

修士論文 2009 年度（平成 21 年度）

広域センサーネットワークにおける実践的な移動ノードの管理

慶應義塾大学大学院政策・メディア研究科
佐藤泰介

修士論文 2009 年度（平成 21 年度）

広域センサーネットワークにおける実践的な移動ノードの管理

論文要旨

人やモノ、自動車などの移動体にワイヤレスセンサノードを取り付け、それらが動きまわることによって、広域でかつきめ細かいセンシングを行うことができる。取得したセンサ情報は自宅や職場に設置したセンサーネットワークで情報システムに取り込む。この場合、地理的な位置が離れていても、ある移動ノードに関連するセンサーネットワークは、サービスや管理ポリシーが同一であることが望ましい。本論文は、インターネットを用いて、地理的に離れたセンサーネットワークを一つの PAN (Personal Area Network) として実現する方法 (PAN トンネリング) を提案し、ZigBee (IEEE 802.15.4) を用いた実装により提案方法の妥当性を示す。PAN トンネリング実現のためには、MAC 層以上の情報を IP ネットワークを通じて、トンネルの片側からもう一方に伝えるとともに、必要に応じて MAC 層の変換とフィルタリングを行う必要がある。論文では、ZigBee の代表的なプロトコルスタックである ZStack と組み込みコンピュータのプログラミングによって、これを実現した。実現した PAN トンネリング手法のスループットを実測により評価した結果、現在の実装で MAC ペイロード 20 byte のフレームを 40 packet/sec 程度の頻度でトンネリングが実現できること、そのボトルネックは現在使用している SoC のシリアルインターフェイスにあることを明らかにした。

キーワード

実空間コンピューティング センサーネットワーク ZigBee
移動ノード PAN トンネリング

慶應義塾大学大学院政策・メディア研究科
佐藤泰介

Practical Management of Mobile Nodes in Wide-area Sensor Networks

Abstract

Numerous mobile wireless sensor nodes attached to things, human and automobiles are essential to realize a wide area sensor network. The collected sensor data need to be retrieved wirelessly in a personal area network (PAN). Connection of remote geographical areas, working place and home for example, as a PAN such that mobile sensor nodes appreciates the same service and the same management policy, is therefore essential to wide area sensor network. This research presents PAN tunneling for ZigBee (IEEE 802.15.4) sensor network, which transparently connect geographical areas by tunneling MAC frame over the Internet. The necessity of MAC address translation and MAC frame filtering are identified. PAN tunneling is realized by using ZStack, one of the representing ZigBee protocol, and embedded computer programming. Measured PAN tunneling throughput is 40 packets/sec with 20bytes MAC payload. The bottle neck is identified to be serial interface of SoC.

Key Words

Realspace Computing Sensor Network ZigBee
Mobile Node PAN Tunneling

Keio University Graduate School of Media and Governance
SATO Taisuke

目次

第 1 章	序論	7
1.1	実空間コンピューティング	7
1.2	広域センサーネットワーク	8
1.3	研究の目的	10
1.4	本論文の構成	10
第 2 章	広域センサーネットワークの通信技術に関する考察	11
2.1	広域センサーネットワークの通信技術の要求事項	11
2.2	従来研究と問題点	13
2.3	IEEE802.15.4 と ZigBee	14
2.3.1	IEEE802.15.4	16
	PHY レイヤ	16
	MAC レイヤ	17
2.3.2	ZigBee プロトコルスタック	17
2.3.3	ZigBee ネットワーク	18
2.3.4	ZigBee ルーティング	19
2.4	ZigBee ネットワークの広域化手法	20
2.5	これまでの試み	21
2.6	本論文の手法が有用な状況	23
第 3 章	ZigBee PAN トンネリング	25
3.1	MAC レイヤ接合による PAN の連結	25
3.2	PAN トンネリング	26
3.3	実装環境	27
3.3.1	ZigBee システム	27

3.3.2	IP ネットワーク通信機器	28
3.4	トンネル両端のルーティング	29
3.5	PAN 間通信フレームのフィルタリング	29
3.6	PAN トンネリング実験	30
3.7	PAN トンネリングの性能評価	32
第 4 章	結論	34
	参考文献	37
付録 A	ZStack を利用したソフトウェア開発	39
A.1	IAR Embedded Workbench MCS-51 での ZStack のコンパイル	39
A.2	MAC フレームの入力	40
A.3	MAC フレームの出力	40
A.4	Promiscuous モード	41

目次

2.1	ZigBee による位置計測の精度と ZigBee ノードの低消費電力性能	15
2.2	IEEE802.15.4 MAC フレームフォーマット	17
2.3	ZigBee プロトコルスタック	18
2.4	ZigBee のノードの種類	19
2.5	ツリールーティングにおける Cskip の構造	20
2.6	上位エンティティにおける情報集約	21
2.7	デジタルサイネージ実験で本学 SFC 構内に設置した PANs	22
2.8	複数の PAN を連結した具体例	24
3.1	PAN トンネリングによる ZigBee ネットワークツリーの連結	26
3.2	PAN トンネリングでのフレームの動き	27
3.3	CC2431 を使用した開発・評価ボード	28
3.4	トンネル両端のルートの確立とデータ伝送	30
3.5	PAN トンネリング実験システム	31
3.6	PAN トンネリング試験フレーム	31
3.7	PAN トンネリングによるパケットロス	32
3.8	トンネルの各段階でのパケット転送成功率	33

表目次

2.1	2.4GHz 帯 IEEE802.15.4 の物理通信方式	16
2.2	ZigBee によるセンサーネットワーク実験のネットワーク構成	23

第1章

序論

本章では、実空間の事象をコンピュータネットワークの情報処理能力で支援する実空間コンピューティングと、それを実現する情報通信基盤である広域センサーネットワークについて述べ、研究の目的を示す。

1.1 実空間コンピューティング

コンピュータは様々な領域で広く利用され、その情報処理能力は現在の社会において欠かすことのできない要素となっている。特に、インターネットが普及し、多くのコンピュータがネットワークに接続されるようになってきてからは、実際の我々の生活の中にもコンピュータとネットワークによる幅広い恩恵を享受するようになってきている。コンピュータおよびインターネットは今後も我々の生活をより豊かに、また、現在では実現できていない新しいサービスをもたらす可能性を持っている。

そのため、人々の社会は、もはや我々が暮らす物理的な実空間だけでなく、インターネットによって構成されたコンピュータネットワークによる情報空間上にも形成されている。とくに Web をメインとしたインターネット上のコミュニティの力は強く、独自の社会を形成している。しかし、情報空間上での社会やコミュニティと、我々の生活空間（実空間）での社会やコミュニティは、別個のものとして考えられることが多い。その場合、利用できるサービスもまた別個のものである。

現在のインターネットは、主に文字やデータなどによって情報化されたコンテンツを流通、共有、利用するためのプラットフォームとして成熟しつつあるが、実際に我々が生活する生活空間の情報の処理に関しては、未だに基盤としては確立されていない。我々が生活する生活空間、即ち実空間に対して、コンピュータの持つ高度な情報処理能力を適用す

ることができれば、直接的に生活を支援する様々なアプリケーションが実現できるようになる。

このようなアプリケーションを実現するためには、実空間の様々な事象を観測、認識、伝達、共有、フィードバックする新たな仕組みが必要になる。すなわち、物理的な事象の情報空間との間の入力（検出）と出力（反映）を行うインターフェイスが、実空間の情報処理を担う社会基盤として存在しなければならない。“センサネットワーク”は、実空間から情報空間への入力インターフェイスの一要素である。実空間上での事象を、既に大きなパワーをもった情報システムと接続することで、実空間の様々な情報を情報空間に取り入れることができるようになり、既存の情報サービスを実空間指向にしていくことができる。このような試みを本論文では“実空間コンピューティング”と呼ぶ。

