■4 群（モバイル・無線）-5 編（モバイル IP，アドホックネットワーク）

3 章 センサネットワーク

（執筆者：阪田史郎）［2010 年 5 月 受領］

■概要■

センサネットワークは，ユビキタスネットワーク社会実現のため一要素として，コンテキストアウェアネス（状況認識）の中核機能を提供する．有線，無線を含めセンサネットワークの研究は，軍事研究を主体に 1980 年代初頭に端を発する．しかし，2000 年代初頭までのセンサネットワークは有線に限られたため，ネットワークの設置が困難であるだけでなく，接続センサ数も少なく利用範囲が限定されていた．このため，無線センサネットワークへの期待が大きくなり，1990 年代年末以降，研究が急速に活発化している．センサネットワークを構成するノードは通常，電池駆動の場合が多く，小型，低価格化に加え，省電力化が必須機能となる．更に，コンテキストに対応するセンサデータについては，そのコンテンツによる制御・管理やセキュリティ保証なども重要となる．

2002 年頃からセンサネットワークに関して物理層からアプリケーション層に至るプロトコルの標準化の議論が活発化し，ZigBee がネットワークの有力候補となり，工場などで徐々に利用が始まりつつある．2009 年以降は，スマートグリッドの末端ネットワーク（ホームネットワーク）としても重要視されつつある．

センサネットワークの応用分野は，防犯・防災，環境保全，健康・医療，家電機器の保守，農場での栽培制御，遠隔検針など公共的な利用から家庭・個人レベルの至る極めて広い範囲にわたり，その新たな産業振興，経済への効果も大きいことが予想され，今後の更なる技術開発が期待される．

【本章の構成】

本章では，センサネットワークの概要（動作概要，構成要素，技術課題）（3-1 節），センサネットワークのプラットフォーム（3-2 節），センサネットワークのプロトコル（3-3 節），センサデータの管理（3-4 節），センサネットワークのセキュリティ（3-5 節），センサネットワークの応用（3-6 節），センサネットワーク標準化例（3-7 節）について述べる．

■4群 － 5編 － 3章

3-1 センサネットワークの概要

（戸辺義人）［2008年7月 受領］

本節ではセンサネットワークの概要について，その背景，構成要素，技術課題などについて述べる．

3-1-1 センサネットワークとは

センサネットワークとは，センサをネットワークで相互に接続することにより多地点のセンシング情報を収集し，利活用するためのシステム，あるいはその通信路としてのネットワークを指す．従来から工場の生産ラインなどでネットワーク化されたセンサ群は利用されてきていたが，工場の生産ラインでは最終的にはモータなどのアクチュエータを制御するための入力信号としてセンサ群があったのに対し，「情報を収集」するところに力点があるのがセンサネットワークの特徴である．応用も工場の生産ラインを離れて，日常生活に密着した領域から地球規模に至るまで多岐にわたって想定されている．

広義にはネットワーク化されたセンサ群でセンサネットワークが定義できるが，狭義には，無線通信，センサと通信が一体化したノード，更には小型化ノードにより特徴づけられる．この狭義のセンサネットワークの初期の研究として，カリフォルニア大学バークレー校で1990 年代後半に研究プロジェクトとして実施されたスマートダストがあげられる．MEMS（Micro Electro Mechanical System），センサ，無線通信技術を集約したものとして，自律的なネットワークを構築することが可能な，「賢い塵」たる超小型センサチップの実現を目指したものである．これら賢い塵を上空から数多く散布することで，軍事や環境測定目的のモニタリングをするというのが想定される応用である．各々のセンサノードが，自律的にネットワークを構成し，アドホックネットワーク同様のマルチホップ転送によって，センシングしたデータを伝える．情報収集点（シンク）を設けることで，センサノードのある領域全体の情報を収集できる．ネットワーク拡張性（スケーラビリティ）をもたせるために，スマートダストのように一面フラットに平等に通信を行うのではなくて，要所要所に通信及び計算処理能力の高いノードを置く，階層的ネットワークなどの発展例がある．

一方で，ユビタキスコンピューティングに端を発するアプローチがある．日常生活空間に存在する人と物が相互に協調動作し，コンピュータを操作するという意識なしに，コンピュータで強化された空間を作ることを目的としている．センサはこのユビキタスコンピューティング環境を実現する情報収集口として必要となる．このアプローチでは，センサノード数やネットワークの規模に重きは置かれない．スマートダストがインフラ志向の究極の姿であるとするなら，ユビキタスコンピューティング環境内でのセンサシステムの究極は，送信センサノード1個と受信情報収集ノード1個からなるシステムとなる．

実際のセンサネットワークは，この二つの究極の間に位置し，応用の要求条件に合わせてシステムが構築される．以上の観点で，センサネットワークを規模の観点から**図 3･1** のように分類される．人体に装着するか，人が手にする小型機器にセンサが付与され，人体周辺でネットワークが閉じるものを BAN とすると，センシング情報が人体を超えて，周辺にある機器と協調をすると PAN となる．更に，センサ情報が宅内，オフィス，ビルの中で行き来す

ると，生活空間規模ネットワークとなり，屋外で街の中，森林，農地などで広域に渡ってセンシングする地域ネットワークとなる．世界規模でセンシングデータの集合体を作るネットワークも構築が可能で，このようなシステムは，ネットワークというよりもデータベースという色彩が強くなる．

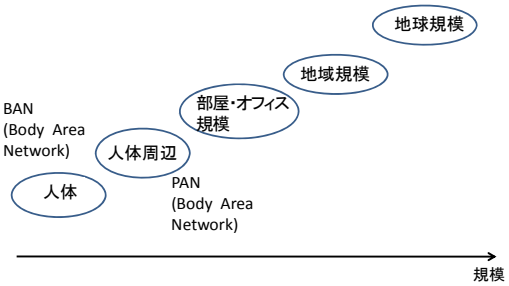


図 3・1　センサネットワークの規模による分類

3-1-2 センサネットワークの構成要素

センサネットワークを構成する要素しては，センサデバイス（詳細は 3-2 節 センサネットワークのプラットフォーム），ネットワーク（詳細は 3-3 節 センサネットワークプロトコル），センサデータ処理（詳細は 3-4 節 データ管理）などがあげられる．

センサデバイスの開発では，すべてを LSI 化する試みが行われている．例えば，Dust Networks 社はアンテナと電源部分を除いて，センサ及び無線回路部分を LSI 化した．小型 LSI 化を追求するのは，動く人に装着したり，建物に埋め込んだりする場合には有効であるが，多くの場合，小型基板実装で十分である．現在国内外で開発されているのはこのタイプであり，例として米 Crossbow 社の Mica Mote や独 Particle Computer 社の uPart，東京大学の U3 や ANTH などがあげられる．

ネットワークプロトコルとして，マルチホップ通信を実現するためのモバイルアドホックネットワークに由来するプロトコルや，センサデバイスの省電力性を考慮したプロトコルなどが存在する．MAC（Media Access Control）プロトコルでは，コンテンションベースのものと TDMA（Time Division Multiple Access）双方でのプロトコルが開発されている．

センサデータ処理については，センサデータの処理を実現するハードウェア構成や多量のセンサデータの保存方法やそのデータから優位な情報を抽出するデータマイニング方法などの検討事項がある．まず，センサデータの処理を，一つのシンクノードで実現するのか，複数のセンサノードで協調的に分散処理を行うかの選択肢がある．また，データの保存においても，保存するデータの量を削減するための圧縮技術が開発されている．センサネットワーク全体をデータベースと見なし，センサネットワークがデータを中心とする点に着目したクエリー・応答を考慮した TinyDB もある．

3-1-3 センサネットワークの技術課題

センサネットワークの技術課題として，電源供給，データ解析，セキュリティについて触

れる．

センサネットワークを構成するノードはバッテリー駆動などの有限な電源供給に頼っている場合が多く，電源消費に関する技術の向上は課題になっている．低消費電力技術の一つに，通信部分での工夫により，ノードがデータ送受信をしていなくて，データの受信を待っているアイドルリスニング状態の時間数を減らす方法がある．これらの取り組みは X-MAC や IEEE 802.15.4 などのプロトコル標準化においても考慮されている．通信部の工夫以外にもバッテリー容量の向上や，環境発電（Energy Harvesting）といったセンサノード自ら発電を行う技術の開発も行われている．

センサネットワークにおける性能向上では，処理性能の高速化やネットワーク帯域の広帯域化といった量的技術革新だけでなく，様々なセンサ情報をデータ解析，有効活用することで新たな展開が開けている．例えば，生体情報をヘルスケアに応用したり，環境情報を農業監視に応用するなど，センサデータの処理により有意な情報を抽出する．センサネットワークアプリケーションに応じて，その処理方法を開発しなければならない．

公共空間に置かれるセンサネットワークでは，センサデータのセキュリティが要求される．通常のネットワークと異なるのは，処理プロセッサの能力が低いことと低消費電力を意識した設計が必要とされる点である．MiniSec はメッセージの秘密性，送信者の認証，リープレイ攻撃の保護を提供するネットワーク層のプロトコルである．こうした暗号化以外にも，センサネットワークが LAN，WAN の公共ネットワークとして成熟してくると，コンピュータネットワークが辿ったセキュリティ対策と同じ道を辿ることが考えられる．

■4 群 － 5 編 － 3 章

3-2 センサネットワークのプラットフォーム

3-2-1 ハードウェア

（執筆者：南　正輝）［2008 年 11 月 受領］

ノードのハードウェアは省電力化を目的とした技術が主体となる．**図 3･2** に示すように，センサノードはセンサ，マイクロプロセッサ，通信デバイス，電源の四つの基本的なハードウェアコンポーネントからなる．必要であれば，これに加えてローカライゼーション（Localization，位置決め）とタイミング（Timing，時刻同期）を行うための補助機能が追加される．これらのハードウェアコンポーネントをマイクロプロセッサ上に実装されるソフトウェアにより制御する．

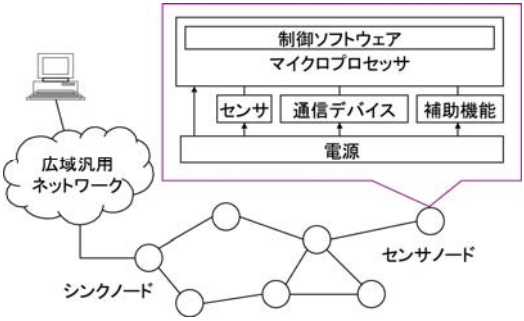


図 3･2　センサネットワークのノード構成

無線センサネットワークでは，無線のもつ自由度を活かすために電源にバッテリーを用いてセンサノードを駆動するのが一般的である．バッテリー駆動のセンサノードの動作時間は，おおよそバッテリーの容量をノードの消費電流で割ることで見積もることができる．一方，センサ，マイクロプロセッサ，無線通信デバイスの各コンポーネントを最大のパフォーマンスで連続的に駆動した場合，コンポーネントの種類にもよるが，ノード全体での消費電力は一般に数十 mA 以上となる．仮に高性能の AAA バッテリーを利用したとしても，連続動作時間を 100 時間確保することは難しい．このため，センサノードを長時間動作させるためには，各コンポーネントに可能な限り省電力なもの選ぶとともに，制御ソフトウェアにより間欠動作させるなどの工夫が必須となる．特に高周波で動作する無線通信デバイスの消費電力が大きく，送信時のみならず受信待機時にも多くの電流を消費する．このため，センサネットワークでは無線通信デバイスの制御が省電力化の観点から重要になり，各種省電力通信プロトコル [1] が提案される背景となっている．

無線センサネットワークにおけるバッテリーの制約を軽減する目的で，発電素子（Energy Harvesting Device あるいは Energy Scavenging Device）や無線電力伝送技術を用いるセンサノード構成も可能である [2), 3)]．発電素子を用いるセンサノードは自然界あるいは住環境に存在する光，熱，振動，電磁場を用い，これを電気二重層キャパシタなどで平滑化して電源とする．具体的には太陽電池，ペルチェ素子，圧電素子，風力発電を用いたり，蛍光灯の漏れ磁束を集めたりすることで電力を得る．発電素子を電源に用いるメリットは発電素子により

十分な電力が確保できればバッテリーの制約から解放され，センサノードの長期連続運用が可能となる点であるが，得られるエネルギーは場所と時間に依存して変動するため，安定動作を確保するための電力管理が難しくなる問題がある．無線電力伝送技術を用いたセンサノード構成では，マイクロ波電力伝送技術や RFID（Radio Frequency Identification）技術などにより，外部からセンサノードへエネルギーを供給するが，長距離化や効率などにまだ課題がある．

センサノードのハードウェア技術は半導体技術の進化とともに機能・性能が向上する．今後はセンサネットワーク専用マイクロプロセッサの開発や高度な信号処理機能の搭載なども進み，開発環境が整備されていくと予想される．

3-2-2 オペレーティングシステム

（執筆者：猿渡俊介）［2008 年 11 月 受領］

ここでは無線センサネットワークにおけるオペレーティングシステムについて，それぞれの研究がどのようなアプローチを採っているかで分類しながら各アプローチの特徴を述べる．

(1) イベントモデル

イベントモデルで構築されたオペレーティングシステムはすべてのタスクをイベントによって起動し，run-to-completion で実行する形態のオペレーティングシステムである．イベントモデルは一つのイベントループと多数のイベントハンドラから構成される．イベントループはイベントの到着を待ち，イベントが届くとイベントに関連付けられているイベントハンドラを実行する．イベントモデルではイベント駆動型プログラミングによってアプリケーションが記述される．イベントハンドラは寿命の短い run-to-completion で記述され，プリエンプションされることがない．つまり，イベントモデルはタスクは関数呼び出しと等価であり，実行ストリームが一つで実現されるため各タスクでローカル変数の領域を共有可能なので省資源かつ低オーバヘッドで並列性を実現できる．また，各タスクが不可分に実行されるので共有資源に対する排他制御が不要となり，安全性が高い．更に，CPU の特殊な機能を用いなくても実装できるので移植性も高い．しかしながら，ユーザが一連の処理を細かい処理に分割しなければならないのでプログラムが書きづらいという問題が発生する．更に，イベントモデルではタスクのプリエンプションをしないことを前提に設計されているのでハードリアルタイム処理のサポートができない．例えば，Kim らは高精度な加速度のサンプリングを一時的にイベントモデルの枠組みを超えて CPU の割り込み内で処理を行うことで実現している [4]．Kim らのアプローチはイベント駆動型の単純さを破壊しているため，他の割り込みを実行できないという問題や，共有資源に対する排他処理の必要性を引き起こす．

無線センサネットワークにおけるイベント駆動型のオペレーティングシステムの研究としては TinyOS [5, 6]，SOS [7]，Contiki [8]，protothreads [9] があげられる．

この中で代表的なものが TinyOS [5] である．TinyOS はカリフォルニア大学バークレー校の SmartDust Project で開発されたオペレーティングシステムである．現在，無線センサネットワークの標準的なオペレーティングシステムとして扱われており，Crossbow 社から発売されている MICA 2 や MICAz [10]，Telos [11]，iMote [12] 上で動作する．TinyOS は CPU の特別な機能を使用せずに実装可能であるため移植性が高く，ATMEL の AVR 128L や Texsus の MSP 430，ARM 7 など様々な CPU に移植されている．

TinyOS では nesC [6] と呼ばれるイベント駆動型の新しい言語で複数のイベントハンドラを一つのモジュールとして設計可能な機能を提供することでイベントモデルのもつプログラムの開発のしづらさを提供している．更に，nesC はイベント駆動型に特化した最適化を行っているので省資源性も実現される．

(2) スレッドモデル

スレッドモデルは複数のスレッドから構成される．各スレッドはそれぞれ独立に実行ストリームをもっており，低い優先度のスレッドは高い優先度のスレッドにプリエンプションされるという特徴をもつ．スレッドモデルではユーザはあたかも CPU を占有しているかのように一連の処理を一つのスレッドとして記述することができるのでプログラムが書きやすい．また，プリエンプションを行うことも想定しているのでハードリアルタイム処理をサポートすることができる．しかしながら，プリエンプション時のオーバヘッドの大きいことや必要とされる資源が多いこと，スレッド間の共有資源へのアクセス制御が必要となるために安全性が損なわれるなどの問題をもっている．

無線センサネットワークにおけるスレッドモデルを用いたオペレーティングシステムの研究としては MANTIS OS [13]，t-kernel [14]，PAVENET OS [15] があげられる．スレッドモデルを用いた研究では，省資源性やオーバヘッドを無視して機能を積極的に拡張していくというスタンスの研究が多い．その中で PAVENET OS は CPU の機能を積極的に利用することで TinyOS [5] と同等の省資源性でスレッドモデルを実現している．

(3) 仮想マシン

仮想マシンとは CPU などの計算資源を仮想化した上でソフトウェアを実現するための仕組みである．機能の少ない CPU を使用することが多い無線センサネットワークでは仮想マシンを用いることで CPU が具備していないメモリ保護機能などを仮想マシンとして実装することが可能であり，プログラムを安全に実行することができる．また，センサノードで動的モジュールを実現する場合，無線センサネットワークに特化した命令セットを具備する仮想マシン上でモジュールを実行することでモジュール自体のサイズを小さくすることができ，モジュール転送に伴う負荷を軽減することが可能となる．更に，仮想マシンを異なる種類の CPU に移植すればモジュールがそのまま使えるので高い移植性も実現できる．

無線センサネットワークにおける仮想マシンの研究としては Mat'e [16], ASVM [17], VM* [18], VAWS [19] があげられる．Mat'e は無線センサネットワーク向けの最初の仮想マシンである [16]．無線センサネットワークに特化した 24 個の命令をもつスタックベースの仮想マシンを構築することで，仮想マシン上で動作するプログラムサイズを小さくすることに成功している．Mat'e の命令セットが固定的だったのに対し，ASVM [17] では仮想マシンをアプリケーションに応じて設計可能な仕組みを導入することでより，よりプログラムサイズを小さく，オーバヘッドを小さくすることを実現している．ASVM の仮想マシンはアプリケーションに応じて作り変えることが可能であるものの，一度，センサノードに仮想マシンを配置した後は拡張ができない．それに対して VM* [18] は付加的に拡張可能な仕組みを実現している．Mat'e，ASVM，VM*がプログラムモジュールの小型化と実行性能の改善に主眼を置いているのに対し，VAWS は仮想マシン上で保護機能を実現しつつハードリアルタイム処理を行うことを目

指している [19].

