については「第２回技術講座：IEEE 802.11e QoS の項を参照）。表に示してある優先度はノードのアクセス（データトラフィック）優先度の高低(high-, or low-priority)を決めるものです：UPが大きい方が優先度が高い。初期状態で，先ずノードでは表に示されている衝突確率（CP：collision probability）が選ばれてチャネルアクセスの判断をします。ノードではランダムな確率 z：[0,1]が発生されて CPと比較されます。もし、z ≦ CPならば、ノードは競合に勝って割り当てチャネルにデータを送れます。もし、ノードが送信権を得られなかった場合には，CP は変わらないで奇数回失敗のナンバーメモリへ格納され，それに続いてそれを等分（半分に）し偶数回失敗がある場合に備えて偶数回数メモリへ格納しておきます。

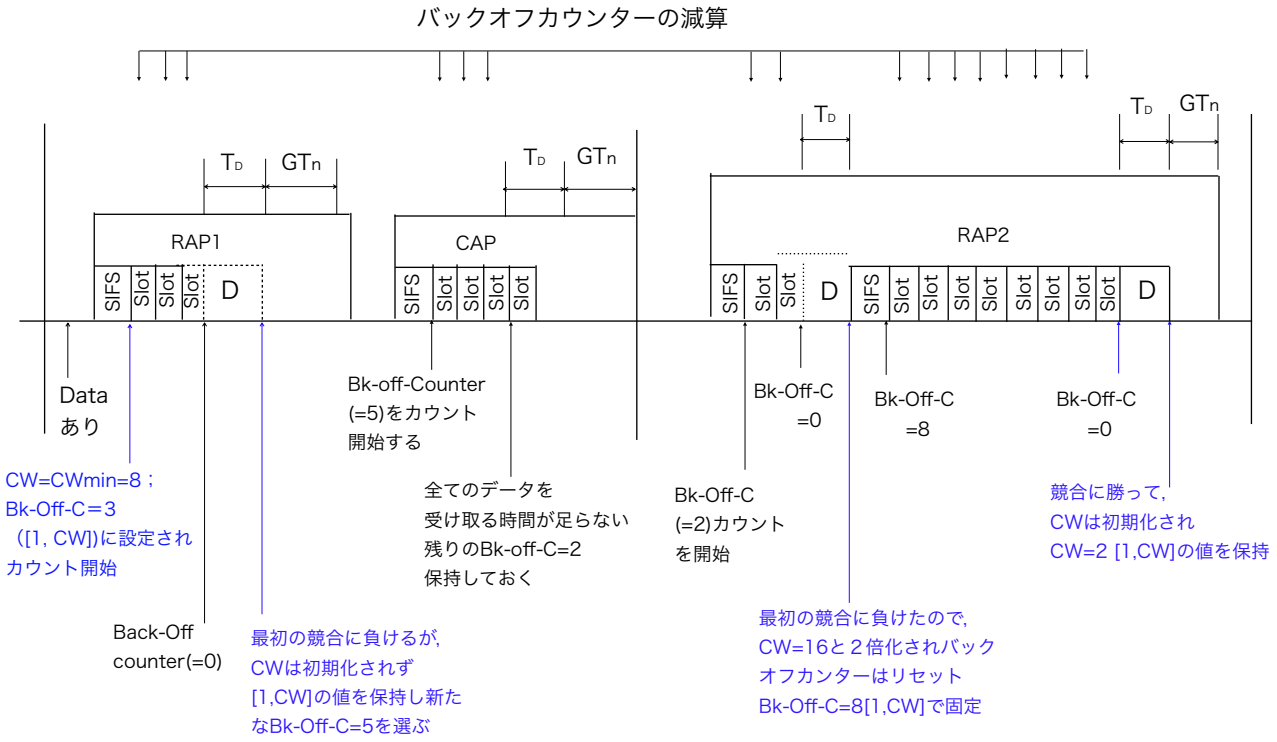
Table 2:	Bounds for	User Priorities Slotted	-ALOHA and CS	MA/CA Protocol
User の優先度	Slotted - ALOHA	Slotted - ALOHA	CSMA/CA	CSMA/CA
	CP_{max}	CP_{min}	CW_{min}	CW_{max}
0	0.125	0.0625	16	64
1	0.125	0.0937	16	32
2	0.25	0.0937	8	32
3	0.25	0.125	8	16
4	0.375	0.125	4	16
5	0.375	0.1875	4	8
6	0.5	0.1875	2	8
7	1	0.25	1	4

表_2 Wireless BANにおけるcontentsの優先度UP(QoS)と規格パラメータ

4.1.2 CSMA/CA プロトコル

CSMA プロトコルでは（アクセスを試みる）ノードは，先ずバックオフカウンターをCW(Contention Window)の範囲 [1，CW]の間から選ばれた任意のランダム数値にセットします：ここでCWは(CW_{mini}，CW_{max})の区間内にある一様分布変数です。CWの範囲はTable_2に示されているようにUP（User Prioritiy)によって異なる範囲に設定されています。UPが高いトラフィックは低いUPのユーザよりCWが小さくチャネルへのアクセスの可能性が高くなるので緊急を要するデータ送信への対応に適しています。（アクセスを試みる）ノードはそれぞれのアイドル状態にある CSMA フレームのバックオフカウンター(Bk-Off-C)（スロット長：Slot）を１づつ減らしてゆきます（第２回技術講座の Back-Off の項参照：本講座 図_Fig.5 参照）。特に当該ノードのあるCSMAのスロットがアイドルであると決定できるのは，CSMAスロットの開始からBk-Off-C(—> 0)までの間でずっとアイドルであった場合です。当該ノードはバックオフカウンターをCSMA スロットの開始から減らしてゆきます。バックオフカウンターがゼロになった時点で（当該）ノードはフレーム（データ）を送信できますが，他のノードがフレームを送信中でビジーな時には，（当該）ノードはチャネルがアイドルになるまでバックオフカウンターをロックして待つことになります（カウントダウンを止めて待つ）。偶