1.2 広域センサーネットワーク

実空間コンピューティングの実現のためには、情報空間と実空間のインターフェイスとなるデバイスが前提となり、そのようなデバイスのためのネットワークが必要である。しかし、そのネットワークを構成する情報通信技術に対する要求事項は、従来のインターネットなどのものと大きく異なる。

センサやアクチュエータは、PCのような通常の計算機を用いてインターネットに直接接続することも可能である。しかし、より多数のセンサやアクチュエータを環境に設置するためには、インターネットと異なる別個のネットワークが必要である。

なぜならば、センサやアクチュエータのほとんどはきわめて安価で、また小型である。例えば温度は熱電対、照度はカドミウムセンサ、音響はマイクロホンなどで検出でき、力学的動作をモータ、光をLED、音響をスピーカなどで反映できる。これらのデバイスは大量生産製品として生産されており、安価で小型で入手性が高い。また、デジタルインターフェイスを備えたワンチップの実装も存在する。これらのセンサやアクチュエータを、高価なPCや計算機資源の必要なインターネットに直接接続するよりも、ミニマムな機能をもったネットワークに収容するほうが、多数のセンサやアクチュエータを環境に設置できるため、実空間コンピューティングの実現に有利である。センサネットワークはそれらの小さなデバイスのための通信基盤である。

センサーネットワークは環境に多数設置された安価なセンサーノードが自律的に構成するネットワークである。軍事利用にその端は発し、現在その適用範囲は例えば気象モニタリング、ホームオートメーション、セキュリティ、医療援助など多岐にわたり、特定のアプリケーションを実現するための技術ではない。しかし、現在のセンサーネットワークは

それらのアプリケーションごとに設計され敷設されている。多様なセンサやアクチュエータのための多目的なネットワークとしてのセンサーネットワークが必要である。

ノードが自律的にネットワークを構成する技術としては、アドホックネットワークも挙げられる。アドホックネットワークとは、無線通信ができるデバイス同士がインフラとしてのネットワークが存在しない環境下で、相互通信により自律的に構成するネットワークである。センサーネットワークに関するサーベイ [1] によれば、両者の違いは次のような点である。

1. センサネットワークのノードの数はアドホックネットワークのそれと比較してとても大きい
2. センサノードは密に配置される
3. センサノードは障害を起こしやすい
4. センサネットワークのトポロジはとても頻繁に変化する
5. アドホックネットワークが point-to-point 通信をベースにするのに対し、センサーネットワークは通信のパラダイムとしてブロードキャストが主となる
6. センサノードは電源、計算機能力、メモリが制限されている
7. センサノードはオーバーヘッドの大きさとセンサノードの多数さから、グローバルな識別子を持たないことがある

このうちの一部、とくに 4 については技術的な制約から対応できていない実装も多いが、概念としてはアドホックネットワークよりも低機能で価格の安いノードを前提とし、それを密に配置することできめこまかい情報を取得するネットワークであるといえる。本論文では、これらの相違点のうち、とくに 4 と 6 に着目した。4 はすなわちノードの移動や参加離脱が高いという点、6 はネットワークの前提となる通信技術は低消費電力で低速のものとなり、またネットワークの自律的な構成には、エンドノードの計算機資源への負荷を抑える手法を用いる必要があると解釈できる。

アプリケーションによらず利用されるセンサーネットワークは、広域であることが望ましい。既にインターネットが世界共通のネットワークとして実現されており、どこにいてもインターネットに接続できれば同じサービスを受けられるように、地理的位置への透過性をもったセンサーネットワークが求められる。

しかし、センサーネットワークがインターネットと異なる大きな点は、実空間の情報を得るために用いられることである。そのため、センサーネットワークが広域であることは、広い範囲の実空間の情報を得られることを意味する。さらに、センサーノードが静止せず移動できるならば、得られる実空間の情報は増大する。センサーノードが同じ地理

的位置の情報を取得し続けるよりも、移動しながらその軌跡上の情報を得ることで、広域の情報を取得できるからである。この、広い地理的範囲をカバーし、センサーノードが移動するセンサーネットワークを本論文では“広域センサーネットワーク”と呼ぶ。

こうした移動ノードによる広域センサネットワークを実現するためには地理的に離れた場所を管理ポリシーやサービスが同一なセンサーネットワークとして接続する技術が必要である。例えば、自宅のワイヤレスセンサーを職場で管理したり、職場に忘れてきた物を自宅で確認することが考えられる。そのためには、職場と自宅を同じ PAN (Personal Area Network) に収容することが必要である。

1.3 研究の目的

本研究は、地理的に離れた位置を同じ PAN に収容する技術を PAN トンネリングと呼び、ZigBee (IEEE802.15.4) を用いて PAN トンネリングの問題を明らかにし、実装によって検討の妥当性を示すことが目的である。

1.4 本論文の構成

本論文の構成は、本章で研究の背景となる実空間コンピューティングと広域センサーネットワークについて述べる。第2章で、広域センサーネットワークで利用する通信技術について考察し、ZigBee が適していることを示し、これまでに行った実験について述べる。第3章で、ZigBee の PAN を MAC レイヤで連結することにより広域化する手法である PAN トンネリングについて、設計と実装および実験結果について述べる。第4章で本論文の結論を述べる。

第2章

広域センサーネットワークの通信技術に関する考察

本章では、まず広域センサーネットワークが利用する通信技術について考察し、ZigBeeがそれに適していることを述べる。また、これまでに ZigBee を利用して行った実験について述べる。

2.1 広域センサーネットワークの通信技術の要求事項

まず、広域センサーネットワークを実現するために、利用すべき通信技術についてまとめる。1.2 に示した特徴をもつセンサネットワークに利用できる無線通信技術は次の特徴を備えるものである。

■低消費電力 広域センサーネットワークではセンサノードは移動するため、電池などの限られた電源で稼働する。そのため、通信プロトコルや通信機器は低消費電力で設計されている必要がある。

さらに、人や小さなもの等とともに移動することも考慮すると、小型の電池での動作が望ましい。あまり電力を消費しないリモコンやラジオなどの一次電池として用いられる LR6 (単 3 型アルカリ) 乾電池は 1.5 Wh, LR6 の代替として利用される単 3 形ニッケル水素電池は 2.4 Wh, 主にカメラに用いられる一次電池である CR2 リチウム電池は 2.5 Wh, 携帯電話などに用いられるリチウムイオン二次電池は様々な形状のものがあるが、概ね 8,000 mm³ 程度で 3.0 Wh 程度の放電容量がある。この程度のサイズと放電容量を持つ電池は可搬デバイスによく利用され、違和感なく受け入れられている。広域セン

サーネットワークに用いられるノードもこの程度の容量で充電や電池交換の手間があまりないよう数日以上稼働することが求められる。

ただし、総てのノードが移動するアドホックネットワークや、総てのノードがデータを長時間保持し、接近した際に適宜通信を行って目的のノードまで転送する長遅延ネットワークは本研究では対象としない。そのため、ネットワークを構築するノードが存在し、有線で電源が接続されているか、鉛蓄電池のような大容量の電池をもっており、移動しないことを前提とする。そのため、ネットワークに存在するノードは移動するセンサーノードと、静止してネットワークを構築しデータの転送を行うノードに二分して考える。

■位置情報の取得が可能であること 広域センサーネットワークではセンサノードは移動するため、センサ情報のメタデータとしてセンサノードの位置が必要となる。また、屋内外にかかわらずネットワークを敷設することで、センサネットワークの基盤としての汎用性を高められるため、GPSなどの衛星通信やPHSなどのキャリアレベルの通信網によらず位置を計測できることが望ましい。

本研究で想定するノードの移動は人が移動する程度の1m/s程度である。またコンテキストとしても人や物がどこにいるか、どこにあるかを検出できることが必要条件である。そのため、必要な位置計測精度は数m程度とする。