3-2-3 時刻同期

（執筆者：鈴木　誠）［2008 年 11 月 受領］

センサネットワークは無線センサノードによって構成される分散システムであるため，時間的整合性が要求されるアプリケーションの構築には，何らかの手段によって時刻同期を行わなければならない．例えば，室内において位置依存型サービスを提供するために超音波を利用して位置検出システムを実現する場合には，1 m 程度の精度を実現するためには 3 ms 程度の精度による時刻同期が必要とされる．また，地震観測のような科学的計測へ応用する場合には，複数のセンサノードが取得したセンサデータを比較するために 100 μs 程度の精度による時刻同期が必要とされる．

時刻同期は時間的整合性やセキュリティの実現に向けて必須の技術であるため，これまでにも，電波時計，GPS（Global Positioning System），NTP（Network Time Protocol）といったように時刻同期に関して多くの研究が行われてきた．これらの同期技術は現在でも広く利用されているものの，電源の制約やノードの多様性といった特徴を有する無線センサネットワークにおいては，必ずしも最適な手段とはならない．MAC 層以上のプロトコルをアプリケーションに特化して開発できること，伝搬遅延が小さいといったような無線センサネットワークの特徴を活用することによって，単純な仕組みで高精度な同期を実現可能である．

(1)　既存の時刻同期技術

時刻同期は時刻情報を送信ノードが送信し，受信器においてその時刻情報をもとに時刻合わせを行うことで実現される．時刻同期には以下の二つの誤差要因が存在する．一つ目は無線のマルチパスやインターネットのルータにおける待ち時間など伝搬遅延の揺らぎである．二つ目は伝送信号の歪みによって生じる誤差である．伝送信号が歪むことによって，正しくビットの境目を認識することが不可能となり，変調レートの約 1/100 程度の揺らぎが生じる．これまでの時刻同期技術では，この二つの不定の遅延による影響をいかにして削減するかを課題として進められてきた．

電波時計は伝搬遅延の補正を行わないため誤差は比較的大きいものの，簡単な仕組みで時刻同期を実現できる．日本においても，独立行政法人 情報通信研究機構が福島県大鷹鳥谷及び佐賀県と福岡県の県境の羽金山において送信局を運用しており，この電波を受信して時刻合わせを行うことによって，電波時計の受信器を具備した時計は時刻のずれを自動的に補正することが可能である．ASK によって 1 bps という低速なビットレートによって送信されており，精度は数 10 ms 程度にとどまる．

GPS は人工衛星を使った位置測位技術である．現在，地球の周りを 24～28 個の GPS 衛星が周回しながら，定期的に測位信号を発信している．受信機は，GPS 衛星の発信する測位信号を受け取ることで各衛星の距離を測定し，3 点測位法によって受信機の位置を算出する．この際，四つ以上の衛星を用い，時間まで変数として解くことによって，時刻を得ることが可能である．50 bps の信号を，チップレート 1.023 MHz の DSSS で二次変調を行っていることから，波形の歪みによる同期誤差も小さく，屋外であれば全世界で 1 μs 程度の時刻同期精度を実現している．

NTP はインターネット上でコンピュータ同士が同期を取るためのプロトコルである [20]．イ

ンターネットではルータでの転送待ち時間により，パケットの転送にかかる時間が数 ms から数 100 ms 程度と遅延が大きく変化する．NTP は，この転送時間の揺らぎによる影響を削減するために 2-way の時刻同期を行っており，数 ms 程度の精度での同期を実現している．

電波時計は簡略な仕組みであるため消費電力も低く，また屋内でも利用可能なことから，数 10 ms という同期誤差が許容できれば無線センサネットワークにも適用可能な仕組みである．GPS は，同期誤差は 1 μs 程度と高精度であるものの，消費電力が大きく屋内では利用不可能という特徴からすべてのセンサノードに具備させることは現実的ではない．

(2) センサネットワークのための時刻同期技術

センサネットワークで時刻同期を行う場合，伝搬遅延の揺らぎによる誤差，伝送信号の歪みによる誤差は小さいものの，以下の二つの誤差要因が追加される．一つ目は，計算処理によって生じる誤差である．これは，現在のセンサノードではすべての計算処理を一つの低速な CPU で実行していることに起因する．センサノードの CPU は数 MHz の低速な発振子で駆動されていることから，他のタスクの影響によっては，ms オーダで不定の遅延が生じる．二つ目は，無線のメディアアクセス制御層による遅延の揺らぎである．電波時計や GPS といった電波を固定的に割り当てられたインフラと異なり，無線センサネットワークでは送信のタイミングを予め正確に決定することができない．特に，CSMA 型の MAC プロトコルを利用している場合，通信開始までの待ち時間は他のノードの通信トラヒックに依存する．

このような背景から，RBS（Reference Broadcast Synchronization）[21]，TPSN（Timing-sync Protocol for Sensor Networks）[22]，FTSP（Flooding Time Synchronization Protocol）[23] など，無線センサネットワークのための同期プロトコルが提案されている．

RBS は，送信ノードでの不定の遅延を削除するために，受信ノード間での時刻同期を実現する．具体的には，まず送信ノードが時刻情報を含まない同期パケットを送信する．受信ノードは同期パケットを受信した各ノードにおける時刻を記録し，受信ノード間でその情報を交換することによって時刻同期を実現する．このとき，各ノード間での誤差の分布がガウス分布となることから，ノード数を大きくすることによって，精度の向上が期待できる．しかしながら，通信量が増大していくために消費電力が増えるという欠点がある．RBS を MICA Mote に実装した結果，平均で約 30 μs の精度を実現できると示されている [22]．

TPSN は，NTP と同様に 2-way での同期を行う同期プロトコルである．NTP とは異なり，木構造を作るすべてのノードが時刻情報を提供可能とすることで，高いスケーラビリティを実現している．更に，RBS とは異なり MAC 層においてタイムスタンプを生成することで，MAC 層での遅延による影響を削除している．この結果，RBS の約 2 倍の精度が実現可能であり，時刻同期の精度を 15 μs 程度にまで削減している．

FTSP では，より精度の高いタイムスタンプを生成する仕組みを導入することで，一方向の同期パケットの送信だけで 1 μs という精度での同期を実現している．TPSN が，MAC 層での送信開始時と受信完了時にタイムスタンプを生成していたのに対して，FTSP ではプリアンブルとスタートコードの送信／受信の直後から 1 バイトずつ送信／受信するたびにタイムスタンプを生成する．これらの各バイトの境目ごとに生成したタイムスタンプからそれぞれのバイトの送信時間の理論値との差を取り，理論値との差が最も小さいタイムスタンプを利用することによって，数 10 μs 程度の精度のタイムスタンプから 1.4 μs 程度にまで精度を

高めている．更に，FTSP は一方向で同期可能という性質を利用し，同期パケットのフラッディングによるネットワーク全体の同期も実現できる．FTSP を MICA に実装した結果，TPSN や RBS よりもはるかに精度の高い，約 1 μs の精度の同期が確認されている [23]．

無線センサネットワークのための同期プロトコルとしては，FTSP が通信量，精度ともに優れている．FTSP は単純な仕組みながら精度の高い同期を実現することができ，実際に Countersniper [24] のような発射源同定技術，Golden Gate Bridge における常時微動観測 [4]，火山モニタリング [26] といったアプリケーションにも利用されている．今後は，電波時計，GPS といった既存の時刻同期インフラを援用しつつ，アプリケーションの特徴応じて同期の手段を選択することによって，アプリケーションが構築されると考えられる．

3-2-4 位置同定

（執筆者：南　正輝）［2008 年 11 月 受領］

センサネットワークは時空間依存の情報を取り扱うシステムである．したがって，センサデータがいつどこで取得されたかという情報が付与されないと，そのデータ自体が意味をなさなくなる．すなわち，センサネットワークにおいては取得したセンサデータに位置情報と前述の時刻情報を付与する機構が必要である．また，これに加えて位置情報と時刻情報を利用することで，通信の高効率化や省電力化を図ることも可能である．

位置情報を取得するための最も有力な手段は GPS（Global Positioning System）を含む GNSS（Global Navigation Satellite System）の利用である．GNSS を用いることで全世界で位置情報と時刻情報を取得することができる．また，主に GPS では搬送波位相を用いる測位方式（Carrier Phase GPS）が利用可能であり，ミリメートル単位での測位を行うこともできる．しかしながら，一般に GNSS の受信モジュールは復調回路が複雑であり，消費電力とコストが高くなってしまう問題がある．このため，現状ではセンサノードに直接搭載するのではなく，間接的に利用してノードの位置決めを行う用途に利用されることが多い．受信モジュールを直接センサノードに搭載する場合には間欠的な駆動による省電力化が必要となる．このとき受信モジュールに保存されている衛星などに関する情報の鮮度に応じて測位に要する時間が変わる点には注意を要する．また，GNSS はマルチパス，電離層伝搬遅延，衛星の幾何学的配置などに依存して測位精度が変動するため，特に精密な位置決めを行う場合には誤差要因を十分に考慮する必要がある．

一方，GNSS を用いないセンサネットワーク用の測位方式に関しては屋内・屋外を含め現在様々な研究が行われている段階にある [27), 28), 31), 29)]．

方式的な分類では，受信信号強度（RSSI : Received Signal Strength Indicator）を用いるもの，基準点からの信号の到来時間（あるいは到来時間差）に信号の伝搬速度を乗算して基準点からの距離を求め位置を算出する TOA/TDOA（Time of Arrival/Time Difference of Arrival）方式，基準点からの信号到来角から位置を求める AOA（Angle of Arrival）方式などがある．

測位に用いる信号としては電波，光，音波が主として用いられる．また，この他にも距離測定などを行うことなく，大規模なセンサネットワークの位置を求める方式なども提案されている [30)]．

いずれの場合においても消費電力と測位精度のトレードオフをどの様に解決するかが技術的課題であり，低コスト・低消費電力で高精度かつ安定的に測位可能な実用的なデバイスの登場が待たれる．

■参考文献

1) H. Karl, et al., “Protocols and Architectures of Wireless Sensor Networks,” John Wiley and Sons, Jun. 2005.
2) J. Paradiso, et al., “Energy Scavenging for Mobile andWireless Electronics,” IEEE Pervasive Computing, vol.4, no.1, pp.18-27, Feb. 2005.
3) P. Dutta, et al., “Trio: Enabling Sustainable and Scalable Outdoor Wireless Sensor Network Deployments,” Proc. of the 5th International Conference on Information Processing in Sensor Networks, pp.407-415, Apr. 2006.
4) S. Kim, S. Pakzad, D. Culler, J. Demmel, G. Fenves, S. Glaser, and M. Turon, “Health Monitoring of Civil Infrastructures Using Wireless Sensor Networks,” Proc. of the 6th International Conference on Information Processing in Sensor Networks (IPSN’07), Cambridge, Massachusetts, 2007.
5) J. Hill, R. Szewczyk, A. Woo, S. Hollar, D. Culler and K. Pister, “System Architecture Directions for Networked Sensors,” Proceedings of the 9th International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS’00), Boston, Massachusetts, pp.93-104, 2000.
6) D. Gay, P. Levis and R. von Behren, “The nesC Language: A Holistic Approach to Networked Embedded Systems,” Proceedings of Conference on Programming Language Design and Implementation (PLDI’03), San Diego, California, pp.1-11, 2003.
7) C. C. Han, R. Kumar, R. Shea, E. Kohler and M. B. Srivastava, “A Dynamic Operating System for Sensor Nodes,” Proceedings of the 3rd International Conference on Mobile Systems, Applications, and Services (MobiSys’05), Seattle, Washington, pp.163-176, 2005.
8) A. Dunkels, B. Gronvall and T. Voigt, “Contiki - a Lightweight and Flexible Operating System for Tiny Networked Sensors, ” Proceedings of the 29th Annual IEEE International Conference on Local Computer Networks (LCN’04), Tampa, Florida, pp.455-462, 2004.
9) A. Dunkels, O. Schmidt, T. Voigt and M. Ali, “Protothreads: Simplifying Event-Driven Programming of Memory-Constrained Embedded Systems,” Proceedings of the 4th ACM Conference on Embedded Networked Sensor Systems (SenSys’06), Boulder, Colorado, 2006.
10) J. Hill and D. Culler, “MICA: A Wireless Platform for Deeply Embedded Networks,” IEEE Micro, vol.22, pp.12-24, 2002.
11) J. Polastre, R. Szewczyk and D. Culler, “Telos: enabling ultra-low power wireless research, ” Proceedings of the 4th International Synposium on Information Processing in Sensor Networks (IPSN’05), Los Angels, 2005. poster.
12) L. Nachman, R. Kling, R. Adler, J. Huang and V. Hummel, “The Intel® mote platform: a bluetoothbased sensor network for industrial monitoring,” Proceedings of the 4th International Symposium on Information Processing in Sensor Networks (IPSN’05), Los Angeles, California, 2005.
13) S. Bhatti, J. Carlson, H. Dai, J. Deng, J. Rose, A. Sheth, B. Shucker, C. Gruenwald, A. Torgerson and R. Han, “MANTIS OS: An Embedded Multithreaded Operating System forWireless Micro Sensor Platforms,” ACM Mobile Networks & Applications (MONET), Special Issue onWireless Sensor Networks, vol.10, no.4, pp.563-579, 2005.
14) L. Gu and J. A. Stankovic, “t-kernel: Provide reliable OS support for wireless sensor networks,” Proceedings of the 4th ACM Conference on Embedded Networked Sensor Systems (SenSys’06), Boulder, Colorado, 2006.
15) 猿渡, 鈴木, 水野, 森川, “無線センサノード向けハードリアルタイムオペレーティングシステムの設計,” 情報処学会研究報告, ユビキタスコンピューティングシステム研究会 (UBI-13-29), 2007.
16) P. Levis and D. Culler, “Mat`e: A Tiny Virtual Machine for Sensor Networks,” Proceedings of the 10th International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS’02), San Jose, California, pp.85-95, 2002.
17) P. Levis, D. Gay and D. Culler, “Active sensor networks,” Proceedings of the 2nd Conference on Symposium on Networked Systems Design & Implementation, vol.2, Boston, Massachusetts, pp.343-356, 2005.
18) J. Koshy and R. Pandey: “VM*: A Scalable Runtime Environment for Sensor Networks,” Proceedings of the 3rd ACM Conference on Embedded Network Sensor Systems (SenSys’05), San Diego, California, 2005.
19) 鈴木, 猿渡, 水野, 森川, “VAWS: 無線センサノードのための仮想マシンの性能評価,” 電子情報通信学会総合大会, 2007.
20) D. L. Mills, “Internet time synchronization: the network time protocol,” Global States and Time in Distributed

Systems (Eds. by Z. Yang and T. Marsland), IEEE Computer Society Press, 1994.
21) J. Elson, L. Girod and D. Estrin, “Fine-Grained Network Time Synchronization using Reference Broadcasts,” Proceedings of the 5th Symposium on Operating Systems Design and Implementation (OSDI’02), Boston, Massachusetts, 2002.
22) S. Ganeriwal, R. Kumar and M. B. Srivastava, “Timing-sync Protocol for Sensor Networks,” Proceedings of the 1st ACM Conference on Embedded Network Sensor Systems (SenSys’03), Los Angeles, California, 2003.
23) M. Maroti, B. Kusy, G. Simon and A. Ledeczi, “The Flooding Time Synchronization Protocol,” Proceedings of the 2nd ACM Conference on Embedded Networked Sensor Systems (SenSys’04), Baltimore, Maryland, pp.39-49, 2004.
24) G. Simon, M. Maroti and A. Ledeczi, “Sensor Network-Based Countersniper System,” Proceedings of the 2nd ACM Conference on Embedded Network Sensor Systems (SenSys’04), Baltimore, Maryland, 2004.
25) S. Kim, S. Pakzad, D. Culler, J. Demmel, G. Fenves, S. Glaser and M. Turon, “Health monitoring of civil infrastructures using wireless sensor networks,” Proceedings of the 6th International Conference on Information Processing in Sensor Networks, pp.254-263, 2007.
26) G. Werner-Allen, K. Lorincz, J. Johnson, J. Lees and M. Welsh, “Fidelity and yield in a volcano monitoring sensor network,” USENIX’06: Proceedings of the 7th conference on USENIX Symposium on Operating Systems Design and Implementation, Berkeley, CA, USA, USENIX Association, pp.27-27, 2006.
27) J. Hightower, et al., “Location Systems for Ubiquitous Computing,” IEEE Computer, pp.57-61, Aug. 2001.
28) A. Boukerche, et al., “Localization Systems for Wireless Sensor Networks,” IEEE Wireless Communications, vol.14, no.6, pp.6-12, Dec. 2007.
29) M. Maroti, et al., “Radio Interferometric Geolocation,” Proc. of the 3rd international conference on Embedded Networked Sensor Systems, pp.1-12, Nov. 2005.
30) T. He, et al., “Range-free Localization Schemes in Large Scale Sensor Networks,” Proc. of the 9th annual international conference on Mobile computing and networking (MOBICOM), 2003.
31) R. Stoleru, et al., “High-Accuracy, Low-Cost Localization for Wireless Sensor Netowrk,” Proc. of the 3rd international conference on Embedded Networked Sensor Systems, pp. 13-26, Nov. 2005.