数回の送信に失敗した場合には，CWは２倍にされ最大　CW_{max}　まで伸ばされます。図_Fig.5にCSMA/CAプロトコルの伝送手順例を示しておきます。この図では，RAP1でバックオフカウンターが解放されます（カウントダウンを開始する）が，競合に負けるのでCWは変わらないでそのままの値が保持されます：CWは奇数回の失敗では変更されない規則になっている。それに続いて、CAP区間です：バックオフカウンターは５にセットされます；しかし，実際には（3まで進んだところで）２にロックされ（て止まり、次のRAP2に引き渡され）ますがこれは（改めて設定されていた５と云う数値では）スロットの終わりとCAPの終わりの間の時間がデータ送信フレームと元々設定されているGuard　Time(GTn)　時間を満足するに足らないからです（そのままカウントダウンをすればRAP2の時間に食い込んでしまう）。それに続いて，RAP2区間でバックオフカウンターが解除されます。今回はCWの値は2倍に増やされますが理由はこれまでの競合に２度失敗しているからです（8×2=16：最初RAP1に設定されたCW=8だった）。バックオフカウンターは８にセットされ解除されます（この８は１から１６の間の数の中からプログラムにより偶然選ばれた数値です）。バックオフカウンターがゼロになると、データが送信されCWは改めてCW_{max}にセットされ直されます。

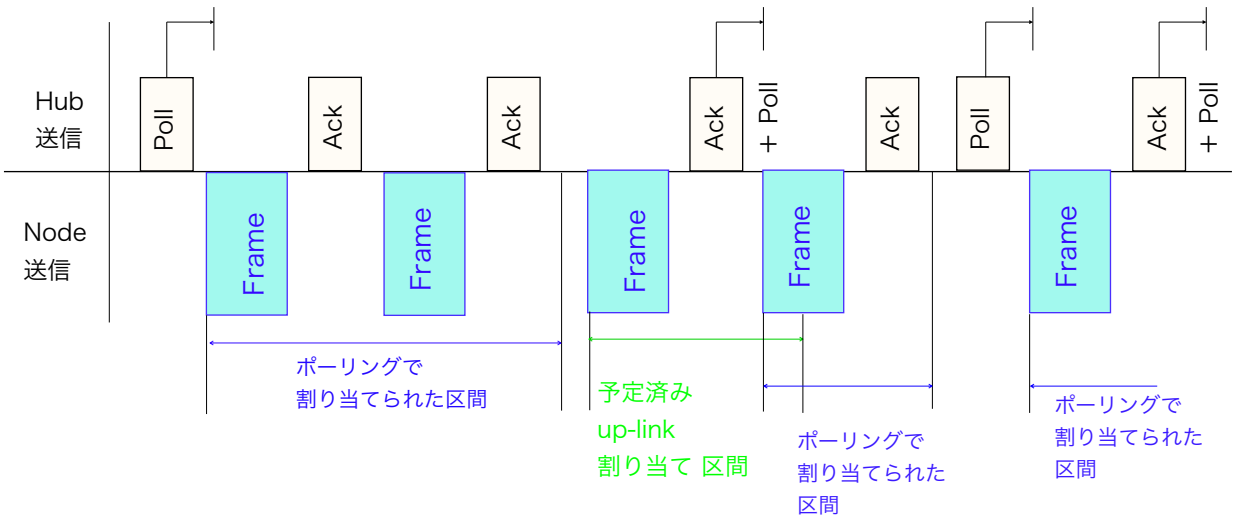


図_Fig. 5　IEEE 802.15.6 CSMA/CA プロトコル：std.準拠アクセス例

図_Fig. 5 中 notation の簡単な解説：slot = CSMA slot, SIFS = Psifs, D = 競合割り当て区分におけるあるノード k によるフレーム処理のための開始時間（例えば，データタイプフレームや Psifs 間隔で出るk - Ack フレームなど），TD = Dを完結するために要する時間，DT_n = 名目上のガードタイム

4.1.3 予約外（即時）アクセス

ハブはスーパーフレーム境界のあるビーコンモードや非ビーコンモードで，前以って予約ししていない場合（緊急割り当て要求）にも接続要求（ポーリングやポスティングコマンド）を送って緊急アクセスを試みることが可能です。この種のコマンドは幾つかのデータフレームを割り当てられたインターバルの外で，ハブやノードが何らかのデータ処理（汎用な術語表現では ”トランズアクション” ）を初期化するのに用いられます。ポーリング信号はノードへの Type I あるいはType II（HARQ）ポーリング割り当てを許可するのに利用されます（どちらのARQ タイプでも利用可）。一方，ポスト信号は特定の相手へ管理フレームを送るのに使われます。Type I ポーリング割り当ては SIFS 時間後スタートし割り当てられたスロット時間の終了とともに終えます：勿論現行のスーパーフレーム内でのことです。同様にType II ポーリング割り当ても SIFS 時間後にスタートし，全てのデータフレームがポーリングノードから送信完了後に終了します。図_Fig.6 に即時ポーリング割り当ての大まかな例を幾つか示しました。



図_Fig. 6 即時ポーリング割り当てのタイミング例

予約外割り込みによるリンク接続要求でも、上りあるいは下りの一方向通信のリンク確立のみでなく双方向のリンク接続で使うことも可能です。フレームの伝送/交換には単一フレームのみで無く複数フレームを連続的に実施することも可能です。これらのデータ交換に関する詳細は省きますが，データ転送頻度の少ないヘルスケア応用などの利用では重要な機能ですので関連分野の方々はIEEE　標準仕様書などで別途知識を得て下さい。

次章ではPHY（物理層）の特性について概要を述べようと思いますが，ネットワーク接続に関する術語の中で ”スーパーフレーム” との記述が使われていましたが，この術語はIEEE　802.15.4（ZigBeeがよく知られているサービス）で使われていますが，他では使われる機会は少ないので馴染みがない方も多いことと思います。

　　Zigbee　が主たるアプリケーション・ネットワークシステムとして知られている　IEEE　802.15.4　std.　に　”スーパーフレーム”　構造が導入されていますが，IEEE　802.15.6では更に一般化された構造に高度化されています。第一回講座で述べた（内容の復習になりますが）ビーコンモードでの各種アクセスフェーズ（EAP, RAP, MAP. CAP）を示したFig.3a には管理ノード（HUB）が周期的に出すビーコンにより配下のデバイス　（node）がアクセスの同期を確立するタイミングの概要が示されています。ビーコン周期の中には最大４個のアクセスフェーズが存在できますが，データ送受信が行われているフェーズで交換されるデータフレームをフレーム（active　frame）と呼んでいます。このようなフェーズの構造からビーコン周期内でactiveなフレーム全体を示す術語として ”スーパーフレーム” が使われています。データの送受信が行われていない区間もありますが，この区間はinactive　phase　と呼ばれHUBは動作を止めておくこもできます。一方，スーパーフレーム境界を有するnonbeaconモードはMAPフェーズでのみ使用可能です。