また、前述のように電源と機器の大きさが限られているため、移動ノードは専用の機器を用いず、電力を消費せずに屋内外で位置情報が取得できることが望ましい。

■マルチホップでネットワークを構築すること 広域にネットワークを構築するため、ネットワークを容易に構築できねばならない。有線ネットワークではケーブルの敷設が必要で多数のノードを接続するのは不可能であるため、無線によりネットワークを構築する。また、センサーネットワークにおいてはノードの数は多数で安価であるために信頼性を得られない。また、ノードが移動するためにネットワークの構成を事前に決定することはできない。そのため、ネットワークは自律的に構成する手法をとる必要がある。

また、マルチホップではない無線通信方式では、ベースステーションからの無線到達範囲がそのままカバーエリアとなる。カバーエリアを大きくするためには大電力で通信を行う必要があり、電源の問題と電波行政上の問題の双方から難しい。

そのため、自律的にネットワークを構成し、小電力で近距離の無線通信をマルチホップで中継する通信技術を利用する必要がある。

■アプリケーションに依存しないこと 実空間ネットワークで利用される情報の性質上、そのため、アプリケーションに依存せず、ユーザが自身でネットワークを構成できる通信

技術を利用する必要がある。また、電波行政上、アプリケーションに依存せず比較的自由に利用できる ISM バンドを利用し、無線局免許が必要でないものが望ましい。

■機器が小型であること 本論文ではセンサーノードが人や物とともに持ち運ばれることを想定している。そのためあまりにも大きい機器は利用できない。とくに、アンテナの大きさは利用する周波数帯域に影響されるため、あまり低い周波数帯域を対象にしたプロトコルを利用するのは困難である。

2.2 従来研究と問題点

広域センサーネットワークを構成する方法は大きく 2 つに分類できる。一つは同一のアーキテクチャに基づくサービスを広域に展開する方法であり、もう一方の代表は ZigBee などの短距離無線通信システムを結合することで結果的に広域性を持たせる方法である。

前者の代表は広域ユビキタスネットワーク [2] である。これは統一したアクセスサービスをキャリアクラスで実現するものであり、280MHz 帯などを使いながらひとつの無線基地局で 5km 程度の覆域を構成し、その内部に含まれる多数の低速端末との通信を実現する。こうした無線通信の情報は固定網に流される。固定網内に、コンテキストに応じて送り先を変えられるなどの機能が加えられている。この手法では、ユーザが自在に新しいセンサーを加えることなど、サービスの多様性を実現することにつながりにくい。また、携帯電話や PHS による無線通信網も既に存在する。通信事業者はテレメトリングなどの用途のために、小規模の通信を多数の端末が行う際のタリフを用意していることがある。しかし、これらの通信技術は電力を消費するために、例えば自動販売機のような、電源が潤沢な機器にしか利用できない。

一方、後者の代表が、ZigBee などの比較的小規模なネットワークを構成する短距離無線通信によるネットワークを多数接続し、結果的に広域なネットワークを構成する手法である。例えば、Smart Energy Protocols over ZigBee [3] はメータリングのプロトコル DLMS/COSEM, IEC62056-21 を ZigBee 上に流すことでスマートメータの情報を共有することを提案している。6LoWPAN [4] は ZigBee を広域に接続するために、ZigBee に IPv6 機能を実装し、離れた場所の ZigBee ネットワークをインターネットで接続することを提案している。ZigBee Binding Automation [5] は ZigBee Cluster を使い、BACnet と呼ばれるプロトコルを ZigBee を使って集めることが検討されている。即ち、BACnet over ZigBee といえる。いずれの手法の場合も新たにプロトコルを開発したり、PDU などのデータスキーマの内容を変更したりなど、プロコルの変更が必要である。

2.3 IEEE802.15.4 と ZigBee

本論文では広域センサーネットワークを実現するための通信技術として、ZigBee [6] を前提とする。ZigBee は前節に述べた広域センサーネットワークで利用する通信技術の要求を満たす、次のような特徴を持っている。

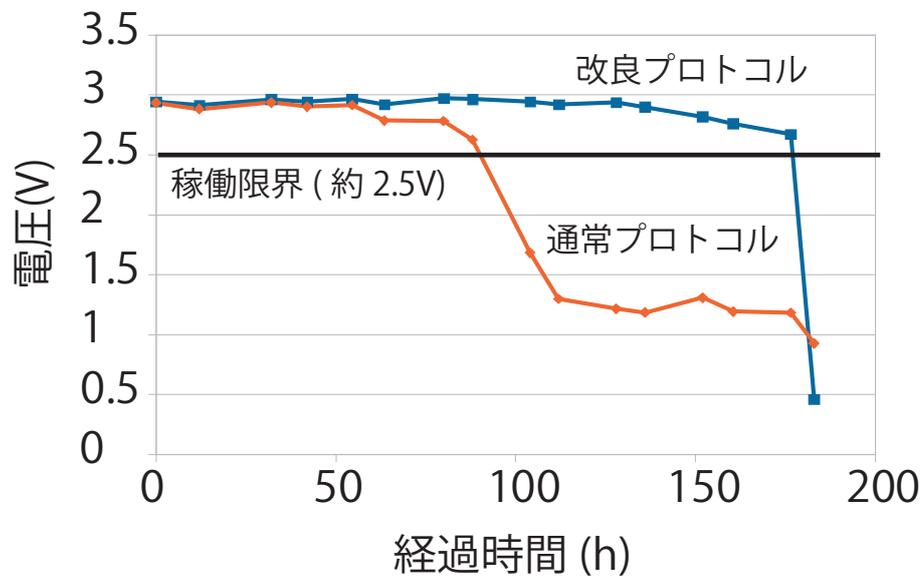
- マルチホップネットワーク
- 低データレート
- 低消費電力
- 受信電界強度による位置計測が可能
- ISM バンドである 2.4GHz 帯を利用し、日本においては機器が技術基準適合認定を得ていれば無線局免許は不要
- ワンチップの小型実装が多数存在

ZigBee はきわめて低消費電力なプロトコルである。低データレート通信を目的にしたプロトコルであり、またノードの利用する空中線電力は数十 mW 程度である。また、ノードのスリープ状態も仕様で定められており、通信を行う必要が無い場合は電源を利用しない。スリープ状態のノードが宛先のデータはネットワークを構成するノードがキャッシュするため、スリープ状態のノードは待機受信を行う必要すらない。本研究で利用したノードは、図 2.1(b) に示すように、位置計測を行うアプリケーションを動作させ続けても、移動ノードは CR2 電池で 1 ヶ月程度稼働することが実験から分かっている。ただし、位置計測のプロトコルはノードのスリープ間隔などの調整を行った。

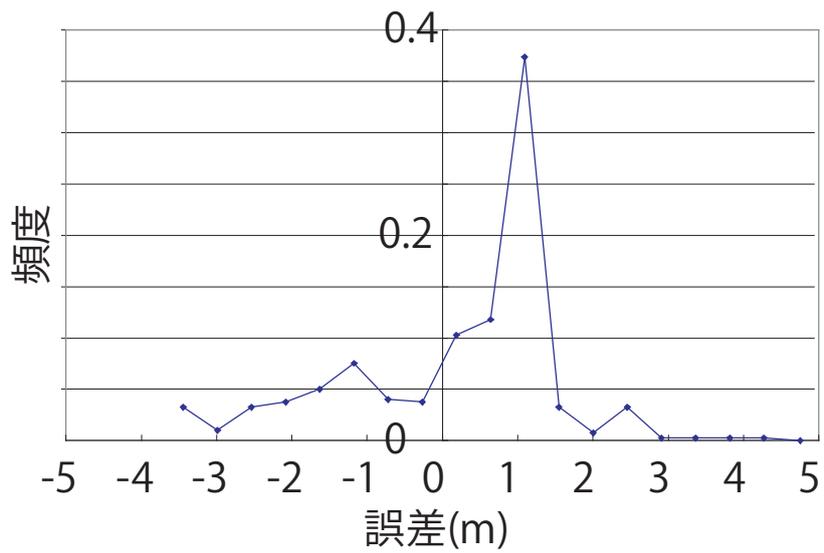
ZigBee ネットワークでの位置計測は受信電界強度による三角測量で可能である。図 2.1(b) に示すとおり、誤差はノードが静止している場合 1m 程度であることが実験から分かっている。また、位置計測アルゴリズムの改良によりノードが移動する環境下でも位置計測精度を静止状態クラスまで近づけることが可能である [7]。なお、位置計測の機構自体は仕様ではなく独自のアプリケーションであるため、スリープ状態の調整や位置計測アルゴリズムの改良により、ZigBee の仕様から外れることはない。