■4群 － 5編 － 3章

3-3 センサネットワークプロトコル

3-3-1 プロトコル概観

（執筆者：石原　進）［2009年7月 受領］

特に無線マルチホップ通信という通信形態に絞れば，無線センサネットワーク（以下単にセンサネットワークと表記する）はアドホックネットワークと同等であり，同様の技術が適用可能といえる．しかしながら，センサネットワークでは，アドホックネットワークで想定されているようなノードの移動は頻繁には起こらない，あるいは移動経路が予測可能であるという違いがある．また，通信はセンサと観測者間でのやり取りがほとんどであること，ノードの電力消費に対する制約が厳しいという違いがある．更に，センサネットワークで使用するアプリケーションによって，様々な最適化のアプローチが考えられる．これらの理由により，センサネットワークでは，アドホックネットワークとは異なるプロトコルが期待されている．

無線センサネットワーク向けのプロトコルは，ネットワークの稼働時間をできるだけ長くするように，消費電力の削減を第一の目標として設計される．ネットワーク全体の消費電力が少なくなっても，特定のノードのみの消費電力が大きいと，ネットワークが分断してしまう恐れがあるので，局所的な電力消費の集中を避けるような設計が行われる．

省電力化のアプローチは，プロトコルの様々な階層で行われている．センサネットワーク中の限られた数のノードのみを稼働させてネットワークを維持することで，省電力化を図る方法（トポロジー制御），MAC 層プロトコル，マルチホップ通信での情報収集のための経路制御での取り組みが特徴的である．3-3-2 項から 3-3-4 項では，これらについて説明する．

センサネットワークでは，ネットワークを構成する個々の機器の ID は問題とならず，そこでどのようなデータが扱われているかに興味がある．センサネットワーク全体をデータベースと見なし，収集あるいは格納したいデータの種類に従ってデータの配送を行うプロトコルが開発されている．このようなアプローチをデータセントリックという．3-3-5 項ではデータセントリックの概念に基づくセンセネットワークプロトコルを紹介する．

最後に，3-3-6 項では，センサネットワークで行われる通信品質（QoS）の管理について述べる．

3-3-2 トポロジー制御

（執筆者：若宮直紀）［2009年11月 受領］

センサネットワークの長寿命化のためには，不要なセンサノードやノードを構成するモジュールの電力供給を停止する休止状態（スリープ状態）と，センシング，メッセージ送受信などを行う起動状態（アクティブ状態）を組み合わせるのが最も効果的である．例えば，1 時間に 1 回の情報収集のために，すべてのノードが常時起動状態にある必要はなく，1 時間ごとに情報収集に必要なノードを短時間だけ動作させればよい．

センサネットワークにおいては，起動状態のノード数や電力消費を最小化しつつ，任意のノード（群）の観測した情報が受信端（ノードや基地局）に伝達されることを保証しなければならない．これをコネクティビティ問題という．無線アドホックネットワーク向けの Span [1] や起動状態を観測状態と送受信状態に分けて制御する STEM [2] などが提案されている．また，

最少数の起動状態ノードによって，観測領域や特定の観測対象のすべてを観測するスケジューリングも必要であり，これをカバレッジ問題という．幾何学的判定に基づいて起動／休止状態を遷移する CCP [3] やマルコフモデルに基づく確率的な状態遷移を実施する CARES [4] などがある．また，モビリティのあるセンサネットワーク向けや，固定的なセンサネットワークに制御可能なモバイルノードを追加することによるコネクティビティ，カバレッジの維持，管理の手法についても研究が行われている．

いずれもノード配置，通信／センシング領域を与条件とした最適化問題を解くことにより最適制御が可能であるが，ノード数の多さや通信／センシング状態の動的な変化，制御オーバヘッドの観点から，近隣ノード間のメッセージ交換のみを利用する自律分散制御が主流である．

以下では，コネクティビティ問題，カバレッジ問題のそれぞれに対する代表的な手法である Span と CCP について紹介する．

(1) Span

Span [1] は，必要最低数のノードが常時起動状態になることによって，センサネットワークの接続性と通信容量を維持しつつ，IEEE 802.11 PSM（Power Saving Mode）の 2.5 倍のネットワーク寿命を達成する．常時起動状態のノードは Coordinator と呼ばれ，Coordinator でないノードのメッセージ転送を行う．ノードは，隣接ノードとの定期的なメッセージ交換を通じて，Coordinator でない隣接 2 ノードが直接，あるいは 1 台または 2 台の Coordinator を介しても通信することができないと判断すると，広告メッセージをブロードキャストし，Coordinator になる．複数のノードが冗長に Coordinator になることを防ぐとともに，電力負荷の大きい Coordinator の役割をノード間で公平に分担できるよう，残余電力や新たに通信可能になる隣接ノード数がより少ないノードほど，広告メッセージの送信が遅延される．

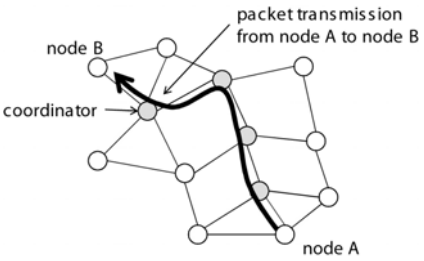


図 3・3 Span

(2) CCP

CCP（Coverage Configuration Protocol）[3] では，通信距離がセンシング距離の 2 倍以上であればカバレッジ問題の解がコネクティビティ問題を同時に満たすということが，幾何学的に証明されている．ノードは，隣接ノードからのメッセージの受信ごとのカバレッジ状態の判定結果，及びタイマ切れに応じて，LISTEN，SLEEP，ACTIVE の 3 状態と，複数ノードが同時に状態遷移することを防ぐための JOIN，WITHDRAW の計 5 状態を遷移する．カバレッジ

が十分かどうかの判定は，自身と隣接ノードのセンシング領域の交点が，$k \geqq 1$ 台（k は要求カバレッジ）以上の起動状態ノードのセンシング領域に含まれているかどうかに基づいて行われる．

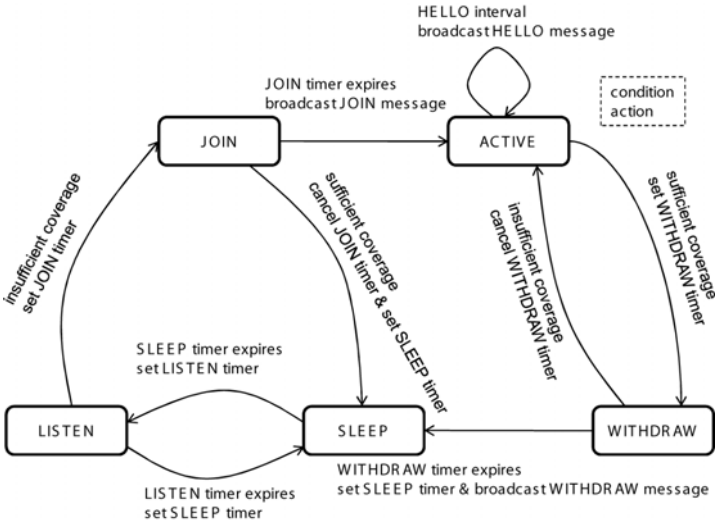


図 3・4　CCP の状態遷移

3-3-3 MAC 層制御

（執筆者：石原　進）［2009 年 7 月 受領］

(1)　MAC プロトコルに求められる特性

無線センサネットワークでの MAC 層制御では，以下のような特性が求められる．

・高いエネルギー効率
・規模性（スケーラビリティ）
・ネットワークのサイズ，ノード密度，トポロジーの変化に対する適応性

一般的なネットワークで重視される遅延やスループットは，センサネットワークでは最重要視されない．公平性に関しても重要視はされない．これは，多くの場合，センセネットワークではすべてのノードが同じタスクをもつので，公平性を左右する要因が少ないためである．

(2)　センサネットワーク MAC プロトコル

(a)　コンテンション方式とスケジュール方式

センサネットワークにおける MAC プロトコルは，CSMA/CA に代表されるコンテンション方式と TDMA に代表されるスケジューリング方式に大別される．また，スケジューリング方式，コンテンション方式を組み合わせたハイブリッド型の手法も提案されている．コンテンション方式では，フレーム送信の必要のあるノードが決められたルールに従って他のノードとチャネル使用権を争奪する．一方スケジューリング方式では，チャネルの使用権を短時間のスロットに区切ってノードごとに予め割り当てる．

コンテンション方式は，スケジューリング方式に対し，規模性と適応性で優れる．センサネットワークでは，機器の故障，電池切れ，機器の追加や電波干渉の状態変化によって利用可能なノード数が増減するため，この数の把握は困難である．スケジューリング方式では，各ノードへの送信権割り当てのためにネットワーク内のノード数を把握する必要があるが，コンテンション方式ではノード数の把握が不要であり，通信のための特別な事前設定も不要である．しかしながら，コンテンション方式では，ノードがデータ送信中でなくとも通信を監視する必要がある．これをアイドルリスニングという．このアイドルリスニングによる電力消費は，送信時の電力の 50 %～100 %にのぼるため，この電力の削減が大きな課題である．多くの MAC プロトコルは，コンテンション方式を採用しているが，これらの電力消費の削減に多くの工夫を凝らしている．代表的なコンテンション方式の MAC プロトコルの例には，S-MAC や B-MAC がある．次項では，両方式について紹介する．

スケジューリング方式は，フレーム送信の必要がない期間に通信デバイスを休止させておくことが可能なので，省電力化に適しているといえる．しかし，前述のように，スケジューリングのために必要なノード数の把握はセンセネットワークでは一般には困難であり，スケーラビリティ，適応性に難がある．また，スケジューリング方式では高い精度のノード間の時刻同期が必要である．

(b) S-MAC

S-MAC[5] では隣接するノード間で休止スケジュールを同期することで，アイドルリスニングを防ぐ．各ノードは定期的にリスニング状態と休止状態を繰り返す．リスニング状態の長さは固定であるが，休止状態の長さは可変である．ノードは，各リスニングの開始時に設けられた Sync 期間に自身のリスニングと休止のスケジュールを隣接ノードに通知する．また，自身のスケジュールを決定していないノードは一定期間チャネルをリッスンし，他ノードから受信したスケジュールに自らのスケジュールを合わせる．

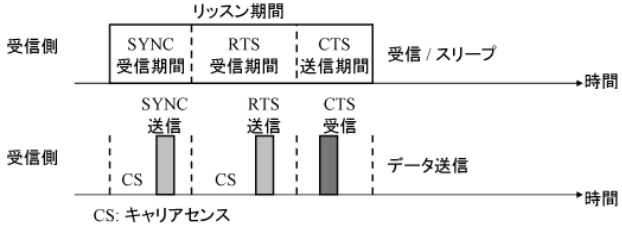


図 3・5 S-MAC

マルチホップ通信時の遅延を抑制するため，S-MAC には Adaptive Listening という拡張が行われている．Adaptive Listening では，ノードが隣接ノードの RTS あるいは CTS パケットをオーバーヒアした場合には，隣接ノードの送信終了時に短い時間起動する．こうすることで，このノードが隣接ノードの次のホップノードとなる場合に，隣接ノードからの送信をすぐに受信できるようにしている．

(c) B-MAC

B-MAC[6] では，Low Power Listening（LPL）と呼ばれる技法によって，アイドルリスニングによる電力消費を抑制する. LPL では, データの前に長いプリアンプルを付けて送信する．ノードは周期的に休止状態からの復帰を繰り返すが，スリープから復帰すると，受信機を作動させて他のノードからの送信が行われていないかを確認する．送信中であれば，このままパケットの受信完了まで起動状態を維持し，受信が完了すると休止状態に戻る．プリアンブルの長さは，ノードの起動周期以上である必要がある．

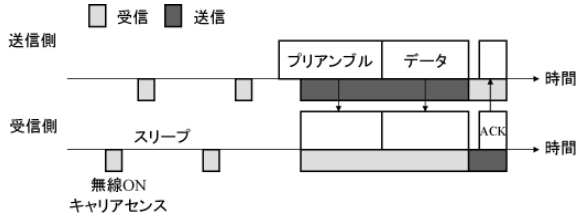


図 3・6 B-MAC の Low Power Listening

3-3-4 情報収集

（執筆者：石原　進）[2009 年 7 月 受領]

無線センサネットワークの代表的な利用方法は，ネットワーク内のすべてのセンサから定期的にデータを単一のノード（シンク）に収集することであり，この用途を想定したプロトコルが多く開発されている．

センサノードからシンクにデータを送信する最も単純な方法は，センサノードからシンクに直接送信することである．しかし，センサノードとシンク間の距離が長い場合，電力消費が大きくなるため, すべてのセンサノードがシンクに直接データを送るのは効率がよくない．そこで，ネットワーク内でクラスタリングを行い，各ノードからのデータを一旦，クラスタヘッドにまとめ，データを集約，圧縮したうえでシンクに送信する手法が多く提案されている．クラスタヘッドの選び方には，確率に応じて各ノードが立候補する方法（LEACH），隣接ノードの残存電力を用いる手法（HEED），ノードの位置と残存電力を用いる方法（GAF）[9] などがある．

(1) LEACH

LEACH（Low-energy Adaptive Clustering Hierarchy）[7] では，各ノードが予めネットワーク内で望ましいクラスタヘッドの割合を知っていることを前提としている．各ノードは，一定間隔で, この割合に基づいて乱数に従って自身がクラスタヘッドになるかどうかを判定する．このルールでは各ノードが同じ割合でクラスタヘッドになるように設定されており，特定のノードがクラスタヘッドになり続けて電力を極端に消費することを防いでいる．クラスタヘッドになったノードは，そのことを通知するパケット（CHA：Cluster Head Advertisement）をブロードキャストする．クラスタヘッド以外のノードは，最も強い電波強度で CHA を受信できたクラスタヘッドのクラスタに参加する．

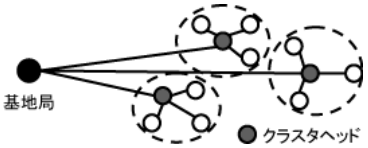


図 3・7 LEACH

(2) HEED

HEED（Hybrid Energy-efficient Distributed clustering）[8] は，各ノードの残存電力を用いて効率のよいクラスタリングを行う分散型プロトコルであり，クラスタ決定のための収束時間が短いこと，制御メッセージ量が少ない（ノード数 n に対して $O(n)$ ）という特徴がある．