4.2 IEEE 802.15.6 PHY 物理層規格（PHY Specifications）

IEEE 802.15.6は３つの運用 PHY をサポートしており，それらはUWB PHY, NB PHY及びHBC(Human Body Communications) PHYです。IEEE 802.15.6 の PHY は（ネットワーク無線装置として）以下の３つの機能を備えていなければなりません。即ち，(1) 無線送受信装置電源の ON/OFF 機能，(2) チャネル割り当ての取り消し機能，及び (3) データの送信・受信機能 です。以下では IEEE 802.15.6 のNB, HBC 及び UWB PHYの規格（特性）を紹介してゆきましょう：

4.2.1 NB PHY

4.2.1a 周波数帯域と伝送パラメータ

表_3は規定されてる周波数帯域と対応するPHYパラメータを纏めたものです：無線変調方式としてはDPSK(Differential Phase Shift Keying)が使用されますが：420 – 450MHz では GMSK(Gaussian Minimum Shift Keying)が指定されています。幾つかの帯域では，複数のパラメーターがセットになっていて表_3中色違いの数字（青紫系色）箇所の設定はオプションです：具体的には，変調次数 M (Modulation order：M)：8，及び拡張指数 SF（Spreading Factor）：1 です。この表に基づいて情報データレートを求めると：

$$Rd = \left(\frac{Rs \bullet N}{S} \times \frac{k}{n}\right) \text{ (kbps)} , \qquad (1)$$

ここで，Rsはシンボルレート，Sは拡張指数(Spreading Factor)，k/nはBCHの符号レート，Mは変調次数で $M=2^N$ で与えられます(即ち，$N = \log_2 M$)。

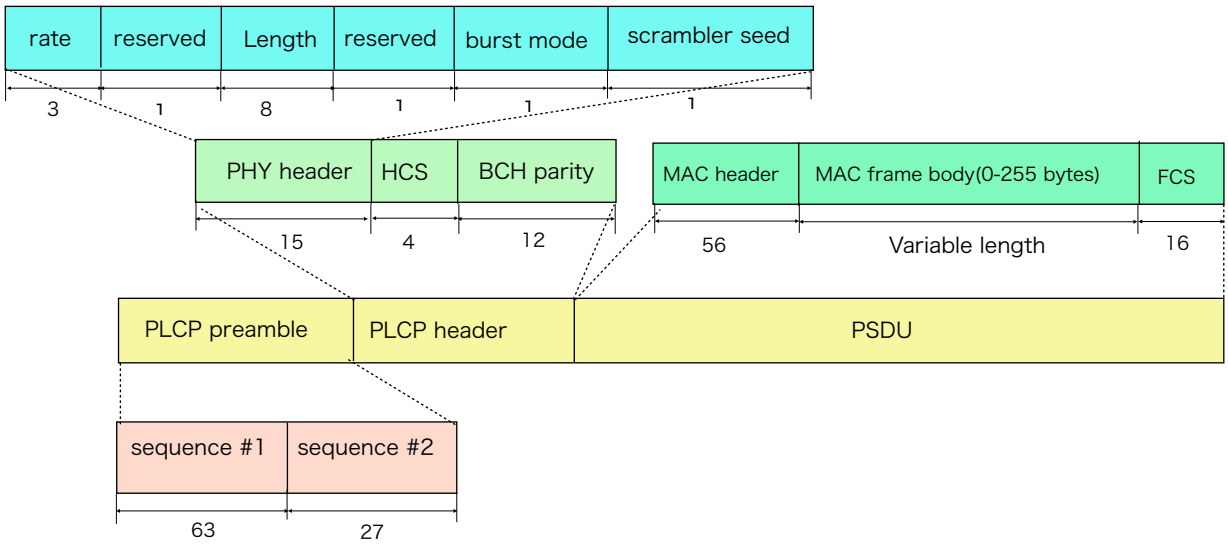
（原稿を書いているcomputerにはMath Type®のような数式作成プログラムがインストールされていないので見辛いのを容赦ください）

周波数帯域	Packet 成分	変調方式	変調次数 (M)	シンボルレート(Rs : kbps)	符号化レート BCH (n, k)	拡張係数 (SF)
402-405 MHz	PLCP header PSDU	π /M-DPSK	2 { 2, 2, 4, 8 }	187.5	(31,19) (63,51)	2 { 2.1.1.1 }
420-450 MHz	PLCP header PSDU	GMSK	2	187.5	(31,19) {(63,51),(63,51), 1 }	2 { 2,1,1 }
863-870 MHZ	PLCP header PSDU	π /M-DPSK	2 { 2, 2, 4, 8 }	250	(31,19) (63,51)	2 { 2.1.1.1 }
902-928 MHz	PLCP header PSDU	π /M-DPSK	2 { 2, 2, 4, 8 }	250	(31,19) (63,51)	2 { 2.1.1.1 }
950-958 MHz	PLCP header PSDU	π /M-DPSK	4 { 2, 2, 4, 8 }	600	(31,19) (63,51)	2 { 2.1.1.1 }
2360-2400 MHz	PLCP header PSDU	π /M-DPSK	4 { 2, 2, 2, 4 }	600	(31,19) (63,51)	4 { 4.2.1.1 }
2400-2483.5 MHz	PLCP header PSDU	π /M-DPSK	2 { 2, 2, 2, 4 }	600	(31,19) (63,51)	4 { 4.2.1.1 }

表_3 Wireless Body Area Network PHY パラメータ

4.2.1b NB PHY PPDUパケットの構成

物理層プロトコルデータユニット（*PPDU:Physical-Layer Protocol Data Unit*）は物理層サービスデータユニット(*PSDU:Physical-Layer Service Data Unit*)をそのフレーム中にカプセル化して幾つかの制御フィールドを付加します：制御フィールドは送受信タイミングの同期を取り，伝送パラメータを相互確認するために使われます。図_Fig.7 にNB PPDU の構成を示してあります。この後の項目で各フィールドの詳細を記しておきます。