ZigBee はマルチホップでネットワークを構成する。ノード-ノード間の通信可能距離は 10m 程度だが、マルチホップでネットワークツリー（またはメッシュ）を構成することで、数百 m³ 程度のカバーエリアのネットワークを構築できる。

このような特徴をもつ ZigBee は ZigBee Alliance により仕様化され標準規格となっている。そのため、ZigBee を実装した安価な製品が存在し、安価なセンサのための通信技



(a) CR2 電池での 4 倍速稼働時における実測電池電圧



(b) 電界強度による位置計測実測誤差

図 2.1 ZigBee による位置計測の精度と ZigBee ノードの低消費電力性能

表 2.1 2.4GHz 帯 IEEE802.15.4 の物理通信方式

利用バンド	2.4 GHz 帯 (2,400MHz~2,483.5MHz)
周波数チャンネル数	16
周波数チャンネル間隔	5 MHz
周波数帯域幅	2 MHz
空中線電力	-3 dBm 以上
受信感度	-85 dBm 以下
変調方式	O-QPSK
シンボルレート	62.5 kSymbol/sec
データレート	250 kbps
日本における空中線電力規制	最大 10 mW/MHz

術として有用である。

2.3.1 IEEE802.15.4

ZigBee はその物理通信とメディアアクセスに IEEE802.15.4 [8] を利用する。IEEE802.15.4 は低消費電力な無線通信の protocols である。IEEE により仕様化され、標準規格となっている。IEEE802.15 シリーズは無線データ通信の protocols を定めた protocols シリーズであるが、IEEE802.15.4 はそのうち特に組み込み機器などの相互通信のために設計されている。その目的のために、低データレートで小電力の物理通信方式を利用し、複雑でない protocols 設計である。IEEE802.15.4 で構成される近距離通信のネットワークは WPAN (Wireless Personal Area Network), または PAN とよばれる。

PHY レイヤ

IEEE802.15.4 の PHY (物理) レイヤについて述べる。IEEE802.15.4 は ISM (Industry-Science-Medical) 目的の周波数帯を利用し、日本においては機器が技術基準適合認定を受けていれば無線局免許を受ける必要なく利用できる。日本における 2.4GHz 帯 IEEE802.15.4 の物理通信方式などについて表 2.1 にまとめる。

なお、実測によると、屋外で 100 m 程度、屋内では数十 m 程度の距離で通信が可能である。

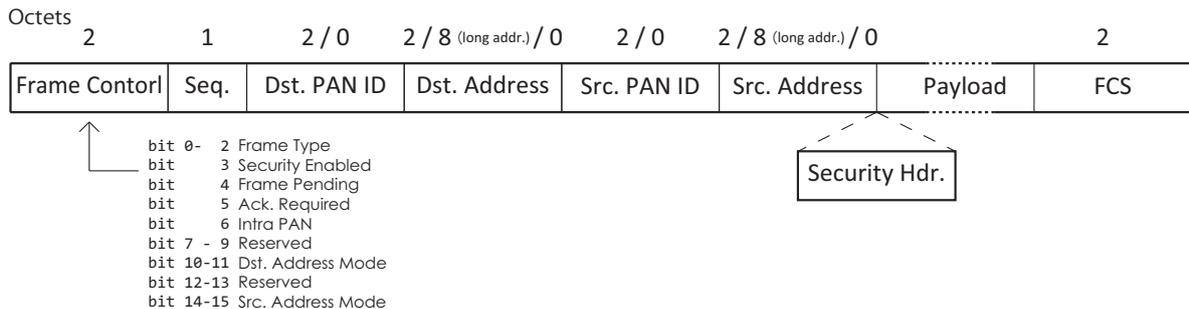


図 2.2 IEEE802.15.4 MAC フレームフォーマット

MAC レイヤ

IEEE802.15 の MAC (Medium Access Control) レイヤについて述べる。まず、IEEE802.15.4 では次の 2 つの識別子を利用する。

PAN ID IEEE802.15.4 ネットワークである PAN の識別子。16 ビット長。

MAC アドレス PAN 内でのノードの識別子。PAN 内で一意な 16 ビットの長のショートアドレスと、IEEE から割り当てを受ける 64 ビット長のロングアドレスの 2 種がある。

双方ともにブロードキャストのために PAN ID を特定しない場合は 0xffff を利用する。MAC フレームのフォーマットを図 2.2 に示す。PAN ID および MAC アドレスのそれぞれについて、Source および Destination が指定できる。必要がない場合は省略も可能であり、またロングアドレス、ショートアドレスはヘッダー中の Frame Control にて指定する。

2.3.2 ZigBee プロトコルスタック

ZigBee スタックは他のプロトコルスイートと同様に、いくつかのレイヤで構成される。PHY と MAC は IEEE802.15.4 のものを利用する。その上位に、マルチホップでネットワークを構成するための Network (NWK) レイヤがある。そのさらに上位の Application (APL) レイヤは Application Support Sub-layer によってイベントハンドリングなどが行われ、複数のアプリケーションが一つのノードで稼働できる。また、NWK Layer 以上の各レイヤの操作をアプリケーションとして抽象化するための ZigBee Device Object (ZDO)、及び暗号化などのセキュリティを提供する Security Service Provider が存在す