LEACH では，そのネットワークでの望ましいクラスタヘッドの割合が機知であるとし，それに基づいてクラスタヘッドになる確率を決めているのに対し，HEED ではそのよう前提がない．HEED では，ネットワーク全体で決められた定期的なタイミングで，各ノードが残存電力に比例した確率でクラスタヘッドに立候補する．各ノードは，隣接ノードがクラスタヘッドに立候補していれば，それらのうちからコスト関数（その候補ノードのネットワーク上の度数，あるいは自身との近接性）が最も低いものを自身の仮のクラスタヘッドとして選出する. この処理を, 各ノードがクラスタヘッドとなる確率を 2 倍しながら繰り返していき，最終的に各ノードは, 自身がクラスタヘッドとなるか, クラスタヘッドに立候補した隣接ノードのうちから最もコスト関数の低いものをヘッダとしたクラスタヘッドとするクラスタに属する．

3-3-5 データセントリック

（執筆者：若宮直紀）［2009 年 11 月 受領］

データセントリックな通信では，「20 度以上の温度の領域」「動体を検出した場所」などの条件に基づいてセンサ情報が送受信される．送受信ノードの多寡に応じて，センサ情報の拡散から通信が開始されるプッシュ型と，クエリー（要求，検索）の拡散から通信が開始されるプル型の手法が使い分けられる．

最も単純なメッセージの拡散手法は，ノードがメッセージのコピーを隣接ノードに配布するフラッディングであるが，オーバヘッドが大きいため，センサネットワークには不向きである．確率的に選んだ隣接ノードにのみメッセージを転送するゴシッピングは，効率のよいメッセージ伝播手法であるが，センサ情報を必要とするノードの割合が低い場合には効果的でない．そのため，事前の交渉に基づいて必要とするノードにだけセンサ情報を効率よく配信する，SPIN [10] や Directed diffusion [11]，D3 [12] などの publish-subscribe 型の手法が提案されている．また，地理的条件に基づくセンサ情報の場合に有効な GPSR [13]，ハッシュ関数を用いてセンサ情報とその管理ノードの位置を対応づけることによりクエリーオーバヘッドを削減する GHT [14] なども提案されている．

データセントリックな通信では，やり取りされるセンサ情報は共通の条件を満たしていることから，相関が高く，集約によるデータ量の削減が有効である．また，「領域の平均温度」のような条件に対しては，センサネットワーク内で最大，最小，平均などの統計処理を行うのが効果的である．効率的に集約を行う手法として，ツリートポロジーで順次，シンクノー

ドへ向けてセンサ情報が転送，集約される TAG [15] や，すべてのノードが分散かつ独立にセンサ情報の集約を行うことによって頑健性を高める CountTorrent [16] などがある．また，センサ情報の時間的・空間的相関を考慮した経路制御などについても研究が行われている．

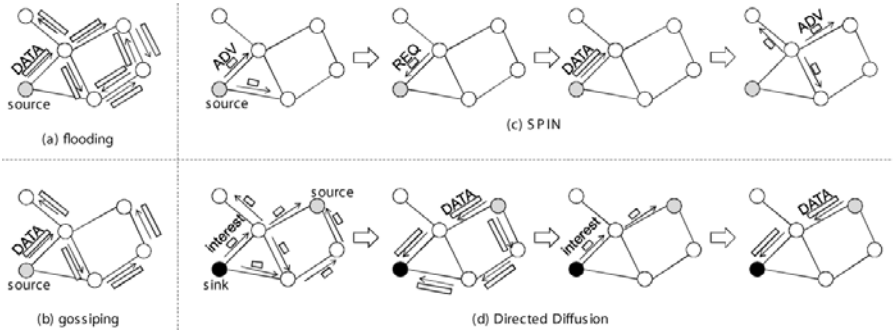


図 3・8　データセントリックな通信方式と通信の例

(1)　SPIN

SPIN（Sensor Protocols for Information via Negotiation）[10] は，センサ情報よりもサイズの小さいメタデータを広告し，送信要求の応答があった隣接ノードにのみセンサ情報を送信することによって，不要なセンサ情報の送受信による帯域や電力の消費を抑制する．まず，ノードは獲得，受信した新しいセンサ情報のメタデータを隣接ノードに送信する．次に，隣接ノードは，所有していないセンサ情報がメタデータに含まれている場合には，そのセンサ情報の送信を要求し，ユニキャストでセンサ情報を受信する．新しいセンサ情報を受信した隣接ノードによって同様の手順が繰り返され，センサネットワーク内の必要なノードにのみセンサ情報が配布される．

(2)　Directed Diffusion

Directed diffusion [11] は，1 対 1，1 対多，多対 1，多対多通信に対応できる周期通信向けのプロトコルである．センサ情報を必要とするノード（シンク）は，条件や収集間隔，期間を記述した interest と呼ばれるクエリーを送信する．クエリーはフラッディングなどによりセンサネットワーク内を転送され，それぞれのノードはクエリーの内容と，送信元の隣接ノードを記録する（gradient と呼ばれる）．条件を満たすセンサ情報を獲得したノード（ソース）は，指定された収集間隔でセンサ情報を送信し，センサ情報は gradient を辿ってシンクへと転送される．シンクは，センサ情報の辿った複数の経路のうち，最も遅延の小さい経路についてセンサ情報の収集間隔を短く設定し，他の経路を障害時の代替経路として維持する．Directed diffusion では，このような要求 － センサ情報送信 － 経路選択の手法は two-phase pull と呼ばれ，経路選択を行わない one-phase pull や，まずソースがセンサ情報を拡散し，シンクが経路選択を行う push が提案されている．

(3) GPSR

位置情報を利用したメッセージ送受信を行う GPSR（Greedy Perimeter Stateless Routing）[13] では，ノードは隣接ノードのうち目的座標に最も近いノードにメッセージを転送する（greedy mode と呼ぶ）．自身より目的地に近いノードが隣接ノードのなかにない場合には，その領域を迂回するように次ホップノードを選択し，メッセージを転送する（perimeter mode と呼ぶ）．

(4) TAG

TAG（Tiny Aggregation）[15] は，ツリー型のセンサ情報収集において収集過程でセンサ情報を集約することにより通信量や電力消費を抑える手法である．TAG では，対象とするセンサ情報や COUNT，MIN，MAX，SUM，AVERAGE などの演算処理などが XML ライクな形式で記述されたクエリーをセンサネットワーク内に拡散し（拡散フェーズ），シンクを根とするツリーを辿ってセンサ情報が収集される（収集フェーズ）．収集期間内（エポックと呼ばれる）にセンサ情報を集約，収集できるよう，エポックをツリーの深さに合わせてスロットと呼ばれる短い時間間隔に分割し，ツリーの葉ノードから順にスロットを割り当てる．

3-3-6 QoS 制御

（執筆者：若宮直紀）［2009 年 11 月 受領］

無線センサネットワークのアプリケーションは多岐にわたり，それぞれ様々な通信品質（QoS）を要求する．定時観測型のアプリケーションでは，遅延や信頼性に対する QoS 要求は比較的緩やかであるが，イベントドリブン型のアプリケーションでは，迅速かつ確実にセンサ情報が伝達されることが求められる．また，同時に複数のセンサから相関の高いセンサ情報が発生するという特徴もある．問い合わせに基づいてセンサ情報が収集されるアプリケーションにおいても同様に，低遅延で信頼性の高い通信が求められる．

エンド間の通信信頼性を向上する手法としては，複数の経路を用いる ReInForM [17] や，複数の QoS を考慮する MCMP [18] などがある．一方，センサネットワークでは多対 1 通信が多く，個々の通信品質よりも観測対象の状態を知り，イベントを検出できることが重要であるため，ESRT [19] では，センサ情報の受信数を信頼性の尺度に用いることにより，ソースの位置や数によらない信頼性制御を実現している．また，CODA [20] では，ホップごとのバックプレッシャとエンド間のフィードバックによるレート制御を組み合わせることにより，多対 1 通信において局所的なネットワークの輻輳を回避する．更に，ソース間の公平な帯域使用を実現する IFRC [21] や，少数の長距離無線通信可能なノードによってセンサ情報を分散して収集する Siphon [22] など，信頼性と応答性の向上のための様々な試みがなされている．

(1) ReInForM

ReInForM [17] は，センサ情報を複数の経路を用いて転送することによって信頼性を高める手法である．ソースは，求める信頼性，近傍のチャネルエラー率，及びシンクからのホップ数に基づき，使用する経路数を算出し，これらの情報を付加したセンサ情報をブロードキャストする．隣接ノードは，指定された経路数に応じて確率的にセンサ情報を転送する．センサ情報の転送の際には，自身のホップ数やチャネルエラー率に応じて経路数を再計算し，付加情報を更新する．ReInForM では，このような局所的な通信状態に基づく動的な経路数制御により，オーバヘッドと信頼性のトレードオフを調整する．

(2) ESRT

ESRT（Event-to-Sink Reliable Transport）[19] では，センサ情報の受信数とセンサネットワークの輻輳状態に応じてセンサ情報の送信レートを調整することにより，過剰なメッセージ送信による輻輳と電力消費を抑制する．ノードは，通信バッファのキュー長によって輻輳を検知し，シンクへ送信するメッセージに輻輳通知ビットを設定する．シンクは，センサネットワークが輻輳していない場合，センサ情報の受信数がイベント検出に不十分であれば，送信レートをセンサ情報の必要数を受信数で割った割合だけ増加させるよう，また，受信数が過剰であれば，送信レートを半分にするよう，全ソースノードに通知する．また，輻輳時には，センサ情報の受信数に応じて送信レートを減らすように指示する．このようにして，ESRT は，輻輳を回避しつつ，必要十分なセンサ情報を受信できるが，輻輳の発生箇所や状況の違いによらずすべてのソースの送信レートを一律に変更するという欠点がある．

(3) IFRC

IFRC（Interference-aware Fair Rate Control）[21] は，シンクを根とするツリートポロジーのネットワークにおいて，ソース間で送信レートに関する Max-Min 公平性を達成するレート制御手法である．ノードはシンクへ送信するメッセージに，自身と子ノードの平均キュー長と送信レートに関する情報を付加し，隣接ノードと輻輳情報を共有する．ノードは，初期状態では指数的に送信レートを増加させていき，輻輳が発生すると送信レートを半分にした後，線形に増加させていく．また，親ノードの送信レートを超える場合，または，隣接ノードまたは隣接ノードの子ノードが輻輳状態の場合には，そのレートに合わせる．これにより，定常的にトラヒックが発生するセンサネットワークにおいて，ソース間の公平な帯域使用が可能となり，輻輳を回避することができる．

■参考文献

1) B. Chen, K. Jamieson, H. Balakrishnan, and R. Morris, “Span: An energy-efficient coordination algorithm for topology maintenance in ad hoc wireless networks,” in proc. of ACM/IEEE International Conference on Mobile Computing and Networking (Mobicom’01), pp.85-96, 2001.
2) C. Schurgers, V. Tsiatsis, M. B. Srivastava, “STEM: Topology management for energy efficient sensor networks,” in proc. of IEEE Aerospace Conference ’02, 2002.
3) X. Wang, G. Xing, Y. Zhang, C. Lu, R. Pless, and C. Gill, “Integrated coverage and connectivity configuration in wireless sensor networks,” ACM Transactions on Sensor Networks, vol.1, no.1, pp.36-72, 2005.
4) M. M-Ismail, F. Sivrikaya, and B. Yener, “Joint problem of power optimal connectivity and coverage in wireless sensor networks,” Wireless Networks, vol.13, Issue 4, pp.537-550, 2007.
5) W. Ye, J. Heidemann, and D. Estrin, “Media access control with coordinated adaptive sleeping for wireless sensor networks,” IEEE/ACM Trans. on Networking, vol.12, no.3, pp.493-506, 2004.
6) J. Polastre, J. Hill, and D. Culler, “Versatile low power media access for wireless sensor networks,” in proc. of the second ACM Conference on Embedded Networked Sensor Systems (SenSys), 2004.
7) W.R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, “Energy-Efficient Communication Protocol forWireless Microsensor Networks,” in proc. of the 33rd Hawaii International Conference on System Sciences, pp.1-10, 2000.
8) O. Younis and S. Fahmy, “HEED: A Hybrid, Energy-Effieicent, Distributed clustering approach for ad hoc sensor networks,” IEEE Trans. on Mobile Computing, vol.3, no.4, pp.366-379, 2004.
9) Y. Xu, J. Heidemann and D. Estrin, “Geography-informed energy conservation for Ad Hoc routing,” in proc. of of the 7th annual international conference on Mobile computing and networking (Mobicom’01), pp.70-84,

2001.
10) W. Heinzelman, J. Kulik and H. Balakrishnan, “Adaptive protocols for information dissemination in wireless sensor networks,” in proc. of International Conference on Mobile Computing and Networking (MobiCom’99), pp.174-185, 1999.
11) F. Silva, J. Heidemann, R. Govindan, and D. Estrin, “Directed diffusion,” Technical Report ISI-TR-2004-586, USC/Information Sciences Institute, 2004.
12) M. Diztel and K. Langendoen, “D3: Data-centric data dissemination in wireless sensor networks,” in proc. of European Conference on Wireless Technology 2005, pp.185-188, 2005.
13) B. Karp and H. T. Kung, “GPSR: Greedy perimeter stateless routing for wireless networks,” in proc. of ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom’00), pp.243-254, 2000.
14) S. Ratnasamy, B. Karp, L. Yin, and F. Yu, “GHT: A geographic hash table for data-centric storage,” in proc. of ACM International Workshop on Wireless Sensor Networks and Their Applications (WSNA’02), pp.78-87, 2002.
15) S. Madden, M. Franklin, J. Hellerstein, and W. Hong, “TAG: A tiny aggregation service for ad hoc sensor networks,” in proc. of Symposium on Opererating Systems Design and Implementation (OSDI), 2002.
16) A. Kamra, V. Misra, and D. Rubenstein, “CountTorrent: Ubiquitous access to query aggregates in dynamic and mobile sensor networks,” in proc. of ACM Conference on Embedded Networked Sensor Systems (SenSys’07), pp.43-57, 2007.
17) B. Deb, S. Bhatnagar, and B. Nath, “ReInForM: Reliable information forwarding using multiple paths in sensor networks,” in proc. of IEEE Conference on Local Computer Networks (LCN 2003), pp.406, 2003.
18) X. Huang and Y. Fang, “Multiconstrained QoS multipath routing in wireless sensor networks,” Wireless Networks, vol.14, no.4, pp.465-478, 2007.
19) Y. Sankarasubramaniam, B. Akan, and I. F. Akyildiz, “ESRT: Event-to-sink reliable transport in wireless sensor networks,” in proc. ofACM International Symposium on Mobile Ad Hoc Networking & Computing (MobiHoc 2003), pp.177-188, 2003.
20) C.-Y. Wan, S. B. Eisenman, and A. T. Campbell, “CODA: Congestion detection and avoidance in sensor networks,” in proc. of ACM Conference on Embedded Networked Sensor Systems (SenSys’03), pp.266-279, 2003.
21) S. Rangwala, R. Gummadi, R. Govindan, and K. Psounis, “Interference-aware fair rate control in wireless sensor networks,” in proc. of ACM SIGCOMM’06, pp.63-74, 2006.
22) C.-Y. Wan, S. B. Eisenman, A. T. Campbell, and J. Crowcroft, “Siphon: Overload traffic management using multi-radio virtual sinks in sensor networks,” in proc. of ACM Conference on Embedded Networked Sensor Systems (SenSys’05), pp.116-129, 2005.