図_Fig.7 NB PHY の標準 PPDU 構成

（図中の数値は bit 数を示す）

PLCP プリアンブル；

物理層のプリアンブル構成組み立てプロトコル(PHY Preamble Convergence Protocol) は二つの系列が繋がっていて， 最初の系列は63 bits 長で初期同期と搬送波再生及びパケット検出に使われます。この系列は２つのパターンを有していて：一つは，奇数番号を有するチャネル（の処理）に利用され，もう一方は偶数番号を有するチャネル（の処理）に使われます。第二の系列は27 bitsの固定長を有し，第一の系列に付加されて，高精度タイミング同期に使われます；63 bits は payload の符号化方式 BCH(63, 51)に依存しています。

PLCP ヘッダー；

PLCP headerは複数のフィールドから構成されているが，これは受信機のためのPHYパラメーターを載せていて（PHY headerと呼ばれる），12 bits の parity checkビットが付加されている：(31,19) 短縮化 BCH 符号。このフィールドの詳細構成は：

(1) Rate : 情報ビットレートを数式 (1) を用いて計算して得られたデータレートの指示値を3 bits で表す：この指示値で変調方式，変調次数，符号レート及び拡張係数を表している。

(2) Length: MAC本体の（バイトbyteで表された）長さ（0-255 bytes）の指示値を8 bitsで表す。

(3) Burst mode : バースト伝送の指示値を1 bitで表す。

(4) Scrambler seed : scrambler 中のレジスター register の初期状態を1-bit (seed) で指定する。初期状態=ゼロ（0） に設定され，その後 PHY フレームの伝送毎に反転される。

(5) HCS : Header Check Sequence（これはheaderの誤り検出に使われる）は4-bits のCRC Cyclic Redundancy Check(CRC-4)でありPHY headerの保護に用いられる。

(6) BCH parity check : BCH field はPHY header とHCSの連接を目的として計算され，誤り訂正のために使用される。このcheckにより 2 bitsの誤りまで訂正可能である。

PSDU；

これまでの内容より，PSDUはMAC header, MAC frame本体とFCSから成ることがわかる

4.2.1c 他のNB PHY 特性

その他,

＊ 波形整形（*Pulse Shaping*）

＊ 記号拡張（*Spreading*）

＊ 送信スペクトルマスク(*Transmit Mask*)

＊ パワーオン/パワーオフの時間保持(*Power-on and Power-Off Ramp*)

＊ 受信機感度（*Receiver Sensitivity*）

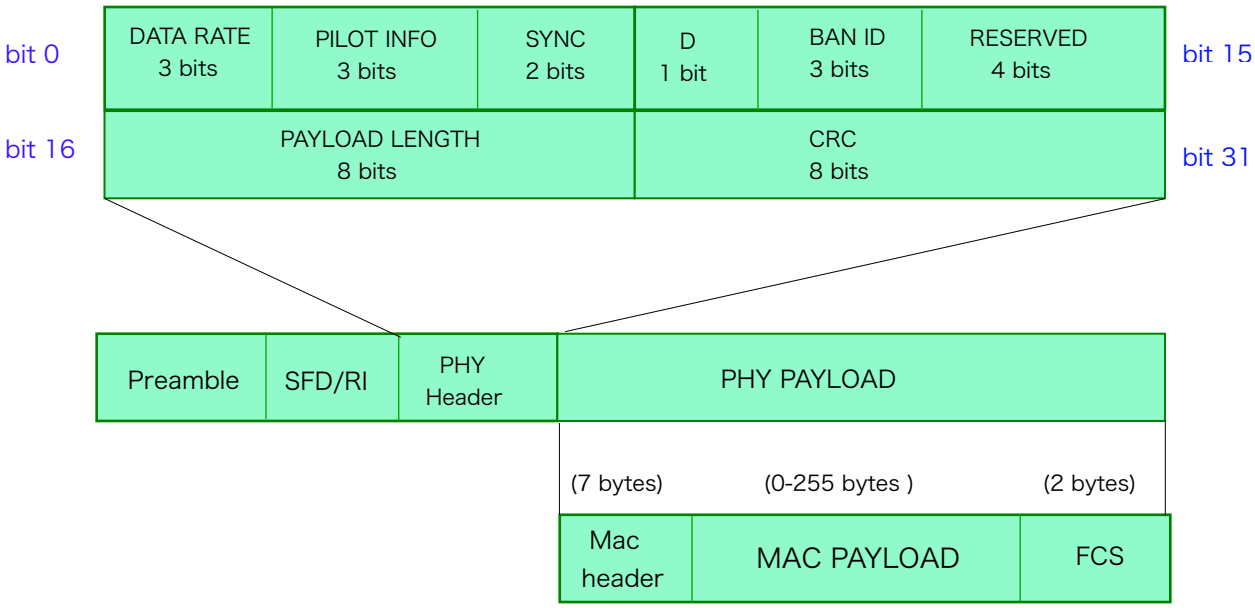
＊　スクランブラー（*Scrambler*）

などの項目についての細部規定がありますが，これらについては省きます。

4.3 HBC PHY 規格特性(*Human Body Communication PHY Specifications*)

HBC PHY は中心周波数 16 MHz及び27 MHzで4 MHz帯域幅の電界強度（base-band）通信技術を使用する。これにより通信装置としてアンテナを必要とせずdigital circuitの後に電極を付けるだけで情報の伝送が可能となります。狭帯域NBC PHYと同様 HBCのパケット構成は，パケットの中に制御ビット；誤り訂正用ビット，及び誤り検出用ビットを付加した後にPSDUをカプセル化します。この構成を図_Fig.8 に示した。以下では，パケット構成を簡単に紹介してゆきます：

(PSDU : Physical-Layer Service Data Unit)



(PPDU: Physical-Layer Protocol Data Unit)

図_Fig.8 HBC_電界強度通信 の PPDU パケット構造

PLCP プリアンブル（*PLCP Preamble*）　；

　初期プリアンブルは 64 or 128-bit gold 符号系列で生成されるが，その後４回繰り返され，最終的に42 Mcps(chip per second)にまで拡散されるよう周波数拡張指数SF=8のFSC (Frequency Shift Code: Walsh 直交系列) で 周波数拡張を実施します。