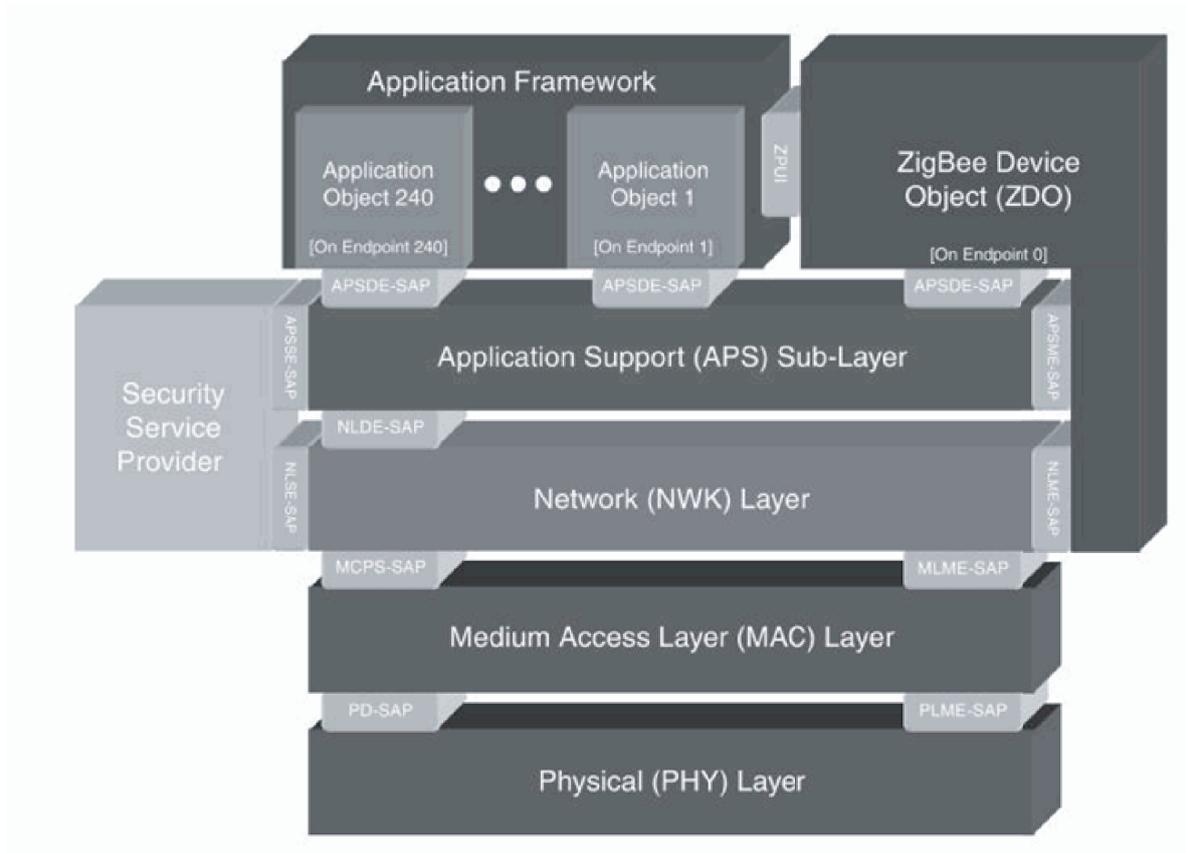


図 2.3 ZigBee プロトコルスタック

る。[9] からスタックの概要を引用し図 2.3 に示す。

2.3.3 ZigBee ネットワーク

ZigBee ネットワークは IEEE802.15.4 同様に PAN といい、3 種のノードで構成される。“ルータ”がマルチホップのネットワークを形成し、データ（フレーム）の中継を行う。また、ネットワークに1つ“コーディネータ”が存在し、ルータとしての機能を果たすと同時にネットワーク全体の制御を行う。“エンドデバイス”は機能の制限されたデバイスで、ルータとコーディネータに依存して通信を行う。図 2.4 にその概要を示す。

ZigBee は 2010 年 1 月現在 3 つのスタックプロファイルが存在する。スタックプロファイルは ZigBee スタックの機能を定めるもので、新しいスタックはツリー構造でないネットワークトポロジを構成できるなど、機能が拡張されている。しかし、その複雑さから対応していない ZigBee 実装も多いため、本論文ではいちばん簡易な ZigBee である

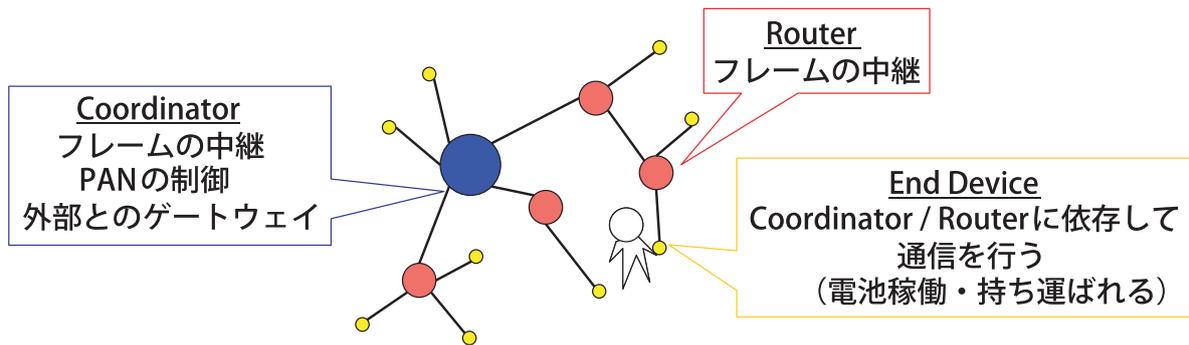


図 2.4 ZigBee のノードの種類

ZigBee Stack Profile 0x01 を利用する。

センサーネットワークのために ZigBee を使用する際には、ルータとコーディネータを設置し、エンドデバイスが移動しながら通信する。

2.3.4 ZigBee ルーティング

ZigBee (Stack Profile 0x01) でのツリートポロジにおけるルーティングは、NWK アドレスの空間を分割しつつ、ルーティング情報をアドレスに含めることによって行われる。ZigBee PAN にはそのアドレス空間の分割を行い、結果的にツリートポロジの制限をするパラメタが存在する。

Max Depth D

コーディネータから経由できるノード数 Depth の最大数。すなわちコーディネータからの最大ホップ数。

Max Children C

各ルータに接続できるノードの最大数。

Max Routers R

各ルータに接続できるルータの最大数。

Max Children はルータとエンドデバイスの双方を含むため、次のパラメタも自明に定義できる。

Max End Devices $E = C - R$

各ルータに接続できるエンドデバイスの最大数。

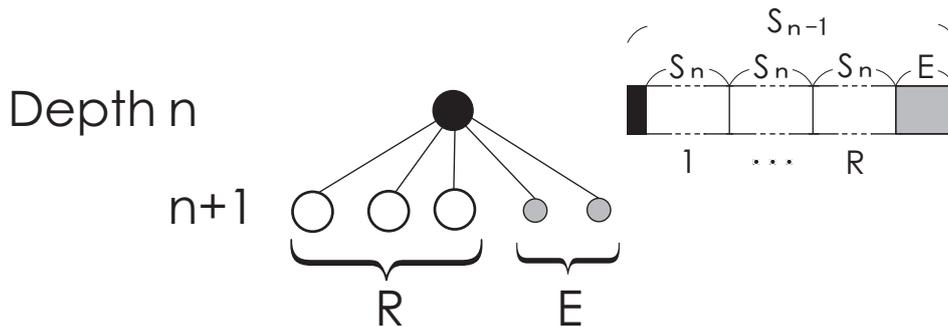


図 2.5 ツリールーティングにおける Cskip の構造

ノードは自身の識別子として NWK アドレスを 1 つ消費するが、ルータの場合は親ノードからアドレスを付与される際、自身の予期される最大の下流ノードのアドレスを同時に予約する。そのため、ルータは NWK アドレスのみで、フレーム宛先のノードが自身の上流か下流か判別できる。Depth d のルータが Depth $d + 1$ のノードに割り当てるアドレス数を Cskip という。Cskip の構造について図 2.5 に示す。Depth n における Cskip S_n は次のように表現できる。

$$S_D = 0$$

$$S_n = 1 + (S_{n-1} + 1) \cdot R + E$$

ZigBee はメディアが無線のデバイスである。そのためツリールーティングにおいては、自分宛でないフレームを受信した Router は、宛先アドレスが自己の Cskip の範囲内かどうかのみで、ルーティングを行うか決定できる。

そのため、ZigBee PAN に存在しえる最大のノード数 N は MAC ショートアドレス数の 65,535 にはならず、次の式で求められる。

$$N = 1 + S_0 \cdot R + E$$

2.4 ZigBee ネットワークの広域化手法

ZigBee ネットワークを広域化するためには PAN と地理範囲、およびその管理ドメインの分離が必要である。通常の ZigBee ネットワークは、PAN が一つの管理ドメインと