■4 群 － 5 編 － 3 章

3-4 データ管理

（執筆者：鈴木　敬）［2008 年 10 月 受領］

3-4-1 センシングデータ処理

センサネットワークにおいて扱う「データ」にはセンシングデータとネットワーク構成やハードウェアなどのリソースを定義するリソースデータがある．本章では，センシングデータに関する処理技術と管理技術を解説する．

図 3･9 はセンサネットワークシステムの構成例である．一般に無線ネットワークとしてのセンサネットワークを考える場合は，図のゲートウェイより右側のサーバやユーザは意識しない．しかし何らかの応用を想定したセンサネットワークシステムを考える場合は，ゲートウェイより右側も含めて系全体を意識する必要がある．過去の研究例を見ると，その対象とする応用や技術の観点によりデータ処理の位置づけや方法も大きく異なり，センサノードとゲートウェイを介して接続するサーバとの役割分担も様々である．ここでは，センサネットワークに対する視点の違いを整理し，データ処理に対する取り組み例を解説する．

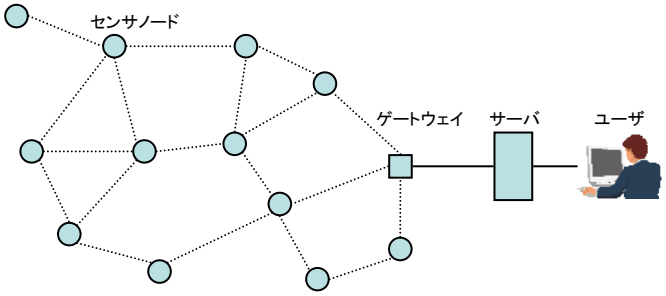


図 3・9　センサネットの構成例

まず，幾つかある視点を以下の 4 点にまとめる．

1. 応用面から見るセンシング
2. データの種類
3. データ保存
4. 計算モデル

(1)　応用面から見るセンシング

様々な応用分野でセンサネットワークの活用が検討されている．それぞれの局面でセンサネットワークへの期待が異なる．期待としては以下の点があげられる．

①ワイヤレスセンシングであること：　センサの設置場所の制限からの解放
②アドホックネットワークであること：　センサ設置の容易性，環境変化への柔軟性
③多くのセンサをつなげられること：　空間の網羅性の向上
④低コストでセンシング環境を構築できること：　端末コストは比較的安価になり得る（精度とのトレードオフ）

これらの期待と，それぞれの応用からセンシングするデータの取得に関して以下の三つの

パターンがある．

(1) イベント通報型

まず，センシングデータを SDi（センサ識別子，時刻，位置，センシング対象，値）の 5 項目で定義することにする．例えば「ドアが開いた」というイベント E は，(センサ識別子，時刻，位置，"ドア"，"開いた") と記述できる．イベント通報型は，イベント E に対して，処理 P を行う，という形式である．例えば，“E（ドアが開いた）ら P（照明を点ける)”といった単純な制御に対応する．この場合，イベントデータそのものに対するデータ処理は存在しない．

(2) リアルタイム処理型

リアルタイム処理型は，あるセンシングデータに対して，そのリアルタイムにデータの加工を行うタイプである．データの加工も，単純に，値を 1 次式に当てはめて変換するもの，同時刻の複数のデータからある値を計算するもの，あるいは，過去のデータ集合と最新のデータを突き合わせて計算するもの，など様々あり得る．例えば，サーミスタを使った温度センサは，一般的にはサーミスタを含んだ回路の電圧を測定することで温度を求める．サーミスタは温度に対応して抵抗値が変化するため，電圧値を温度値に変換できる．

(3) バッチ処理型

バッチ処理型は，必要なセンシングデータを一旦，データベースに集約し，そのデータベースからデータを読み出して解析処理を行う．その点，従来の一般的なデータ処理とシステム構成上は変わりがない．この場合，センサネットワークの特徴は，①センサの数が多い（地理的な網羅性，時間軸での網羅性)，②センシングデータの信頼性が（専用のセンシングシステムに比べて）仮定により様々である．

これらは，一つのシステム上で排他的な処理ではなく，リアルタイム処理とバッチ処理を組み合わせた応用もある．

(2) データの種類

センサというと一般的には物理量を測定するセンサ（温度，圧力，振動）やガスなど物質の濃度を測定するセンサをイメージするが，広義には，単純なスイッチやカメラ，マイク，あるいは RFID リーダもセンサの一種と考える．また，例えば PC や機械が生成するログデータもセンシング情報の一種と考えることができる．ここでは，前記のようなセンシングデータのソースの種別ではなく，センシングの周期とデータの形式から分類する．

(a) センシングの周期

センシングをどのようなタイミングで行うかは，どのような事象を測定するかにより異なる．振動する値を解析しようとすれば，一定周期でその対象をセンシングし，周期性のあるセンシングデータを生成する．また，気温のように急激には変化しない値は適当な間隔で測定する．一般的に MOTE のような小型電池で駆動するセンサノードを長期間運用する場合，時々測定し，そのデータを送信し，それ以外のときはノードを待機状態にして消費電力を下げる，という運用により電池寿命を延ばすため，間欠的な測定は電池寿命を延ばすためにも用いられる [1)].

もう一つのセンシングの方法は, 不定期に発生する事象のセンシングである. 例えば, RFID

リーダの前を RFID が通過したとき，その ID を送信する，あるいは人感センサの前を人が通過したら知らせる，といったケースがこれにあたる．

これらの場合，センシングしたい事象（イベント）がいつ発生するか定かではなく，イベントの発生は一般的にはランダムである．このようなセンシングではセンサは常時稼動しておく必要がある．

(b) センシングデータの形式

一般に物理量を測定するセンサ素子の出力はアナログの電圧値でこれを AD 変換器でデジタル値へ変換する．値はスカラー値である．単純なスイッチのようにオン／オフ 2 値の値もスカラー値の一種と考えられる．一方，3 軸加速度センサの出力は 3 軸（XYZ）のベクトル値となる．また，センサによっては値を補正するために温度センサを内蔵するものもある．この場合，本来の値と温度値という複合型の値となる．RFID リーダの出力も，ID やその付加情報という形の複合型とみることができる．

振動やマイクでとる音のようにスカラー値の連続データもある．カメラの出力のビットマップやログデータは複合型の連続データと考えることができる．

(3) データ保存と計算モデル

前節で述べたセンシングデータの発生周期と形式に対し，データを記録するだけであれば単純なシーケンシャルファイル形式になる．センサの位置やセンシング時刻で検索することを想定すると，それらの値で検索しやすいデータベース構造が必要になる．しかし，センシングデータが膨大な量になると，通常のハードディスク装置を用いたデータベースでは処理速度が課題になるため，新しい計算方式が提案されている．

(a) ストリームデータ処理

ストリームデータ処理とは，流れてくるデータ列に対して，ある時間範囲内のデータのみを保持して計算し，出力する処理方法である [2), 3)]．例えば，データ列の値の平均値を求めたり，最大・最小値を求める，などの処理がある．ストリームデータ処理は，オンメモリの処理であること，ネットワーク経路上で分散処理できること，などが特徴であり，センサネットワークと親和性がある．

(b) イベントアクション処理

ストリームデータ処理がデータ列に対する処理であるのに対し，イベントアクション処理は単発のデータ（イベント）に対する処理方式である [4)]．イベントアクション処理とは，あるイベント種 E に対して A という処理を実行するイベントドリブンのデータ処理方法である．イベントアクション処理は離散的なデータを扱うセンサ処理に適した処理方式である．

センサネットワークの処理は，大きく無線ネットワーク上での処理とデータを集約するサーバ側の処理に分けられる．前者はネットワーク上での分散処理であり，後者はサーバでの集中処理になる．前者の方がよりセンサネットワーク特有の上記のストリームデータ処理もイベントアクション処理もどちらもネットワーク上，サーバ上それぞれの処理が可能である．

3-4-2 データ管理・マイニング

センサネットワークが役に立つ局面（新しい価値）は幾つか考えられる．単純にはセンサネットワークのワイヤレス，センサの網羅性などを活かした今までにないセンシングには価値がある．更には，それらのデータを用いてシミュレーションやデータマイニングにより，将来の傾向を予測することで価値が高まる．例えば，産業機器では，振動データなどの経年変化を解析して故障時期を予測する予防保全が行われている．同様に建造物の振動データなどの解析により建造物のヘルスケアといった応用が考えられている [5].

データ管理という観点では単純にデータを時系列に保存するのではなく，センシングする対象（環境とその中の物や人の関係）をモデル化し，例えば「机の上にある物」といった修飾語で位置や物の状態を検索するシステムもある [6].

また，センシングデータが地理学的な空間上にマッピングされていると考え，それを表現する共通の表現形式を定義する動きもある [7].

■参考文献

1) Jason L. Hill and David E. Culler, “MICA: A Wireless Platform for Deeply Embedded Networks,” IEEE Micro, vol.22, no.6, pp.12-24 Nov.-Dec. 2002.
2) “TinyDB A Declarative Database for Sensor Networks,” http://telegraph.cs.berkeley.edu/tinydb/
3) Arvind Arasu, Brian Babcock, Shivnath Babu, Mayur Datar, Keith Ito, Rajeev Motwani, Itaru Nishizawa, U. Srivastava, D. Thomas, Rohit Varma, Jennifer Widom, “STREAM: The Stanford Stream Data Manager”, IEEE Data Engineering Bulletin, vol.26, no.1, pp.19-26 , Mar. 2003.
4) Keiro Muro, Takehiro Urano, Toshiyuki Odaka, Kei Suzuki, “AirSenseWare: Sensor-network Middleware for Information Sharing,” 3rd International Conference on Intelligent Sensors, Sensor Networks and Information, 2007 (ISSNIP 2007), pp.497-502, Dec. 2007.
5) 中村　充, “建築構造物のヘルスモニタリング,” 計測と制御, 第 41 巻, 第 11 号, pp.819-824, Nov. 2002.
6) 岡留剛, 岸野泰恵, 前川卓也, 柳沢豊, 櫻井保志, “s-room？ 実世界情報の生成とそのリアルタイムコンテンツ化,” NTT 技術ジャーナル, vol.19, no.6, pp.13-18, Jun. 2008.
7) “VAST - Introduction to SensorML,” http://vast.uah.edu/SensorML/

■4群 － 5編 － 3章

3-5 セキュリティ

（執筆者：西山裕之）［2008年11月 受領］

マルチホップ転送を伴うアドホックネットワークによって構築されるワイヤレスセンサネットワークでは，任意のノード間におけるパケットの送受信は，途中経過に存在する不特定多数のノードを経由することにより実現される．しかしながら，悪意のある攻撃者によるパケットの盗聴はもちろん，ネットワーク内に改ざんを行うノードを配置することにより，容易にネットワークのシステム全体を破綻させられる危険性が存在することになる．ここで，各センサノードは非常に小さなリソースしか備えていないため，通常の計算機で使用されているセキュリティ技術を導入することは極めて困難である．しかしながら，センシング及びモニタリングする適用対象によっては，環境情報だけでなく，個人情報や生態情報がネットワークに流出する恐れがある．そのため，センサネットワークにおけるセキュリティの導入は必須である．

このような問題に対して，センサネットワークのセキュリティに対する数多くの研究が実施されている [4), 5)]．本節では，これらの研究のなかから，比較的初期の段階でセンサネットワークセキュリティの重要性を提唱し，セキュアなプロトコルである SPINS（Security Protocol for Sensor Networks）[2), 3)] を提案した A. Perrig らの研究に焦点を当てて説明を行う．

Perrig らはブロードキャスト通信における安全性の研究を行っている研究者であり，センサネットワークを非常に計算機資源が限定された環境として位置づけることで，二つのセキュアなプロトコルである SNEP とμTESLA の設計を行った．SNEP（Sensor Network Encryption Protocol）は低いオーバヘッドでデータの機密性，二者間のデータ認証，及びデータの新規性を提供する．また，μTESLA はブロードキャスト認証のためのプロトコル TESLA（Timed Efficient Stream Loss-tolerant Authentication）[3)] を軽量化するために修正したものであり，センサネットワーク間の認証されたストリーミングブロードキャストを提供している．以下では，SNEP 及びμTESLA について簡単に説明する．

3-5-1 システムの要件

Perrig らは，センサネットワークと外部ネットワークのインタフェースとなる基盤ステーションが存在することを基本とした通信アーキテクチャを前提としている．ここで，基盤ステーションは，センサノードより長い寿命をもつ十分なバッテリーパワー，暗号化鍵を格納するのに十分なメモリ，そして，外部ネットワークと通信可能であることを除いては，センサノードと同等の能力をもつ．以上より，Perrig らは，基盤ステーションを中心とした通信プロトコルを提唱するとともに，センサノード間通信やセンサノードからのブロードキャストに対しても適応させる方法を示している．また，各センサノードは，製造時に基盤ステーションと共有するマスタ秘匿鍵（Master Secret Key）を保持しているものとする．

3-5-2 SNEP

センサネットワークに求められるセキュリティの特徴として，データの機密性，データ認証，データの新規性が存在する．これは，センサネットワークの通信はブロードキャストで

あることから，攻撃者によるトラヒックの盗聴，新たな偽造メッセージの混入，そして，古いメッセージの再生などに対処するためである．Perrig らは，これらの問題を解決するためのプロトコルとして SNEP を設計しており，各特徴に対して次のような手法を用いている．

- **データの機密性**：盗聴者に同一の平文の複数の暗号文を収集されても，平文に関する情報を与えないセマンティックセキュリティを用いる．これは，各メッセージの後でカウンタの値が加算されるので，同じメッセージも異なる暗号化がなされる．
- **二者間のデータ認証**：メッセージ認証コード（MAC）を用いる．なお，MAC 鍵の生成には，製造時に保持しているマスタ秘密鍵に対して，擬似乱数関数により独立した鍵を生成する．MAC が正しく検証できれば，受信者はメッセージが本来の送信者により送信されたことを確認できる．
- **データの新規性**：MAC に含まれるカウンタ値により，古いメッセージの再送信を防止する．また，メッセージが正しく検証されれば，受信者は古いカウンタ値との比較によりメッセージの順序付けを可能にする．なお，SNEP ではカウンタの状態を同期させるために，カウンタ交換プロトコルが提供されている．

3-5-3 μ TESLA

TESLA はブロードキャストされたメッセージを認証可能なプロトコルであるが，一定以上の計算機資源を必要とする．Perrig らは，センサネットワークにおけるノード間のブロードキャストを認証可能にするために，計算機資源が限定された環境に対応するためのμTESLA を提案している．μTESLA は，TESLA に対して以下の項目を修正することで設計されている．

- TESLA は最初のパケットを非対称暗号方式によるデジタル署名で認証するが，センサノードには負荷が大きすぎるため，μTESLA は対称鍵の遅延開示による非対称性を導入することで克服する．
- 各パケットで鍵を開示するには，送受信に多大な電力を要する．μTESLA は一定期間ごとに 1 回だけ鍵を開示する．

以上の二つのプロトコルにより，SPINS ではセンサネットワークにおける安全なノード間通信を可能にする．実際に，本提案に基づくセキュアなセンサネットワークシステムの構築が試みられるとともに [1]，本研究を基盤として様々なセンサネットワークセキュリティの研究が実施されている [5]．

■参考文献

1) 溝口文雄 他, “TinyMRL：センサネットワークへのマルチエージェント言語の導入によるセキュアな相互協調システム,” 電子情報通信学会論文誌 D, vol.J89-D, no.8, pp.1764-1776, 2006.
2) A. Perrig, R. Szewczyk, V. Wen, D. Culler, and J. Tygar, “SPINS: Security protocols for sensor networks,” Wireless Networks, vol.8, no.5, pp.521-534, 2002.
3) A. Perrig and J. Tygar（溝口文雄監訳）, “ワイヤード/ワイヤレスネットワークにおけるブロードキャスト通信のセキュリティ,” pp.159-184, 共立出版, 2004.
4) A. Vaseashta and S. Vaseashta, “A Survey of Sensor Network Security,” Sensors & Transducers Journal, vol.94, pp.91-102, 2008.
5) J. Walters, Z. Liang, W. Shi, and V. Chaudhary, “Wireless Sensor Network Security: A Survey,” 2006 Auerbach Publications, CRC Press, 2006.