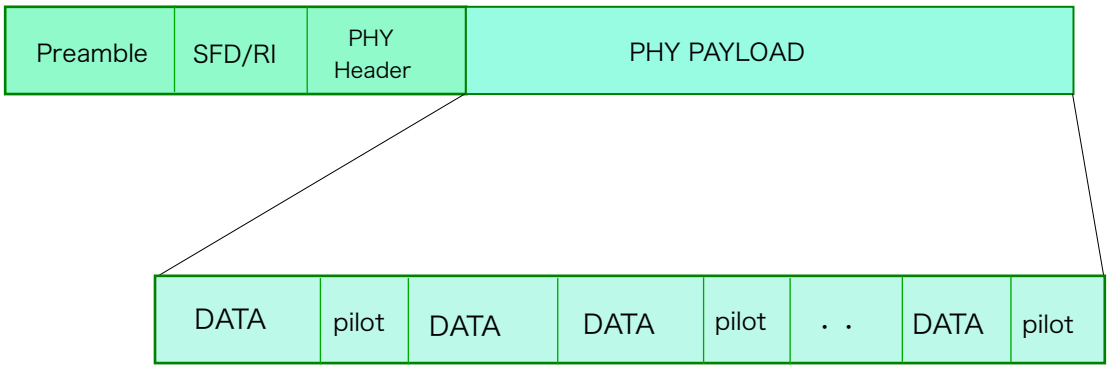
スタート・フレーム・デリッミター(*Start Flame Demiliter*：*SFD*)；SFD はフレームの先頭を示す。その系列はやはり64 or 128-bitのゴールド符号系列発生器で生成されるが，そのゴールド系列は SF = 8 のFSCで拡散されるので，やはりchip rateは42 Mcpsとなる。

データレート指示値(*Rate Indicator*)；SFD/RI field が伝送レートを指示するために利用できる。SFD/RI fieldに指示値がある場合には，受信機はデータレートを決めるために PHY ヘッダーを読み取る必要がない：SFD/RIの構成によりPHY headerの再生必要時間を短縮化できてHBCで高効率伝送を実現することに貢献できます。

PHYヘッダー(*PHY Header*)；PHY ヘッダーは32-bit の系列でレート42 Mcps に拡張されています：即ち，Preamble やSFD/RIと同じチップに拡張されています。PHYヘッダーは図_Fig. 8 に示すfields 等から構成されていますが、そのうちの幾つかは：

(1) Data Rate：式 (1)で計算されたデータレートを3 bits で示す

(2) パイロット情報(Pilot Information)：2 bitsはパイロット信号の挿入区間の長さを示す。パイロット系列（これはSFDと同じである）はPSDUに周期的に挿入されていて，これはビット同期外れを起こさないための処方である。PSDUがパイロット挿入区間より短い場合には（これはshort packetの場合に他ならない）もちろんパイロットは不要である。pilot信号の挿入状況の一例を図_Fig. 9に示しておきました



図_Fig. 9 PSDUへのパイロット(pilot）信号の配置

(PSDU: Physical-Layer Service Data Unit)

(3) CRC-8：CRCの値がPHYヘッダー全体にわたって誤りを検出目的で計算され添付されます

(4) Dフィールド：1:1の専用通信を指定する。D=1にセットされていれば主master 従slave間の通信で専用利用されており，他の従局は指定された従局の通信モードが終了するまで待たなければならない

(5) FS-Spreaderの構成：HBCにおける各種パケットは42 Mcpsに周波数拡張されていますが，この周波数の拡散には元データをS-P 変換したデータ系列をwalsh 直交符号系列を用いて拡張します。拡張係数は最終的に42 Mcpsに拡げた時に与えられる拡張のための指数です。

(6) Sync フィールド：マスター（主）デバイスとスレーブ（従）デバイスの間の同期確立のための情報で：

＊ ”10” は：ダウンリンク全てのフレームに乗っているフレーム同期のための（初期設定された） 同期レジスターを更新するためのフレーム同期要求情報です

＊ ”11” は：（ブロードキャストされる）スーパーフレームに乗っている（初期設定された）スロット及びチップカウンターの同期レジスターを更新するための情報です

(7) スクランブラー(Scrambler) ：PSDUは32 次多項式によるスクランブラーで白色化されます

4.4 UWB(Ultra Wide Band)ネットワークの諸規格

これまで述べてきた２つのPHY規格に比較してUWB PHY は高性能，低複雑性，低消費電力を達成する目的で設定されています。加えて，特性はローバスト（汎用対応）で，MICS(MIC systems)のパワーリミットは諸規制を満たしているます（UWBの利用に関しては当該国における干渉規制が異なるためそれらに準拠しなければなりません。更に，人体への暴露に際して安全なパワーレベルに制限するための規制もあります）。UWB PHY は11チャネルあって，低い方の帯域 3-channel（channel 0-2）と高い方の8-channel（channel 3-10）があリます：ここでchannelの中心周波数は，channel 0では3,494.4 MHzで，channel 10 では9,984 MHz であり，それぞれのchannelの帯域幅は499.2 MHzです。

4.4.1　使用可能送信装置と利用可能モード

PHYではImpulse Radio UWB(IR-UWB) 方式と広帯域周波数変調(wide-band Frequency Modulation) UWB(FM-UWB)方式が利用可能です。HUBはこれらの技術のうちの一つのみを装着化できるが，デバイスには IR-UWB かFM-UWBの一方，あるいは両方式を，搭載可能です。更に，UWB PHY は以下に挙げる二つのモードで運用可能です：具体的には，デフォールト・モード（初期設定）及び高 QoS モードがありますが，後者の高 QoS モードは高優先度の医療応用向けに設計仕様されています。デフォールト・モード（初期設定）は医療用でも非医療応用いずれにでも利用できます。

4.4.2 複数ネットワーク共存のためのIR-UWBのシンボル構成

シンボル時間長 T_{symbol} はパルスシンボル波形位置の数 N_w で決まります（ここで各位置パルスは継続長 T_w を有しているとします：このパラメータを今後参照することは無いと思いますが思考の便宜にと挙げておきます）。DPSK（B-DPSKとQ-DPSK がある）とON-OFF keyingでは，それぞれ $(N_w - 1)$ 及び$((N_w/2) - 1)$ 個のパルス波形位置が時間ホッピングの目的で使用されます。これにより，UWB - PHYは複数-BANネットワークの共存を実現しています。