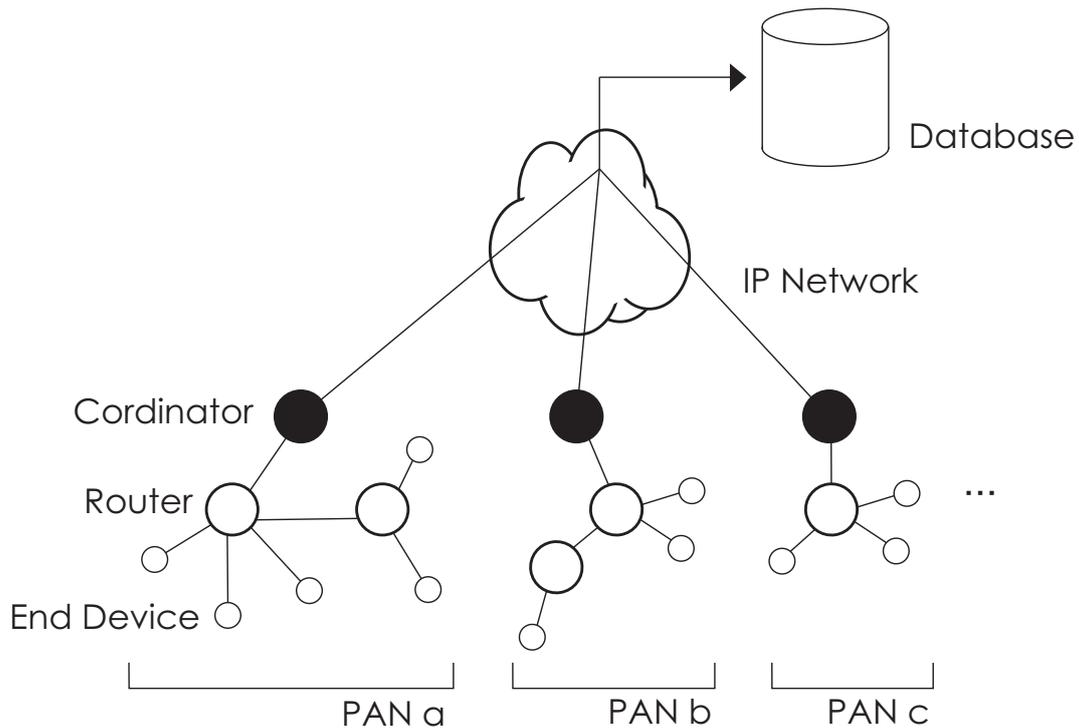


図 2.6 上位エンティティにおける情報集約

なり，また PAN は無線マルチホップによってのみ構成されるために，その 3 つが不可分である。

通常，ZigBee によるセンサネットワークを広域化するためには，複数の PAN を展開し，それぞれの PAN で独自のネットワークの管理を行い，上位エンティティのデータベースなどで集約する手法が一般的である。予備実験でも同様の構成とした。図 2.6 に上位エンティティにおける情報集約を行うシステムの概要を示す。

この手法は ZigBee プロトコルの変更は必要なく，上位エンティティのみによって広域化が実現できる簡便な方法である。しかし，小さなネットワーク，特に ZigBee のような小規模な PAN を多数構成する場合にはコーディネータを含めた ZigBee のネットワークを多数構築する必要があり，また，PAN を超えたデバイス間の通信が難しい。

2.5 これまでの試み

これまでに，ZigBee を使用してセンサーネットワークを構築する実験を複数回行った。それらの実験は他のプロジェクトを含むイベントや実証実験と同時に行った。実験の名称

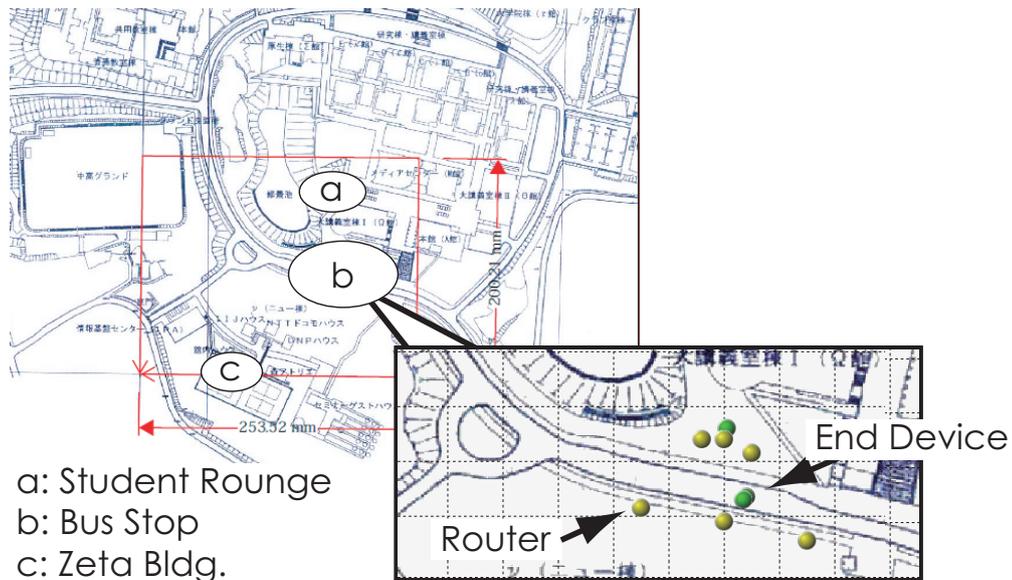


図 2.7 デジタルサイネージ実験で本学 SFC 構内に設置した PANs

とその目的を次に示す。

(A) SFC Open Research Folum 2008 2008 年 11 月

本学の対外向けイベント。会場は六本木ヒルズ内アカデミーヒルズ。本研究のためには、来場者および出展者に ZigBee の機器（ノード）を持ち歩いてもらい、展示ブースを訪れた履歴を取得。この結果のマイニングにより、各出展ブースのテーマの関係を抽出。

(B) デジタルサイネージ実験 2009 年 1 月

本学湘南藤沢キャンパスとその最寄り駅の湘南台駅周辺の飲食店でのデジタルサイネージ（電子広告）の実験。学生に ZigBee ノードを携帯してもらい、サイネージで出力する情報をそのサイネージの前にいる利用者たちにマッチするものとし、位置情報を利用した利用者へのフィードバックを実証。

(C) The Survival Show 2009 年 3 月

会場は新丸の内ビル。一般の来場者が来訪するイベントで、ZigBee を用いた位置計測が実用可能なレベルを模索。

Open Research Folum では会場内に 1 つの PAN を構成した。また、同時に稼働する移動ノードの数も他の実験と比較して少なかった。そのため、ノードの移動に関する問題

表 2.2 ZigBee によるセンサーネットワーク実験のネットワーク構成

実験名	複数 PAN 構成	覆域
(A) ORF	N	ビル 1 フロア
(B) デジタルサイネージ	Y (5 PANs)	学内 3 箇所・遠隔 2 箇所
(C) Survival	Y (2 PANs)	ビル 1 フロア

はあまり見られなかった。しかし、デジタルサイネージ実験において、複数の PAN を構成し、多数のノードが移動する環境下では、エンドデバイスが通信できない場合があった。それぞれの実験の ZigBee ネットワークの構成などを表 2.2 に示す。

デジタルサイネージ実験では、PAN は 5 つ構成した。そのうちの 2 つは遠隔地であったが、他は同じ本学 SFC 構内であった。近距離に複数の PAN を構築したのは電源の都合などからマルチホップで統一した PAN を構築できなかったためである。図 2.7 に、構内に構築した 3 つの PAN と、そのうち 1 つの位置計測の様子を示す。

Survival Show では PAN は同じビルのフロア内に 2 つ設置したが、これもデジタルサイネージ実験同様、移動ノードの通信の問題が発生した。

3 つの実験を表 2.2 にまとめる。

2.6 本論文の手法が有用な状況

本研究では、ZigBee による小規模な PAN を連結し、仮想的に広域な 1 つの PAN を構築する手法を提案する。この手法が有用な分野や状況は、PAN の無線による覆域と管理ドメインが合致しない場合である。