■4 群 － 5 編 － 3 章

3-6 センサネットワークの応用

（執筆者：阪田史郎）［2009 年 1 月 受領］

センサネットワークの形態は,大きく屋外である程度の広域を対象としたネットワークと，屋内に閉じた比較的狭域のネットワークに分けられる [1]．広域センサネットワークでは，森林や海洋，河川，砂漠，都市，戦場などに飛行機などからの数千～数万のセンサの散布による自然環境やその変化などの観測，地雷や爆発物の探索，あるいは河川流域の地盤や橋梁の耐震強度の測定，街中の多地点へのカメラ（視覚センサ）設置による災害やテロの発生の監視，などの例があげられる．狭域センサネットワークとしては，工場やビル，オフィス，家の中へのセンサの設置により，例えば ZigBee Alliance で規定中の**表 3･1** に示すような応用が考えられている [2)~4)]．

表 3・1 ZigBee の主な標準アプリケーションプロファイル

プロファイル名	概要
HA (Home Automation)	ホームネットワーク向け
CBA (Commercial Building Automation)	ビル管理向け
IPM (Industrial Plant Monitoring)	工場管理向け
ZSE (ZigBee Smart Energy)	省電力制御向け
WSA (Wireless Sensor Network Application)	大規模環境モニタリング，資産管理， 機械器具モニタリング向け
TA (Telecom Application)	携帯電話を利用した各種サービス向け
AMI (Advanced Metering Infrastructure)	電力，水道，ガスの各メータの読取向け
PHHC (Personal Home Health Care)	健康モニタリング向け

実用面からは，規模や給電，配線の容易さから屋内の狭域センサネットワークが先行すると考えられ，小規模なネットワークは一部実用が開始されつつある．現在は実験段階であるが，狭域センサネットワークの普及がある程度進展した時点で，広域センサネットワークの実用化が徐々に開始されると考えられる．また，当面センサは固定的に設置されるものが主流であるが，将来は歩行者や車，ロボットなどに装着し，移動するセンサ群を制御するセンサネットワークも出現すると考えられる [4)~6)]．

総務省におけるユビキタスセンサネットワーク研究会では，2002～2004 年にかけて調査検討を行い，そのときの全体的な結果を**図 3･10** のようにまとめている [5)~7)]．応用の場に関しては家庭，公共，企業に分類され，それぞれ以下の項目が主要な応用と考えられている．

(1) **家庭**：防犯・防災，省電力・省エネ，医療・健康・介護，家電機器の故障検出
(2) **公共**（屋外の広域センサネットワークが主体となる）：防犯・防災（地震，火災，洪水など）・テロ監視，環境モニタリング・保全（大気中の NOx，SOx，その他の有毒ガス

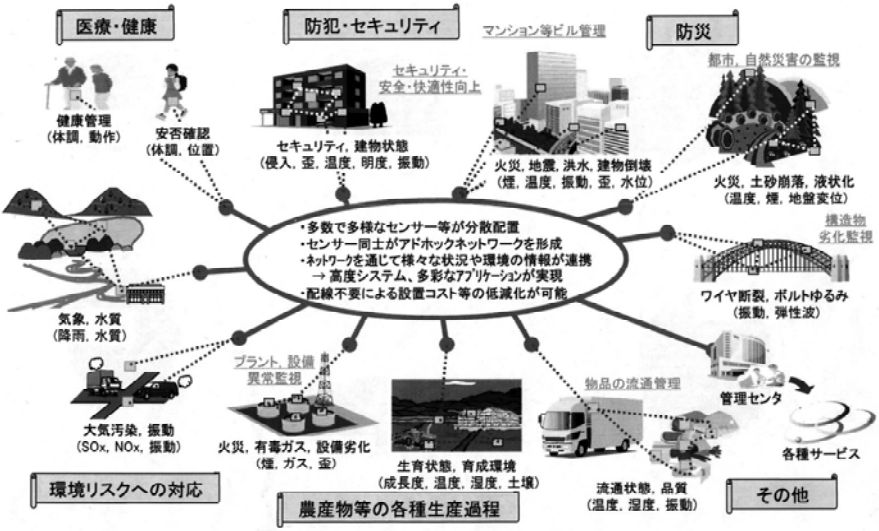


図 3・10　ユビキタスセンサネットワーク技術の将来の利用イメージ（総務省）

の検知，工場の排出ガスや車の排気ガスの測定，火山ガスの濃度測定・監視など），道路や橋梁などの構造物の劣化監視・保全，道路沿いに各種センサを高密度に配置した交通制御支援（渋滞解消，環境改善，緊急車両の優先化）

(3) **企業**：工場での製造管理，物品の物流・保管・輸送管理，農場における食物栽培支援，建設現場での作業支援，ビルなどの環境管理・耐震管理，オフィスにおける温度・湿度・塵埃測定

今後，非接触センサとして機能する RFID（Radio Frequency Identification，電子タグや IC タグとも呼ばれる）では，食物や薬品にタグ（センサに対応）を付与し，バックエンドのファイルで電子タグの情報を逐次格納・管理して，トレースできるようにして，人々に安全・安心を提供することを狙いとするトレーサビリティも重要になると考えられる [8].

■参考文献

1) I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, “A Survey on Sensor Networks,” IEEE Communications, vol.40, no.8, pp.102-114, Aug. 2002.
2) 稲坂朋義, “特集 実現が待たれるユビキタスセンサネットワーク利活用から見た将来イメージ,” コンピュータネットワークス&LAN, vol.23, no.4, Apr. 2005.
3) 阪田史郎編著, “ユビキタス技術　センサネットワーク,” オーム社, May 2006.
4) 安藤繁, 田村陽介, 戸辺義人, 南正輝, “センサネットワーク技術,” 東京電機大学出版局, May 2006.
5) 総務省, “ユビキタスセンサネットワークに関する調査研究会,” Aug. 2004. http://www.soumu.go.jp/s-news/2004/040806_4.html
6) 阪田史郎編著, “ZigBee センサネットワーク技術,” 秀和システム, Jul. 2005.
7) 阪田史郎, “工場におけるワイヤレスネットワーク活用技術とその動向,” 計装, Nov. 2008.
8) 阪田史郎, “センサネットワークの最新動向,” ケミカル・エンジニアリング, Nov. 2007.

■4 群 － 5 編 － 3 章

3-7 センサネットワーク標準化例

3-7-1 IEEE 802.15.4 と ZigBee

（執筆者：福永　茂）［2009 年 5 月 受領］

(1)　ZigBee の特徴

センサネットワークの標準無線方式として，ZigBee Alliance [1] で規格化された近距離無線方式の ZigBee が期待されている．

図 3･11 に各無線規格の範囲を示す．ZigBee は大容量データの伝送はせず，「低消費電力」，「低コスト」を重視して規格化された．これは，映像や音声などのマルチメディアデータも安定して伝送できることを目指した Bluetooth や無線 LAN などとは大きく異なる．

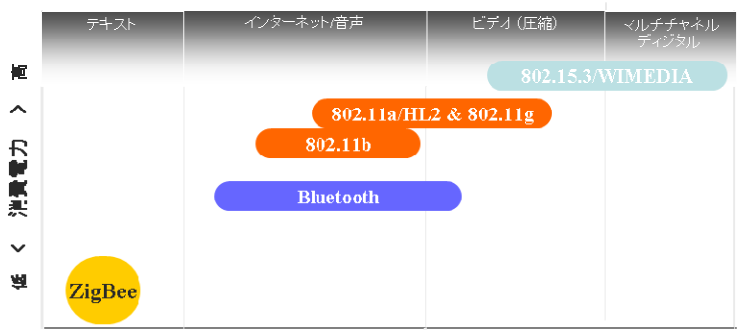


図 3・11　各無線規格の範囲

以下，ZigBee の特徴を Bluetooth 及び無線 LAN とそれぞれ比較したものを**表 3･2** に示す．

表 3・2　各無線方式の比較

特徴	ZigBee	Bluetooth	IEEE 802.11b
電池寿命	数年	数日	数時間
複雑さ	○	△	×
接続可能デバイス数	64000	7	32
接続遅延時間	30ms	10s	3s
通信距離	30-100m	10m	100-300m
伝送レート	250kbps	1Mbps	11Mbps
セキュリティ	128bit AES による認証，暗号	64bit，128bit	認証用 ID，WEP

(2)　ZigBee と IEEE 802.15.4 の通信レイヤ構成

図 3･12 に ZigBee の通信レイヤ構成を示す．下位レイヤである PHY レイヤや MAC レイヤは IEEE 802.15.4 で標準化されており，ネットワークレイヤやセキュリティ機能，アプリケー

ションとのインタフェースなどは，ZigBee で規格化が進められている．

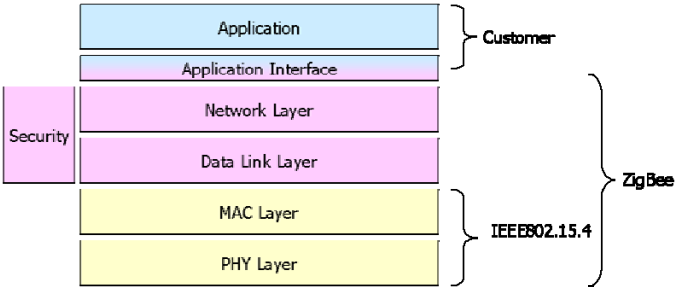


図 3・12　ZigBee のレイヤ構成

(3)　IEEE 802.15.4

(a)　IEEE 802.15.4 シリーズ

IEEE 802.15[2] は，WPAN（Wireless Personal Area Network）向け無線通信方式の標準規格である．IEEE 802.15.4[3] は，低伝送レート規格として 2003 年に標準化され，現在も修正規格を審議中である．

(1) 15.4

低伝送レートを対象とした WPAN の PHY と MAC の規定であり，2003 年に標準化された．現在の ZigBee の PHY と MAC の規定である．

(2) 15.4a

UWB（Ultra Wide Band）技術を用いて，距離測定機能を高めた 15.4 PHY の alternative 規格であり，2007 年に標準化された．

(3) 15.4b

15.4 PHY の修正規格であり，2006 年に標準化された．15.4 の曖昧な記述の修正だけでなく，新しい変調方式の追加，ビーコンモード，セキュリティなどの機能拡張を行った．

2003 年のバージョンと区別するために，明示的に IEEE 802.15.4-2006 と表現する場合もある．なお，最新の ZigBee では，まだ IEEE 802.5.4-2006 には対応しておらず，IEEE 802.15.4-2003 を参照したままである．

(4) 15.4c

中国で WPAN 向けに新しく割り当てられた 780 MHz 帯に適応するための 15.4 PHY と MAC の修正規格であり，2009 年に標準化された．

(5) 15.4d

日本で 2008 年に省令改正され WPAN 向けに割り当てられた 950 MHz 帯に適応するための 15.4 PHY と MAC の修正規格であり，2009 年に標準化された．

(6) 15.4e

15.4 MAC の修正規格であり，現在審議中である．

(7) 15.4f

RFID 向けの規格であり，現在審議中である．

(8) 15.4g

電力・ガス・水道のメータ間ネットワーク（SUN：Smart Utility Network）向けの規格であり，現在審議中である．

(b) IEEE 802.15.4 の周波数帯

IEEE 802.15.4 では，三つの周波数帯が規定されていたが，2009 年に 15.4c と 15.4d により，870 MHz 帯と 950 MHz 帯が追加された．**図 3･13** に 15.4 の三つの帯域（868 MHz，915 MHz，2.4 GHz），**図 3･14** に 15.4d（950 MHz）のチャネル割当を示す．

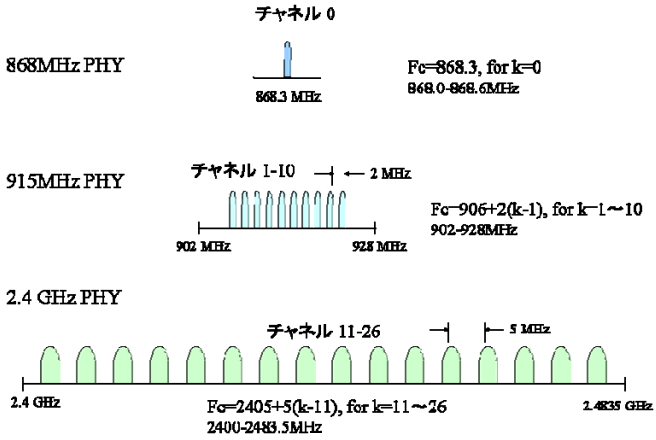


図 3･13 IEEE 802.15.4（868 MHz, 915 MHz, 2.4 GHz）のチャネル割当

(1) 868 MHz 帯（欧州）

欧州のみで利用できるサブギガバンドである．チャネル幅が 600 kHz で 1 チャネルしか割り当てられていないため，やや利用しにくい帯域である．

(2) 915 MHz 帯（米）

米国でのみ利用できるサブギガバンドである．2 MHz 間隔で 10 チャネルが割り当てられており，多くの応用例での利用が期待されている．

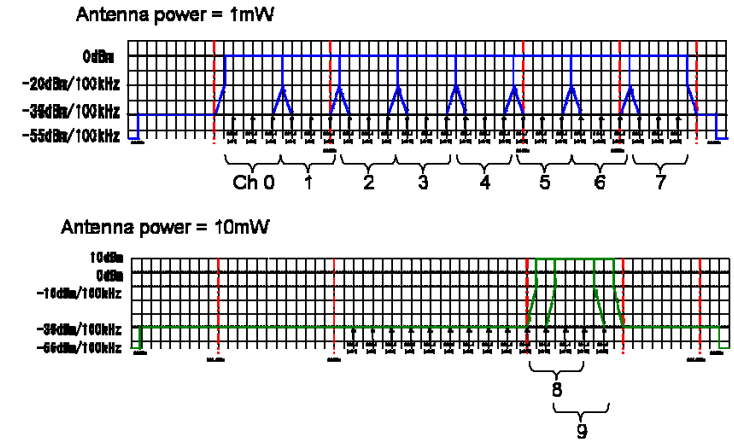
(3) 2.4 GHz 帯（全世界）

全世界で利用できる ISM バンドである．

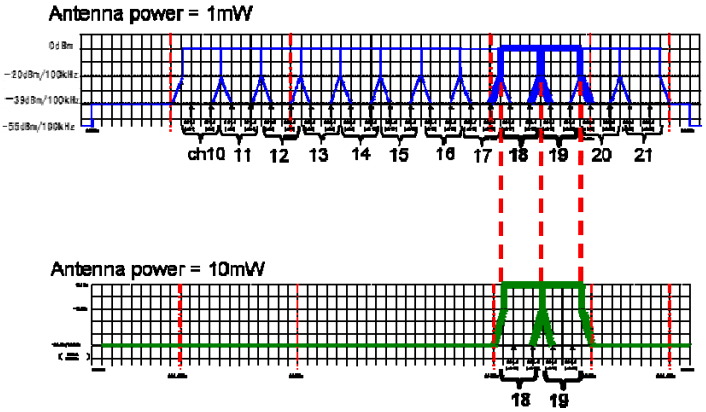
2 MHz 幅のチャネルが 5 MHz 間隔で割り当てられているため，拡散変調方式の効果が高く，電波干渉に強い仕様になっている．

グローバルに利用できることから，多くの LSI や機器が既に製品化されており，グローバルな応用に適している．また，出荷量が多いため，コストパフォーマンスが高くなることも期待されている．

一方，無線 LAN や Bluetooth，RFID システムなど，多くの無線方式が利用しており，電子レンジや機械装置から発生する雑音なども混在する帯域であるため，通信品質が不安定になる可能性がある．



(a) BPSK 方式の場合



(b) GFSK 方式の場合

図 3・14　IEEE 802.15.4d（950 MHz 帯）のチャネル割当

(4) 870 MHz 帯（中国）

中国のみで利用できるサブギガバンドである．

(5) 950 MHz 帯（日本）

日本でのみ利用できるサブギガバンドである．元々950 MHz を利用していた RFID の規格に合わせたため，チャネル幅が狭い．チャネル割当は採用された変調方式や最大送信出力により異なる．

(c)　変調方式

表 3･3 に IEEE 802.15.4-2003 と 2006 の変調方式を示す．IEEE 802.15.4-2003 では三つの周

波数帯でそれぞれ変調方式が規定されており，IEEE 802.15.4-2006 で，サブギガバンドの周波数利用効率を高めるため，二つの変調方式がそれぞれ追加規定された．

また，**表 3･4** に IEEE 802.15.4d の変調方式を示す．15.4d では二つの変調方式が規定された．

表 3・3　IEEE 802.15.4-2003, 2006 の変調方式

周波数帯	2.4 GHz		915 MHz		868 MHz		
チャネル数	16		10		1		
変調方式	O-QPSK	BPSK	ASK	O-QPSK	BPSK	ASK	O-QPSK
伝送レート	250 kbps	40 kbps	250 kbps	250 kbps	20 kbps	250 kbps	100 kbps
使用可能地域	全世界		米国		欧州		

表 3・4　IEEE 802.15.4d の変調方式

周波数帯	950 MHz	
チャネル数	8	12
変調方式	BPSK	GFSK
伝送レート	20 kbps	100 kbps
使用可能地域	日本	

(d)　デバイスタイプ

IEEE 802.15.4 では，FFD（Full Function Device）と RFD（Reduced Function Device）の二つのデバイスタイプが定義されている．

- FFD の主な機能
  - PAN コーディネータやルータになれる．
  - 他の FFD や RFD と通信可能．
  - スター型や P2P 型，クラスタツリー型など複数のトポロジーに対応．
- RFD の主な機能
  - エンドデバイスにのみなれる（PAN コーディネータやルータにはなれない）．
  - FFD とのみ通信可能．
  - P2P 通信には対応できない．
  - 低コストを実現．

(e)　ネットワークトポロジー

IEEE 802.15.4 では，スター型と Peer-to-peer（P2P）型の二つのネットワークトポロジーが定義されている．**図 3･15** にネットワークトポロジーの例を示す．

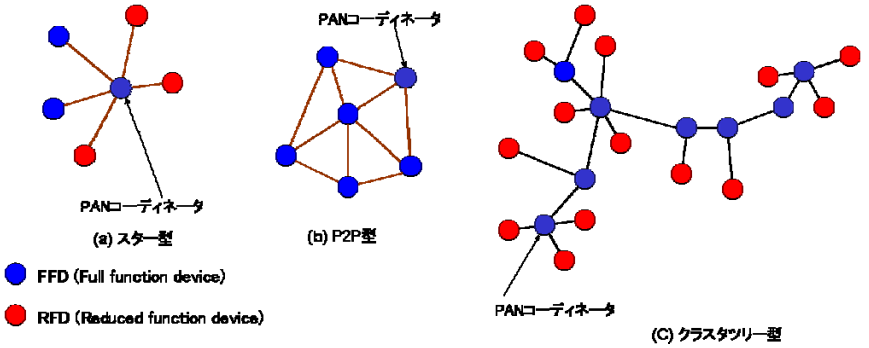


図 3・15　ネットワークトポロジー

(4)　ZigBee

(a)　ZigBee Alliance

ZigBee Alliance は，低コスト，低消費電力のオープンな国際標準無線方式を提供することを目的に設立された非営利の業界団体であり，2009 年 5 月時点で 200 社以上の会員が参加している．また，日本への ZigBee 普及を目的に ZigBee SIG-J（Special Interest Group-Japan）[4] も活動している．