4.4.3 UWB PHY フレーム

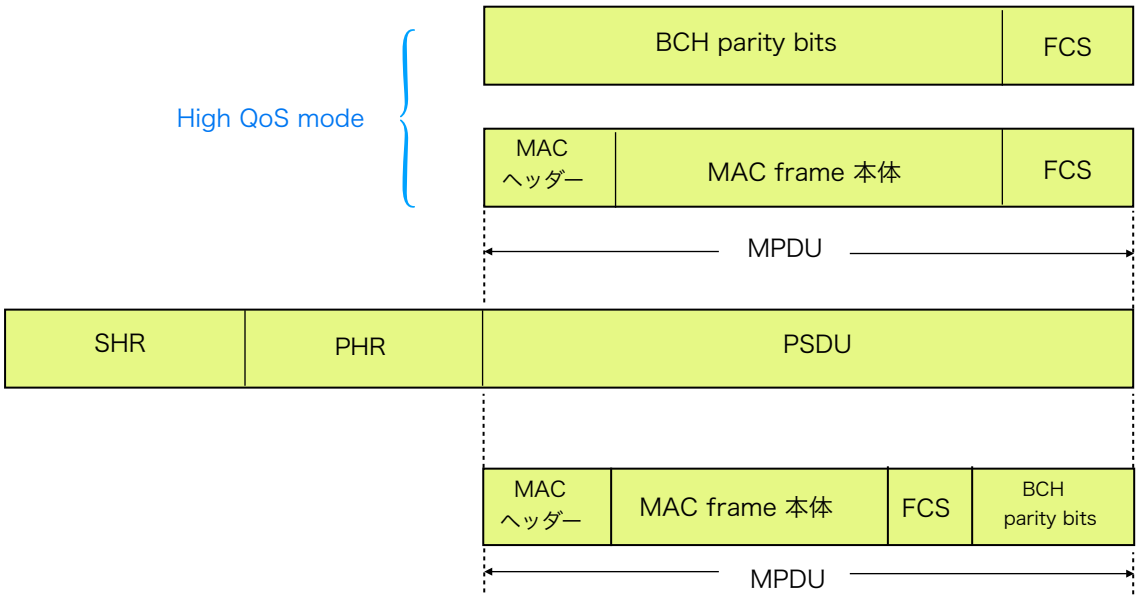
UWB flame の PPDU(Physical-layer Packet Data Unit）は同期確立のための同期ヘッダー(Synchronization Header: SHR)と物理層ヘッダー(Physical-layer Header: PHR)及び PSDU(physical-layer Service Data Unit) より成る。

PSDU: 図_Fig.10に示したように，PSDUは運用モードによって異なる。デフォールトモード（初期設定）ではPSDUはMAC Protocol Data Unit (MPDU)とBCHパリティビットの連接になっているが，high QoSモードでの運用ではMPDUかあるいはBCHパリティビットのいずれかで構成されている。MPDUのデータビットはデータ系列をランダム化するためにスクランブル化，ブロック符号化され，最終的にPSDU伝送のためビット交錯される。

BCH 符号器(BCH Encoder)；初期設定(default)モードではBCH (63,51) が high QoS モードでは BCH (126,63) が用いられる。 BCH (126, 63) はこ

の後説明するH-ARQ (hybrid ARQ) の利用に伴い使われるものである（再送時処理：第３回講座 3.2.2 Type II Hybrid ARQ も参照）。

ビット交錯 (Bit Interleaving)：インターリービングは誤り伝搬の悪影響を避け，データ伝送における頑健さを達成するために導入される：言い換えれば受信機で集中的に発生する複数ビット誤り (Burst Error) の発生を抑えるためである。一定サイズの単純マトリックス型インターリーバーが使われる。



図_Fig. 10　UWB PHY PPDUフレーム構成

4. 4. 4　物理ヘッダー(PHR)構成

図_Fig.11に示した24個のPHRデータフィールドはBCH (40, 28)で符号化される前に4-bitのCRC-4 ITU誤り検出チェックビットが加えられ，最終的にPPDUに送り込まれます。以下，幾つかのデータフィールドの簡単な説明を記しておきます。

データレート (R_0 - R_2)：これらの３ビットはデータレート，シンボル継続長，BCH符号化レート，その他の変調に関したパラメータを規定している。IR-UWBでは，ON-OFF keying の場合には5組のパラメータが定義されていて，一方，任意の差動化変調方式の場合には8組のパラメータが定義

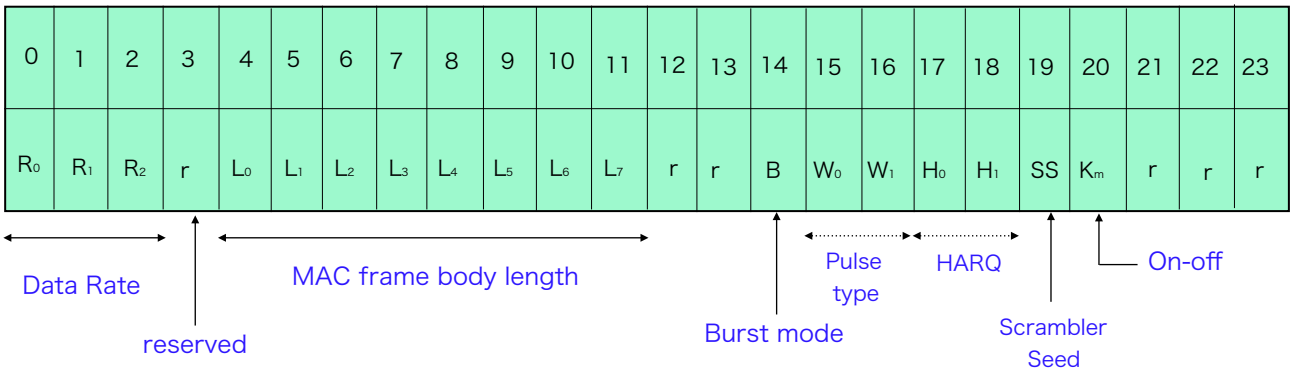
されている。FM-UWBの場合には単一のデータタイプのみが（３ビットをゼロにし，他のオプションをリザーブして）定義される。

パルス波形(W_0 - W_1)： UWB PHYは３種類のパルス波形を支える：これらはチャープパルス波形，カオス波形(Chaotic pulse)，ショートパルス波形です。残ったオプションはW_0 = W_1 =1で，これはリザーブされている。