前節で述べたデジタルサイネージ実験のように、遠隔地や同じキャンパス内でも IEEE802.15.4 無線の届かない数百 m 離れたエリア、同じビルの違う階などのように、PAN の無線による覆域と管理ドメインが一致しない場合がある。また“忘れ物検知”アプリケーションのように、遠隔地に多数でセンサーネットワークを同じ管理ドメインとして敷設することで実現しやすいアプリケーションも存在する。図 2.8 に具体例を示す。

このようなアプリケーションを実現するために、それぞれの覆域に別個の PAN を設置するよりも、同じ PAN として連結することで簡易にアプリケーションが実現でき、またセンサノード同士の直接の通信も地理的位置にとらわれず可能になる。

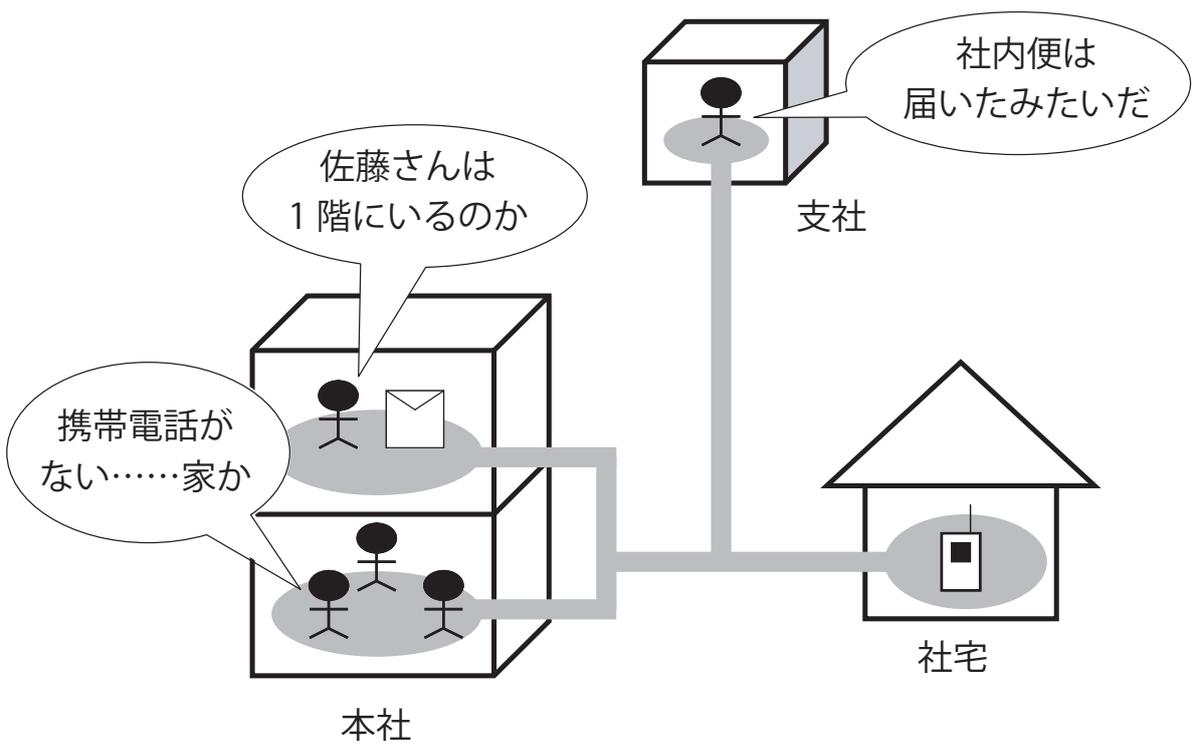


図 2.8 複数の PAN を連結した具体例

第 3 章

ZigBee PAN トンネリング

本章では，ZigBee による広域センサーネットワークを実現するために，PAN のトンネリングを行い，複数の PAN を統一する手法について述べる。

3.1 MAC レイヤ接合による PAN の連結

本論文では PAN の MAC レイヤでの接合により広域センサーネットワークを実現する手法を提案する。

2.2 に示した従来研究のように，特定のアプリケーションプロトコルの ZigBee 上への実装や，IPv6 により ZigBee PAN 間，PAN とインターネット間のネットワークングを可能にする技術は既に存在するが，それらの技術は特定のアプリケーションのために用いられていたり，あるいはそのプロトコルを利用する ZigBee アプリケーションに修正を加えたりする必要がある。これまでのアプリケーション，およびスタックをそのまま利用しながら PAN を広域化するために，ネットワークとして透過な形で地理的位置にとらわれずネットワークを拡張できる必要がある。

本論文の提案する手法は，ZigBee のネットワークツリーのホップをインターネットプロトコルで仮想的に接続することで，単一の PAN として構築する“PAN トンネリング”である。提案手法では，トンネルの両端のノードのみが PAN トンネリングに対応すればよい。図 3.1 にその概要を示す。

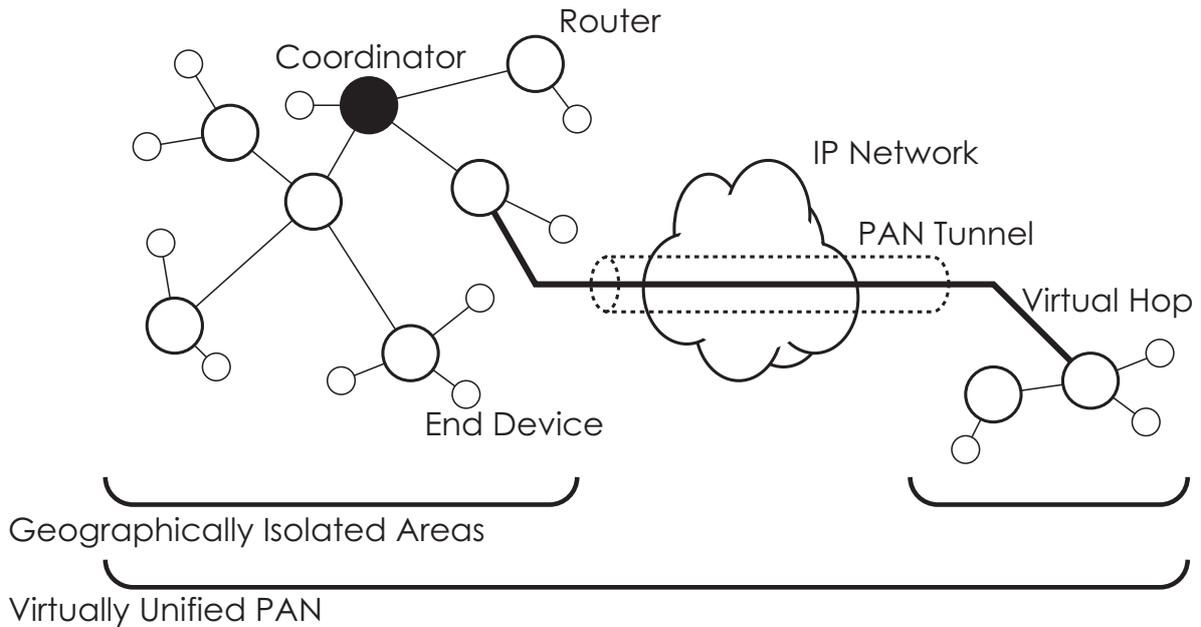


図 3.1 PAN トンネリングによる ZigBee ネットワークツリーの連結

3.2 PAN トンネリング

PAN トンネリングを実現するためには、まず 2.3 に示した ZigBee のどのレイヤでトンネリングを行うか考慮する必要がある。APL 層での透過性を実現したい以上、NWK レイヤ以下でのトンネリングが必要である。