(b)　ZigBee 仕様

ZigBee 仕様は，2004 年 12 月に初版が規定され，2006 年，2007 年に改版された．現在は，2 種類の NW スタックが定義されており，標準的な ZigBee スタックと，高機能対応した ZigBee Pro スタックがある．

ZigBee ネットワーク（PAN）は，ZigBee コーディネータ，ZigBee ルータ，ZigBee エンドデバイスから構成される．ZigBee コーディネータは，PAN 全体を管理する機能をもち，PAN に必ず一つ存在する．また，ZigBee コーディネータや ZigBee ルータはマルチホップ機能をもち，ネットワークの「幹」を構成する．ZigBee エンドデバイスは，中継機能をもたず，ZigBee コーディネータや ZigBee ルータにスター型に接続することにより，ネットワークの「葉」を構成する．

(c)　ZigBee の機能

(1) ルーチング機能

ZigBee では，クラスタツリー構造を利用したクラスタツリールーチングと，メッシュ構造で P2P 通信を行うテーブルルーチングをハイブリッドに利用できる．

(i) クラスタツリールーチング

図 3･16 にクラスタツリールーチングの例を示す．クラスタツリールーチングでは，ネットワークの幹を構成する ZigBee ルータや ZigBee コーディネータを経由して，マルチホップ通信を行う．

クラスタツリーの枝葉の構造によって固有の ID を割り当てるルールを採用しており，転

送先の ID を見ただけで，パケットを自分の上に転送すればよいか，下に転送すればよいかがわかる仕組みになっている．これにより，どの ID がどこに接続されているかを管理するルーチングテーブルをメモリ上に記憶しておく必要がなく，また転送先へのルートを送信前に探索する必要もないため，低コストで低消費電力のルーチングを実現できる．

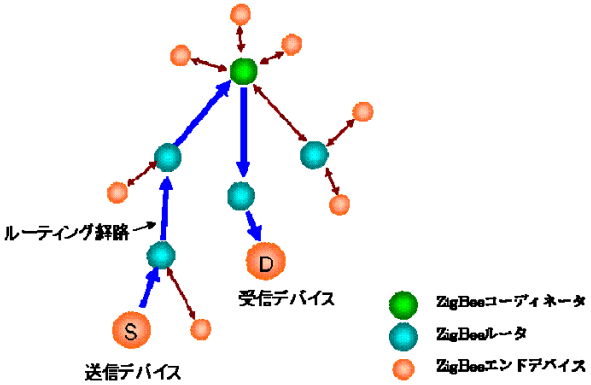


図 3・16　クラスタツリールーチング

(ii) テーブルルーチング

テーブルルーチングは IETF（Internet Engineering Task Force）の MANET（Mobile Ad Hoc Networking）WG において標準化されている AODV（Ad Hoc On Demand Distance Vector Routing）のアルゴリズムに従って動作する．

図 3･17 に AODV テーブルルーチングの例を示す．ZigBee デバイスでルーチング機能をもつのは，ZigBee コーディネータと ZigBee ルータのみであり，ZigBee エンドデバイスは機能を限定して低コスト化するためにルーチング機能をもっていない．このため，ZigBee エンドデバイスがテーブルルーチングによるマルチホップ通信を行う場合，ZigBee エンドデバイスが接続している ZigBee ルータが代わりに AODV の機能を実行する．したがって，ZigBee コーディネータ及び ZigBee ルータ間のみで AODV によるメッシュネットワークが構成されることになる．

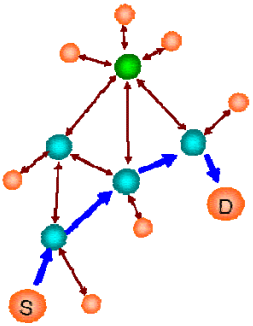


図 3・17　AODV テーブルルーチング

(iii) Many to One ルーチング

ユビキタスセンサネットワークでは多くのデバイスからのセンサデータを収集するケースが多いため，その手順を効率化するために，Many to One ルーチングが追加された．

図 3･18 に Many to One ルーチングの例を示す. まず, データを集めたいシンクデバイスが，フラッディングでソースアドレス（シンクデバイスのアドレス）と中継元のアドレスを覚えるコマンドをネットワーク全体に送る．フラッディングと反対向きの経路を各ルータが記憶したことになり，データ収集のためのルートが出来上がる．

従来のクラスタツリールーチングやテーブルルーチングでデータ収集を行う場合，すべてのデバイスからのルートを設定し，全ルートのアドレスを記憶する必要があったが，Many to One ルーチングでは，1 回のルート検索でルーチングテーブルを作成することができ，更に一つのシンクデバイスに対して，一つのアドレスを覚えるだけでよいため，低消費電力で低コストなデータ収集のためのルーチングを実現できる．

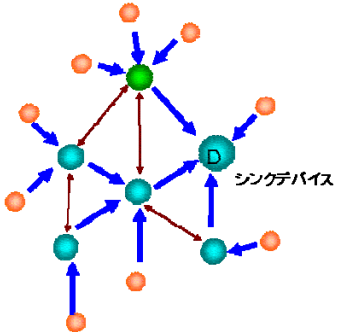


図 3・18　Many to One ルーチング

(iv) マルチキャストルーチング

複数の相手に効率よく伝送するためのマルチキャスト機能もオプション機能も追加された．

マルチキャストは，一つの相手にデータを送る通常のユニキャストと異なり，複数の相手にデータを同時に送る仕組みのことであり，IP マルチキャストと同様に，予め複数の相手を登録したマルチキャストアドレスを用意しておく必要がある．

図 3･19 にマルチキャストルーチングの例を示す．各ルータは，登録された複数のアドレスに対してそれぞれ転送先を判断するのではなく，マルチキャストアドレスに対して，通常のユニキャストと同じように転送先を管理しており，一つのマルチキャストアドレスを覚えるだけ複数の相手にデータを届けることができる．

複数の照明を一つのスイッチで制御する場合など，制御データをマルチキャスト伝送する場面が多いシステムでは，ユニキャストでルーチングするよりも，消費電力，低コストを実現できる．

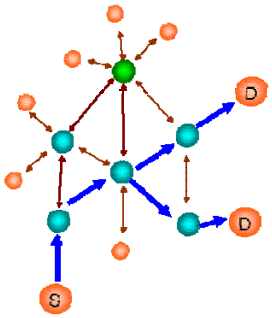


図 3・19　マルチキャストルーチング

(2) アドレッシング機能

ZigBee のネットワークアドレスとしては, IEEE 802.15.4 で規定されている 16 ビットショートアドレスを利用しており, IEEE 802.15.4 の規定外となっているアドレス割当方法を ZigBee が規定している.

(i) クラスタツリールーチング用アドレス割当

ZigBee では，クラスタツリー構造に従ってネットワークアドレスを割り当てる方法を規定している.

ネットワークごとに，各ルータに接続できる子デバイスの最大数（Cskip）やツリーの深さを予め決めておき，親デバイスに 1 を加えたアドレスを Cskip 間隔で子デバイスに割り当てる．**図 3･20** に Cskip = 4，ツリーの深さ = 4 の場合のアドレス割当の例を示す.

例えば，デバイス 2 の下には四つのデバイスがぶら下がることができるが，デバイス 3 しか接続していないので，デバイス 4，5，6 は空席となり，デバイス 2 の隣はデバイス 7 となる．デバイス 7 の下には既に最大数と同数の四つのデバイスがぶら下がっているため，これ以上，子デバイスは接続できない.

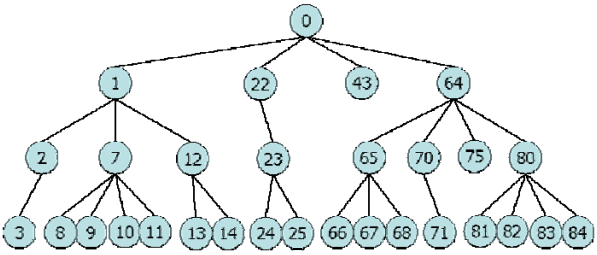


図 3・20　クラスタツリーのアドレス割当

(ii) その他のアドレス割当

ZigBee では，Cskip によるアドレス割当が必須ではなく，各ルータが予め割り当てられたアドレス空間の中で，子デバイスのアドレスを自由に割り当てることもできる.

更に ZigBee では，予めルータに対してアドレス空間を割り当てずに，各デバイスにランダ

ムにアドレスを割り当てることとし，ネットワーク内で重複していることが発見されたらアドレスを変更するという，簡易なアドレッシング方法なども規定されている．これにより，ルータごとの接続デバイス数の制限がなくなり，フレキシブルなネットワークを実現可能となる．

(3) セキュリティ機能

ZigBee は，低コスト，低消費電力を追求するため，共通鍵暗号方式を利用する．暗号方式は，IEEE 802.15.4 と同じ 128 ビットの AES ブロック暗号方式を使う．

鍵の種類は三つ定義されている．

* リンク鍵
* ネットワーク鍵
* マスタ鍵

リンク鍵は，二つのデバイス間で 1 対 1 に保持する鍵で，セキュアにユニキャスト通信をするために使われる．相手デバイスごとに異なる鍵を利用する．

ネットワーク鍵は，全デバイスに共通に保持する鍵で，ネットワーク内のすべてのデバイスと通信することができる．また，セキュアにブロードキャスト通信をすることができる．

マスタ鍵は，各デバイスがトラストセンタ及び任意のデバイスとの間で 1 対 1 に保持する鍵で，この鍵を使ってリンク鍵を生成する．マスタ鍵は，セキュアに各デバイスに記憶させる必要があるが，その方法は ZigBee では規定していない．設置した各デバイスに鍵の書き込み装置を有線で接続して鍵を書き込む方法などを想定している．

(4) その他の新しい機能

ZigBee-2006 以降，以下のような機能も追加された．

* デバイスが移動して他のルータに接続する手続きを簡略化するポータビリティ機能
* リンクが切れて元のルータに再接続する際に簡易接続するリジョイン機能
* 使用中のチャネルの干渉量が多くなった場合に，PAN 全体でチャネルを変更する機能
* 大きいサイズのデータを送信するために，パケットをフラグメントする機能

(d) アプリケーションプロファイル

ZigBee Alliance では，相互接続性を保証することも大きな目標としており，応用分野ごとに標準的なアプリケーションプロファイルを規定して，相互接続性を高めている．

これまで述べてきた機能は，応用分野によっては不要なものもある．必要な機能の組合せや，最適なパラメータの範囲を応用分野ごとに規定したものが，アプリケーションプロファイルである．照明のスイッチや空調の温度など，各プロファイルではその応用例で扱う属性を管理する仕組みも定義されている．

なお，アプリケーションプロファイルは，ユーザが自由に規定してもよいが，その場合は，他のユーザとの相互接続は保証されない．

主な標準のアプリケーションプロファイルは以下のとおりである．

* HA（Home Automation）プロファイル：ホームネットワーク向けプロファイル
* CBA（Commercial Building Automation）プロファイル：ビル管理向けプロファイル
* IPM（Industrial Plant Monitoring）プロファイル：工場管理向けプロファイル
* SE（Smart Energy）プロファイル：自動検針向けプロファイル

* WSA（Wireless Sensor Network Application）プロファイル：大規模環境モニタリングや資産管理，機械器具モニタリング向けプロファイル
* TA（Telecom Application）プロファイル：携帯電話を利用した各種サービス向けプロファイル
* AMI（Advanced Metering Infrastructure）プロファイル：電力・水道・ガスメータの読み取り向けプロファイル
* PHHC（Personal Home Health Care）プロファイル：健康モニタリング向けプロファイル

■参考文献

1) ZigBee Alliance, http://www.zigbee.org/
2) IEEE802.15, http://grouper.ieee.org/groups/802/15/
3) IEEE802.15.4, “Wireless Medium Access Control (MAC) and Physical Layer (PHY) specifications for Low Rate Wireless Personal Area Networks (LR-WPANs), ” http://www.ieee802.org/15/pub/TG4.html
4) ZigBee SIG-J, http://www.zbsigj.org/

3-7-2 IEEE 802.15.4a と UWB

（執筆者：河野隆二）［2010 年 5 月 受領］

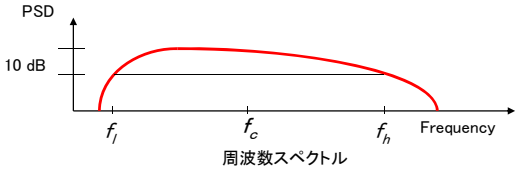
高速センサネットワークを理解するためには，超広帯域 UWB（Ultra Wideband）無線技術の原理を知る必要がある．また，UWB 技術による低速無線 PAN（Personal Area Network）の国際標準として，既に標準化が 2007 年 3 月に完了している標準が IEEE 802.15.4a である．また，2010 年度中の完了が予定される無線 BAN（Body Area Network）の標準 IEEE 802.15.6 にも UWB 技術によるものと狭帯域無線技術によるものがある．

これらの基盤技術である UWB 無線技術の原理，特徴，応用を解説し，特に，UWB 技術による低速無線 PAN の標準 IEEE802.15.4a について紹介する．

(1) UWB 無線技術の定義と原理

UWB 方式は，数 GHz の帯域幅にわたって電力スペクトル密度の低い信号を用いて通信を行う方式の総称である．UWB 信号の定義は，**図 3･21** に示すように，送信機の部分的帯域幅として 500 MHz 以上か，または中心周波数（最高と最低周波数の和の 1/2）に対する占有帯域幅の比，すなわち比帯域幅 =(帯域幅)/(中心周波数) が 20 %以上の伝送方式である．

比帯域幅 $BW = 2\dfrac{f_H - f_L}{f_H + f_L} = \dfrac{f_H - f_L}{f_c}$



- **UWB 帯域幅**
  - 比帯域幅 = (帯域幅)/(中心周波数) が、通常25%以上（米DARPA）
  - 比帯域幅 > 20% または，500MHz以上の占有帯域（米FCC，日本総務省）

図 3・21 UWB 信号の定義

UWB 方式とは，**図 3･22** に例示するように，スペクトルを広帯域にする多様な方式の総称である．その中で，UWB 方式は二つに大別される．

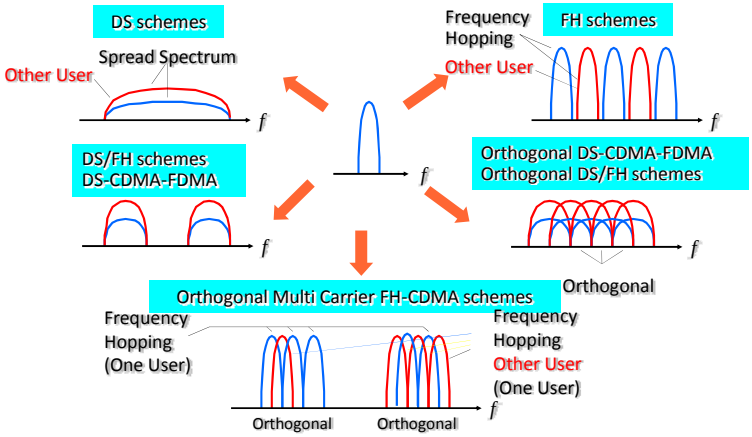


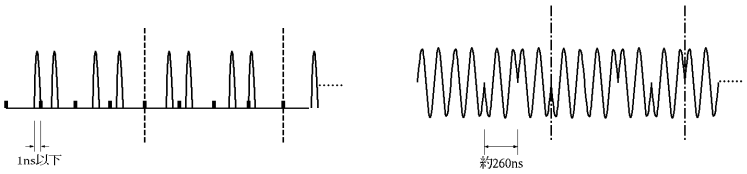
図 3･22　UWB 無線 PAN･センサネットワークで検討されている SS，OFDM などの電力スペクトル

一つは，搬送波による変調を用いた直接拡散（Direct Sequence：DS）や周波数ホッピング（Frequency Hopping：FH）などのスペクトル拡散（Spread Spectrum：SS）方式，OFDM などのマルチキャリア方式，及びそれらの組合せにより，超広帯域無線伝送を実現する方式である．これらは既存技術による UWB 無線伝送の早期実現などの視点からマイクロ波帯における無線 PAN への応用が検討されている．

もう一つは，狭義の UWB 無線であるインパルス無線（Impulse Radio）方式である．搬送波による変調を用いず，1 ナノ秒以下の数百ピコ秒程度の非常に短いインパルス状のパルス信号列を無線で送受信する．