ハイブリッド ARQ(H_0 - H_1)：Hybrid ARQは（第３回講座で説明したように）伝送データに誤りが発生した場合に複数回の誤り訂正再送を許可する伝送方式です。UWB PHYでの最大再送回数は４回である。初期設定モード(default mode)ではBCH パリティビットが（HARQ無しで）MPDU フレームに付加される。それに対して高 QoS モードでは，送信機では組織データ(systematic data：MAC ヘッダー＋MAC フレーム本体，で構成されている) C_dを（データ系列と同一長の）パリティ系列 q を得る目的で符号化する（具体的内容は invertible code のparity を求める）。送信機では C_dとq 両方の系列を保持しておく。最初に，C_dとBCH FCSとが組み合わされてPSDUが送信される。誤りが発生し，ACKが返されなければ，今度は q が BCH FCS に付加されて再送信される。受信機ではC_d とq の両方がオリジナルデータをBCH 復号により復元するために用いられる。この過程は復号が完了するまでかあるいは最大再送信回数に達するまで繰り返される。この伝送アルゴリズムの内容指示のために (H_0, H_1) = (0, 0)，(1, 0)，(0, 1)，(1, 1) が載っている。これらの意味するところは，(1, 1) = HARQ disabled(default mode)，(0, 0) = C_dとq にBCH 符号化が適用済み：どちらもparityがregisterに載っている：誤りが発生した場合の準備が整っている：最初のデータ送信にHARQ利用可を送る，(0, 1) = C_dを送信している，(1, 0) = C_dとq を送っている，である。(C_d とq 表示については第３回講座の表記を参照してみて下さい)

スクランブラー情報 SS：スクランブラーのレジスター初期状態設定ビットであり，”0” か “1” いずれかである。

ON-OFF 変調での記号配置図(Constellation Mapper) ：$K_m = 0$と$K_m = 1$があり，それぞれ16-値 (16-ary: option) 及 び2-直(binary: mandatory)波形である。



図_Fig.11 PHR フレーム構成

4.4.5 同期用ヘッダー：*SHR*

SHRはプリアンブル及びSFD (Start-of-Flame-Delimiter)から構成されていて，前者はタイミング同期，パケット検出，搬送波周波数オフセット再生を受け持ち，後者はフレーム同期に利用される。

プリアンブル(Preamble)：プリアンブルには系列長 63の嵩系列が使われていて，８系列が利用できる。最初の４系列は奇数番号を有する物理-チャネルで使われ，後りの４系列は偶数番の物理チャネル番号で使用可能である。制御局(coordinator)は最小の受信機電力で同期可能なプリアンブル系列を使う。

フレーム・スタート識別子 SFD (Start-of-Flame-Delimiter)：SFDは嵩系列の反転系列です(0 -> 1, 1 -> 0)。この符号選択によりFSDとpreambleの間の相関を最小にできるので，SFDの検出が一層正確になる。

4.5 IEEE 802.15.6 の セキュリティ

IEEE 802.15.6 は異なるセキュリティ特性（保護レベル及びフレーム形式）について３つのセキュリティ・レベルをサポートしています。

非保護レベル(Unsecured Communication Level)：このセキュリティレベルは最も低レベルの安全性しか無くてデータは保護なしフレームとして送られる。本レベルではデータの認証(authentication)，フレームの完全性（改竄、データ欠落のある/無し等）(integrity)，承認(confidentiality) など即ち個人情報の保護について何の保証もない。

認証済みレベル(Authentication Level)：これは中間の安全性を保証するレベルである。そこでは送信データは暗号化はされていないがデータの認証はされている。このレベルの安全性では，承認を受けた保証(confidentiality)はなされていない。

認証及び暗号化済みレベル(Authentication and Encryption Level)：これはこのデータ伝送において利用可能な最高のセキュリティレベルであり，認証と暗号化を施されたフレームとしてデータが送られる。このレベルではこれまであげてきた最低レベル，中間レベルのセキュリティで得られなかった全ての課題が応えられている。

これら３つのセキュリティレベルのいづれかがチャネルアクセスのネゴシエーション中（規格では “association process” と表現されています）に選択可能です。シングル・セッション向けセキュア通信に対してはマスタキー（MK）が有効化(activated)されます。その（activateされる）MKは前もって共有化されていても良いので，（共有を設定した場合には）認証のされていないチャネルアクセス・ネゴシエーションでマスターキーが生成されていることもあり得るということです。MK activate に継いでシングル・セッションでは１組の一時鍵(pairwise temporal Key：PTK)が生成されます。マルチキャストのセキュア通信では，グループ向けの一時鍵(groupe temporal key : GTK)が，１対１通信（unicast）で使われた方法で共有化されます。

4.5.1 安全なネットワーク接続と切断手順

: Security Association and Disassociation Procedure

IEEE 802.15.6 セキュリティプロトコルでは一般にDiffie-Hellman 鍵交換暗号

方式が基本的手法ですが，この暗号化は楕円暗号公開鍵方式を採用しています。ネットワークへの接続と切断過程に使われるプライベート鍵はそれぞれ独立で一意の256-bit 整数です（推奨されています）：

：Cipher-Based Message Authentication Codes(CMAC) が Key-Message Authentication Codes(KMAC)とMaster Key(MK)の取得には用いられている。

＊　CMACはブロック暗号に基づくメッセージ認証符号アルゴリズムで，認証及びデータの機密保護に用いられ，（CBC-MACの欠点を修正して）非固定長のメッセージ伝送においてもセキュリティを保証できます。

初期状態としてノードとハブは前もって共有されている鍵を持ってますが，この鍵は（ノードとハブが）安全に接続するための認証手順に必要なものです。当該ノードは，”安全なネットワーク接続フレーム要求”をハブへ送ることでセッションが開始されます。一方ハブは接続手順への ”許可(joining)” か ”中止(aboating)” を返答します。ノードが ”中止” の返答を受け取った場合には，当該接続手順を取りやめます。一方，もし “許可” の返答を受け取ったら前もって共有されているMK鍵は相互間での合意の下で有効化（activate）されノードとハブで（実際に）共有されます：次いで，その共有鍵はPTK(Pairwise Temporal Key)を生成するのに使われます。

一方，

接続の切断（disassociation）手順はノードあるいはハブどちらからでも開始できます。発案側（sender）は ”安全なネットワーク切断フレーム要求”（security disassociation frame request）を送り同時にMK鍵を削除しますがこれは蓄積装置(storage)からPTKを削除することと同一内容になります。受け手側は要求を受け取るとこれまで有効化されていた鍵情報を記憶媒体 (storage) から削除します。