(2)　UWB 無線技術の特徴

図 3･23 に Impulse Radio による UWB 信号波形を，通常の 2 相位相変調（BPSK：Binary Phase Shift Keying）信号波形と比較して示す．図に示すように，インパルス無線方式ではコサイン波のような搬送波による変調をせずにパルスを複数送信する．そのため，UWB 信号は BPSK



(a) Impulse RadioによるUWB時間信号波形
(時間幅の非常に狭いパルスを送信)

(b) 2相位相変調(BPSK)による時間信号波形
(搬送波に情報を乗せて送信)

図 3･23　Impulse Radio による UWB 信号と搬送波を用いた位相変調信号の比較

などの被変調信号に比べても超広帯域（数 GHz の帯域幅）であり，電力スペクトル密度も 1 MHz 当たり 10 ナノワット：10 nW/MHz 以下と低いので，他のシステムが共存しても干渉を与えにくいばかりでなく，他のシステムからの干渉にも耐えられる．また､通常のスペクトル拡散通信方式と同様に秘話性・秘匿性に優れ，他の狭帯域通信に与える影響は小さいなどの特長をもつ通信方式である．超広帯域に拡散されるので，よりその特長がさらに強調される．

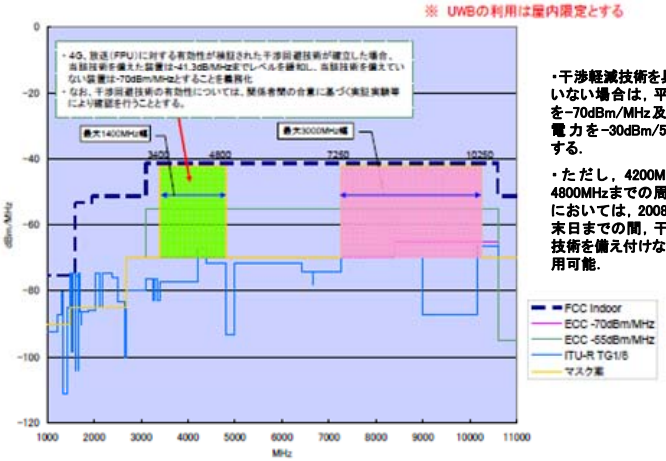
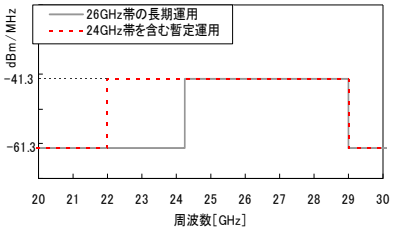
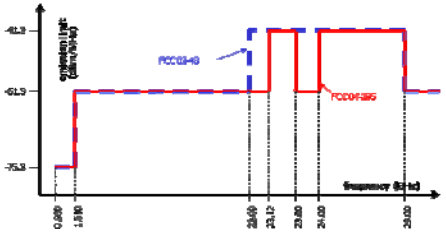


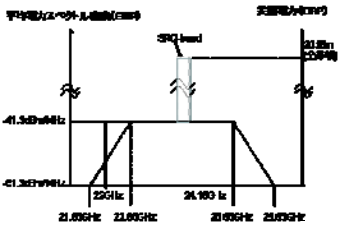
図 3・24　日本のマイクロ波帯 UWB スペクトルマスク



(a) 日本のミリ波帯スペクトルマスク



(b) 米国のミリ波帯スペクトルマスク



(c) 欧州のミリ波帯スペクトルマスク

図 3・25　ミリ波帯 UWB スペクトルマスク

更に，パルスの時間幅が非常に小さいため，マルチパスを細かく分解でき，RAKE 受信が可能となるので，マルチパスにも強い方式である．また，UWB では 1 ns 以下のパルス（モノサイクル）からなるベースバンド信号を複数用意する．そのモノサイクルをユーザごとに固有のタイムホッピング（TH）系列分だけシフトさせて送信する．そのため，多元接続する際，他局のモノサイクルが衝突（ヒット）したときに誤りとなり，このヒットする確率が誤り率などのシステム性能を左右する要素となる．

UWB では非常に広い帯域を用いることに依存して，次のような特長がある．

(1) マルチパスの遅延時間を 1 ns 以下に分解できる．この結果，マルチパスフェージングの影響を十分抑えることができる．
(2) この高いパス分解能力により UWB による室内の高品質近距離無線通信が可能となる．
(3) また，フェージングの影響が低く抑えられ，送信電力が少なくてすむ．

更に，送信電力の低い UWB では電力スペクトル密度が非常に低くなるので他の狭帯域伝送に影響をほとんど与えない．

一方，UWB を商用化するために検討すべき課題としては次の問題点がある．

＜UWB の問題点＞

(1) 超広帯域で時間幅の非常に短いパルスを発生させる回路，素子，および超広帯域アンテナ・高周波回路の製造
(2) 受信時にパルス位置ずれの検出精度
(3) マルチパス環境下でのパルス符号間干渉
(4) マルチユーザ環境下でのパルス衝突によるユーザ間干渉（システム内干渉）
(5) 周波数共用（共存システム）によるシステム間干渉

超広帯域スペクトルを利用できる周波数帯が電波法上困難であったが，現在では電波法により，UWB 無線システムが他の無線システムと周波数共用できる放射電力の規定が定められ，実用化されている．**図 3･24** にマイクロ波帯，**図 3･25** にミリ波帯（車載レーダー対象）の UWB 無線システムの送信機からの放射電力の上限を示すスペクトルマスクを示す．

(3) UWB 無線技術の主な応用

(a) 無線 PAN，センサネットワーク

商用化に向けて最も盛んに標準化や法制化が研究開発と共に進められている UWB システムは，無線 PAN（Personal Area Network）である．複数のパーソナルコンピュータ（PC）やディジタルビデオカメラ，TV，プリンタなどの情報機器に組み込ませて，無線 LAN のような基地局を介さず P2P（Peer-to-Peer）の対等分散により相互を無線によって結び，5～10 m の近距離において動画像信号などの情報伝送を数百 Mbps 程度（USB version2.0：480 Mbps）の超高速伝送速度で高速に伝送することが可能となる．標準化組織 IEEE 802 では，IEEE 802.15.4a として UWB 方式による無線 PAN が標準化されている．PAN は，室温を測るセンサ，室内の明るさを測るセンサ，人間を感知するセンサなどのセンシングのためのセンサネットワークばかりではなく，それぞれ UWB デバイスを搭載し，互いに通信を行いながら自動的に人の在・不在を確認しつつエアコンの調整を行い，明かりをつけるといったことなどが特別な配線などを必要とせずに可能となる．

(b) 無線ボディエリアネットワーク（BAN）

UWB の特長である周波数スペクトル密度が極めて低く，PC や医療機器からの放射雑音以下であることから，医療機器や人体に与える干渉や侵襲性がほとんどないことにより，人体の周りで用いる BAN（Body Area Network）に応用できる．特に，心電図，脳波，血糖値などの生体情報のセンシング，インスリンポンプやカプセル内視鏡などの遠隔制御などの医療用に用いる身に付けるウェアラブル BAN や体内に植え込むインプラント BAN に応用できる．医療以外のエンターテイメントなどにも応用され，IEEE 802.15.6 として無線 BAN の標準化が行われている．

(c) 準ミリ波帯（24 GHz 帯，26 GHz 帯）・ミリ波帯（77 GHz 帯）車載レーダ

通信と測距が同一 UWB システムで同時に実現できることから，24 GHz 帯における ITS（車車間通信・測距など）への応用があげられる．**図 3･35** に UWB システムの許容可能放射電力を示すスペクトルマスクを示す．UWB レーダは UWB 通信以前の UWB の起源であるインパルスレーダ技術である．従来型レーダは測距における距離分解能が数十 cm から数 m 程度の分解能であるが，UWB レーダは数 mm から数 cm の高分解能を有する．従来型レーダでは目標物を点としてモデル化し目標の距離，位置測定，目標探知を行うが，UWB レーダは目標の各部散乱，自然共振などの合成モデルによる目標のプロファイル（形状）の測定，目標識別が可能となる．送信波形が伝搬路で受ける波形歪みを含む目標の応答として受信波を仮定し，目標のプロファイルを測定することができる．そのため，高分解能で複数目標や構造の複雑な目標に対して，インパルス応答（レンジプロファイル）として正確に認識することができる．

(d) 低速無線 PAN の標準： IEEE 802.15.4a

UWB 高速センサネットワークのなかで，比較的に低速なものが低速無線 PAN の IEEE 802.15.4a である．IEEE 802.15.4a では，直接拡散（Direct Sequence：DS）変調を用いたインパルスラジオ方式（Impulse Radio：IR）が採用されている．その理由の一つとして，高速データ伝送だけでなく正確な測距を実現することが求められているからである．また，対象とする応用や利用領域が広範囲であるため，それらに応じて複数の復調方式やパルス形状などのオプションが基本モード以外に設定されていることが特徴である．

(1) バンドプラン

表 3･5 に低速無線 PAN の標準 IEEE 802.15.4a のバンドプランを示す．WLAN などとの干渉を避けるため，UWB の周波数バンドは 3.1～4.9 GHz のローバンドと 6 GHz 以上のハイバンドとに分けられている．ここで，チャネル No.1 はサブ GHz，No.2～5 はローバンド，No.6～16 はハイバンド用である．ローバンドにおいて，No.4 は必須であり，その他はオプションである．また，ハイバンド用のチャネル No.6～16 は日本と EU の輻射電力マスクを考慮に入れたものである．更に，No.5, 8, 12, 16 は比較的広い帯域幅をもっているが，これはより高速なデータ通信，及びより高精度の測距をサポートするために用いられる．IEEE 802.15.4a では，3.1 GHz～10.6 GHz の UWB の周波数バンド以外に，2400～2483.5 MHz のチャープ方式を用いるバンドおよび 1 GHz 以下の 3100～10000 MHz のバンドも標準に含まれるが，ここでは省略する．

表 3・5　低速無線 PAN（IEEE 802.15.4a）のバンドプラン

バンドグループ	チャネル番号	中心周波数	チップレート (Chip Rate)	Mandatory/Optional
		(MHz)	(MHz)	
1	No. 1	399.36	499.2	Optional
2	No. 2	3494.4	499.2	Optional
	No. 3	3993.6	499.2	Optional
	No. 4	4492.8	499.2	Mandatory in low band
	No. 5	3993.6	1331.2	Optional
3	No. 6	6489.6	499.2	Optional
	No. 7	6988.8	499.2	Optional
	No. 8	6489.6	1081.6	Optional
4	No. 9	7488	499.2	Optional
	No. 10	7987.2	499.2	Mandatory in high band
	No. 11	8486.4	499.2	Optional
	No. 12	7987.2	1331.2	Optional
5	No. 13	8985.6	499.2	Optional
	No. 14	9484.8	499.2	Optional
	No. 15	9984	499.2	Optional
	No. 16	9484.8	1354.97	Optional

(2) データ伝送速度とプリアンブル系列

IEEE 802.15.4a では，高精度測距が特徴であるため，データ伝送速度は比較的に低速であるが，0.811 Mbps を基本モードとし，0.1，0.811，3.24，6.49，12.97，26.03 Mbps のオプションモードがある．プリアンブル部分は，データの同期捕捉と測距のための信号の先頭を同期追尾するために用いられる．**表 3･6** にプリアンブル長を示す．

表 3・6　低速無線 PAN（IEEE 802.15.4a）のプリアンブル長

符号長	プリアンブル Index	Mandatory /Optional	平均 PRF (MHz)	プリアンブル長	時間長
31	**1**	**M**	**15.875**	**64 symbols**	**124.976 uS**
31	**2**	**M**	**15.875**	**256 symbols**	**500 uS**
31	**3**	**M**	**15.875**	**1024 symbols**	**2 mS**
31	**4**	**M**	**3.96875**	**64 symbols**	**500 uS**
31	**5**	**M**	**3.96875**	**256 symbols**	**2 mS**
31	**6**	**M**	**3.96875**	**1024 symbols**	**7.998 mS**
127	**7**	**O**	**127.48**	**64 symbols**	**32.907 uS**
127	**8**	**O**	**127.48**	**256 symbols**	**131.627 uS**
127	**9**	**O**	**127.48**	**1024 symbols**	**526.51 uS**

同期検波と非同期検波を用いた受信機を同時にサポートするために，符号系列にはターナリ符号（Ternary Code）を用いている．符号長 31 チップと 127 チップの PBTS 符号（Perfect Balanced Ternary Sequences）が使用される．PBTS は完全な周期自己相関特性を有するため，プリアンブルにおけるチップとシンボル同期，チャンネル推定および測距のための先頭波検出に好都合である．31 チップの PBTS 符号で最も良い自己相関特性を有するものは 8 個ある．様々なチャネル条件に対応するため，プリアンブルの長さは 16，64，1024，4096 シンボルなどを用いることを可能としている．

(3) **パルス形状**

IEEE 802.15.4a において，共通に用いられる基本パルスはルートレイズドコサインパルス（Root Raised Cosine Pulse）である．その時間波形 $r(t)$ を式(1) に示す．

$$r(t) = \sin c\left(\frac{\pi t}{T_c}\right)\frac{\cos\left(\pi\beta t/T_c\right)}{1-\left(2\beta t/T_c\right)^2} \tag{1}$$

ここで，ロールオフファクタは $\beta = 0.6$ であり，T_c はパルス時間幅である．

これを基本パルスとするが，その他のパルスについても，上記ルートレイズドコサインパルスとの相互相関係数が 0.5 ns のタイムスパンにおいて 0.8 以上で，サイドローブの相互相関係数が 0.3 以下であれば，基本パルスの代わりに利用できる．すなわち，パルス波形 $p(t)$ が基本パルス $r(t)$ との間の相互相関関数 $\phi(\tau)$

$$\phi(\tau) = \frac{1}{\sqrt{E_r E_p}}\int_{-\infty}^{\infty} r(t)\,p^*(t+\tau)dt \tag{2}$$

に対して，相互相関係数$\phi(0)$

$$\phi(0) = \frac{1}{\sqrt{E_r E_p}}\int_{-\infty}^{\infty} r(t)\,p^*(t)dt \tag{3}$$

が上述の条件を満たす．これはルートレイズドコサインパルスを基本パルスとする受信機でその他のパルスでも同等に受信できることを保証するためである．また，基本パルス以外に利用してもよいオプションパルスとして，①線形合成パルス，②チャープ UWB パルス，③ Contineous パルス，④Chaos パルスなどが採用されている．これらは既存無線システムへの干渉を軽減する機能を高めたり，同時通信可能なピコネット数（SOP 数）を増加させるなどの目的で付加的に用いることが認められている．

(4) **変調方式と誤り訂正符号**

図 3･26 に IEEE 802.15.4a に採用された変調方式と誤り訂正符号のブロック図を示す．変調方式として，同期検波と非同期検波受信機を同時にサポートできる 2PPM（Pulse Position Modulation）＋BPSK 変調方式が用いられる．図 3･36 に示すように，パルスバースト（DS 符号）を用いて一つのビットを伝送するが，2PPM ではパルスバーストの位置をもってビット“0”とビット“1”を表す．更に，2PPM+BPSK では，同じ位置にあるパルスバーストに＋／－符号を付けてもう一つのビットを表す．同期検波受信機は上記二つのビットを検出し，2 bits/symbol の割当てとなる．これに対して，非同期検波受信機はパルスバースト位置のみを検出するので，1 bit/symbol の割当てとなる．

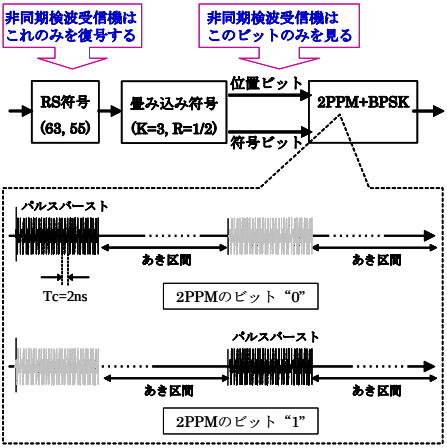


図 3・26　低速無線 PAN の標準 IEEE 802.15.4a の 2PPM + BPSK 変調と誤り訂正符号

誤り訂正符号として，リードソロモン RS(63,55)符号を内符号とし，符号化率 1/2 の畳み込み符号（拘束長 $k = 3$）を外符号とする連接符号が採用されている．良好な符号性能とシンプルな構成が決め手となっている．RS(63,55)符号は生成多項式

$$g(x) = \prod_{k=0}^{7} \left(x + a^k \right)$$

により構成される組織符号である．a は GF(2^6)上の 2 元原始多項式 $1 + x + x^6$ の根 $a = 010000$ である．また，非同期検波受信機をよりシンプルな構成にするため，非同期検波受信機は RS(63,55)符号のみを復号する．