4.5.2　PTKとGTK 手順

上に述べた接続手順を使ってMK(Master Key)を共有した後、ノードまたはハブはPTK(Pairwise Temporal Key)を生成するステップへと進みます。当該ノード（あるいはハブ）はハブ（あるいはノード）へPTKフレーム要求を送ります。相手側（受信者）はフレームペイロードにあるPTK フィールドを使って ”join”か”abort” で意志を示します。送信側は ”否定” の返答を受けたら当該手順を止め，”受諾”の

回答ならばPTK フレーム要求を受け側へ送ります。２つ目のPTK要求は，フレームペイロードの中にあるPTKフィールドの認証が完了した後にのみ送られます。２つ目のPTK要求が受信できると送信者と相手側（受信者）は新たなPTKを発生します。GTK(Groupe Temporal Key)はPTKを用いてノード間で分配され，ハブがGTKを多数ユーザ間秘匿通信に参加（データ送信）希望のユーザへ配布します。

4.5.3 メッセージの安全性

通信でのフレームは保護（secured）モードあるいは非保護（unsecured）モードのいづれでも送信可能です。セキュリティを求めないノードはビーコンを含め全てのフレームをセキュリティ情報を評価しないで受け入れます。保護モードでのフレームは認証を受けた後，更に暗号化あるいは復号化(decrytped)されますが，これにはAES-128 Counter(CCM)が使われます。13-octet ノンス（nonce：“ナンス”と原語発音通りに記されることもあります） が 個別のCCMフレームの認証と暗号化/復号化(encryption or decryption) に必要です。

　当該フレームが新規のPTKあるいはGTKで秘匿されている場合には，Low-order Security Sequence Number（低次 セキュリティ・シークエンス番号）（LSSN）はゼロにセットされますが，そのフレームが直前のフレームが再送されたものである場合には＋１加算されます。当該フレームが PTK で秘匿されている場合にはHigh-order Security Sequence Number（HSSN：高次セキュリティシークエンス番号）がゼロにセットされます。もし最新のSSNフレーム番号が最後に受け取ったSSNフレーム番号より小さい場合にはHSSNが＋１加算されます。

5. BANシステム設計にあたって

これまでIEEE 802.15.6 Wireless BAN標準のMAC（Media Access Control：媒体アクセス制御）について諸特性を紹介してきましたが，標準化された内容には多くの自由度が残されています。基本的なシステム分類としてはNBC，HBC，及びUWBの３応用分野が規定されていますが，実際のシステム設計に際しては各応用分野内においても利用シチュエーションでそこでの特性がシステム設計に関するパラメータに大きく影響します。その場合，設計で最も大きく影響するのは：

＊電波伝搬環境

です。無線を通信媒体として利用するシステムの全てにおいて電波電波伝搬特性の把握は不可欠です。特にIEEE 802.15.6で規定対象としているMeadical&Health分野では：

＊電力消費の軽減
と

＊データ欠落の回避

はシステム設計の重点課題と言えます。IEEE 802.15.1標準に準拠するBluetooth Low Energy（LE）などの規定により適用領域を広めている実例もあるように，WBANのシステム設計でも電力消費量を少しでも減らす工夫が必要です。

これらについてMACレベル制御で考慮すべきところは多様な点に渡って存在しますがここでは以下に示す２点を挙げておきましょう：

＊再送手順(retransmission procedure)

＊誤り制御(error control)

これら二つに関する選択肢は独立なパラメータから選ばれるのではのではなくお互い密接な関係にありますが，項目としては分けて挙げておきます。理由は，既に述べたようにビーコンモードでのEAP, RAP, MAPフェーズ，及び非ビーコンモード等多くのアクセスフェーズがありそれらによりデータ伝送手順の好ましい条件は異なることに依ります。また，Slotted ALOHAのようにアクセスタイミングが指定されているスケジュールモードでのチャネルアクセスと非スケジュールモードでの割り込みアクセスなど多種多様なアクセスが可能で，更にデータカテゴリによるQoS制御を受けるデータの再送可能/再送不可などの課題もあります。これらの多くの課題を取り上げることは本講座の範囲外と思いますので，幾つかの研究報告を以下に挙げておきます。アクセスフェーズによる伝送効率に関する特性評価を必要とする方はこれらを参考にして下さい。

6. IEEE 802.15.6 MAC 評価に関する幾つかの参考文献

＊ Athanassios Boulis, David Smith, Dino Miniutti, Lavy Libman and Yuriy Tselishchev,

“Challenges in Body Area Networks for Healthcare: The MAC”, IEEE Communications Magazine, Special Issue for Communications in Ubiquitous Healthcare, pp.100-106(May 2012).

＊Hend Fourati, Hanen Idoudi, Thierry Val, Adrien Van Den Bossche and Leila Azzouz Saidane, “Performance evaluation of IEEE 802.15.6 CSMA/CA-based CANet WBAN”, Open Archive Toulouse Archive Ouverte(OATAO), cited from 12th International Conference on Computer Systems and Applications(AICCSA 2016), 17 November 2015(Marrakech, Morocco).

次の文献は Wireless BANへの誤り制御適用に関する網羅的 review で非常に多くの研究者による成果を紹介しています。

＊Rajan Kadel, Nahina Islam, Khandakr Ahmed and Sharly J. Halder, “Opportunities and Challenges for Error Correction Scheme for Wireless Body Area Network-A Survey”, Journal of Sensor and Actuator Networks (JSAN), Vol.8 Issue 1(March 2019).

その他，IEEE 関連研究論文へのIEEE HPからのアクセスはIEEE society 会員IDを有する者に限られているのでここでは挙げてありません。

第４回 技術講座あとがき：

第４回技術講座の原稿を書き始めたのは年々過ごすのが大変になっている酷暑の真っ最中でしたがもう2020年も余すところ25日ほどになってしまい冷気が街に満ちる季節になってしまいました。20ページの草稿を進めるのに半年掛かったことになりますが新型コロナと暑さに気力を奪われてしまった結果です。この間COVID-19 の感染拡大が第３期到来と危惧されていますが，このような状況改善のためにもWBANネットワークを利用した安全・安心ヘルスケアから医院・病院内システム構築提案が各所の技術開発者からなされれば嬉しいと感じています。世界的にはまだまだ IEEE 802.15.6 std.をimplimentした実際のネットワークシステム運用は殆ど開発されていないと思われます。これは当該 std.の包括性にもあると思われますが，技術のイノベーションは急激なので今後の deploying に期待しています。