PHY レイヤでのトンネリングは、無線周波数帯域を光ファイバで伝送したり [10]、サンプリングしてネットワークで伝送したりすることで可能である [11]。しかし、必ずしも物理通信を別の場所にそのまま移動することはメリットばかりではない。まず同一の無線空間として接続されてしまうため、帯域が混雑する。また、ZigBee は 2.3 に示したように 1 チャンネルあたり 2MHz と広い周波数帯域を使用するため、設備として大がかりになってしまう。

そのため、MAC レイヤのフレームを IP/UDP データグラムにカプセル化してトンネリングする手法をとる。そしてトンネルの両端で MAC フレームを行き来させ、NWK レイヤからは透過に利用できるメディアを構築する。即ち、IEEE802.15.4 の仮想ブリッジを IP ネットワーク上で構成する。MAC レイヤでのトンネリングを行うために、PAN トンネリングを行うノードには次の機能が必要である。

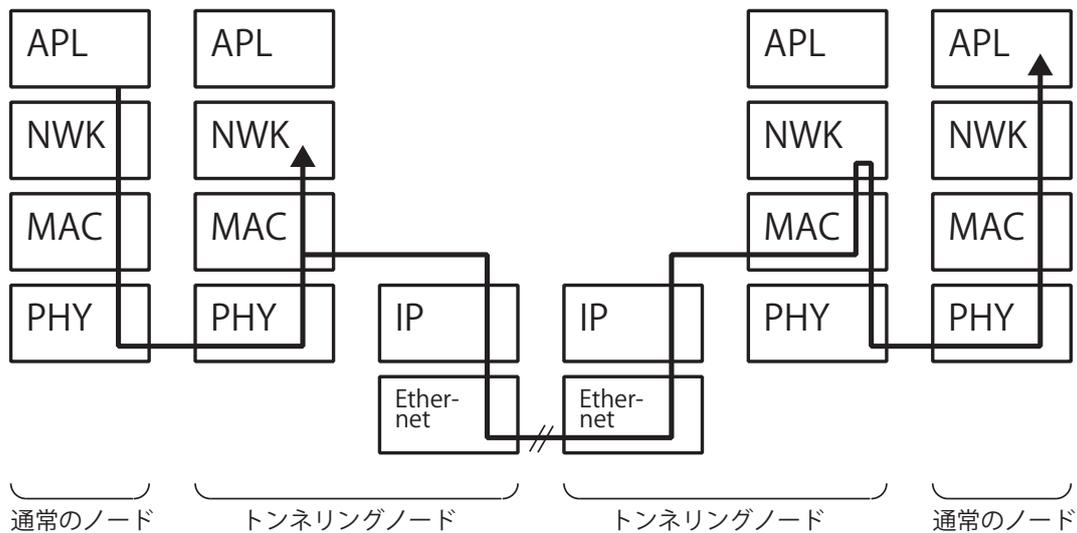


図 3.2 PAN トンネリングでのフレームの動き

- IP と IEEE802.15.4 の双方で通信可能であること
- IEEE802.15.4 のすべてのパケットをキャプチャできること (Promiscuous モード)
- IEEE802.15.4 Full Function Device であること (スリープしないノードであること)

この条件を満たす ZigBee ルータを IP ネットワークに接続するための組み込みボードに接続し、IP 網で MAC のフレームを行き来させる。ZigBee プロトコルスタックおよび IP においてのフレームの動きを図 3.2 に示す。

3.3 実装環境

PAN トンネリングが実現可能なこと、また、既存のアプリケーションやスタックへの影響を最小限に抑えて実現できることを確認するために、既存の ZigBee デバイスを改良して PAN トンネリングを実装した。次にその詳細を示す。

3.3.1 ZigBee システム

ZigBee システムは、Texas Instruments 社の製品を利用した。

■CC2431 ZigBee SoC CC2431 は、Texas Instruments 社の ZigBee SoC (System-on-Chip) 製品である。無線デバイスからアプリケーションまでワンチップで実装されてお

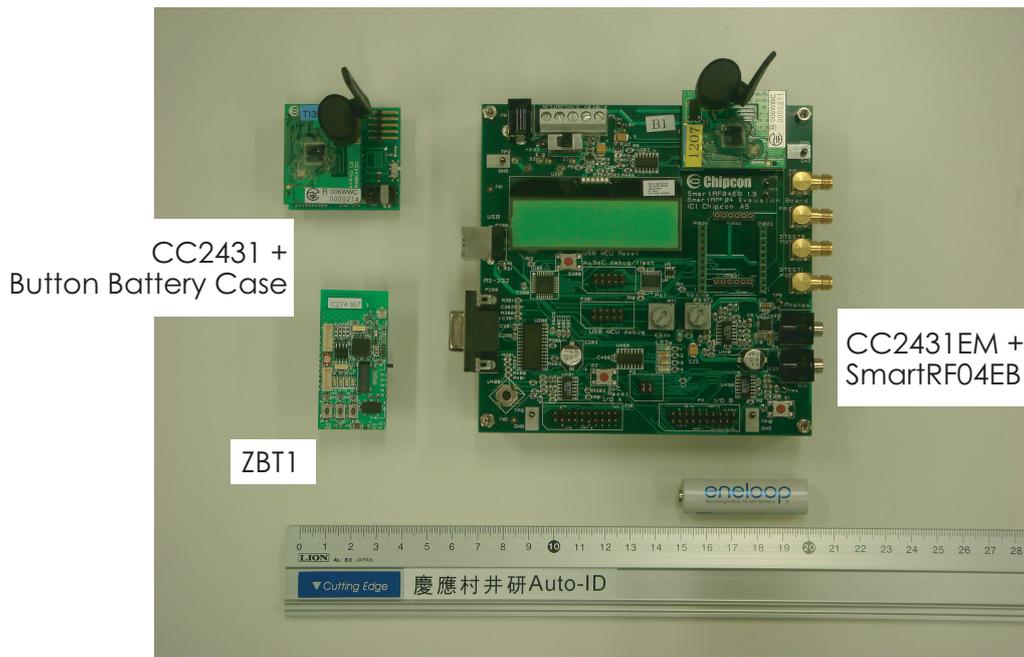


図 3.3 CC2431 を使用した開発・評価ボード

り、またソフトウェアは in-circuit で書き換え可能である。また、スタックは後述する ZStack がソースコードを含めて公開されており、開発が容易である。本論文ではこの SoC を使用した同社の評価ボード CC2431EM、およびそのインターフェイスボードである SmartRF04EB、また電池で稼働する小型の開発ボードであるオー・エス・テクノロジー社の ZBT1 を使用して実験を行った。図 3.3.1 にこれらの機器の外観を示す。なお、法令遵守の観点から、電波法令に基づき技術基準適合認定を得てから使用した。

■ZStack ZigBee スタック ZStack は Texas Instruments 社による ZigBee スタックである。MAC レイヤのローレベルの部分など、一部のデバイス依存の部分を除き、C 言語で記述されており、ソースコードが入手できる。このうち ZigBee Stack Profile 0x01 に適合し、CC2431 で稼働できる Ver. 1.4.3 を使用した。統合開発環境としては IAR 社の Embedded Workbench MCS-51 を使用した。

3.3.2 IP ネットワーク通信機器

IP ネットワークに ZigBee を接続するために、PC Engine 社の ALIX シリーズを使用した。ALIX は i386 互換の AMD Geode CPU ベースのボードコンピュータである。SmartRF04EB 評価ボードとの接続は USB 経由で RS-232C で行った。インターネッ

トとの接続は FastEthernet インタフェイスを用いた。使用したネットワークは WIDE Project の実験ネットワークである。ソフトウェアは OS に OpenBSD 4.4 または 4.6, スクリプティングに Ruby 1.8.6 を用いた。

3.4 トンネル両端のルーティング

PAN トンネリングで PAN を接続しても, ZigBee ネットワークとしてルートが確立されていなければノード間での通信ができない。MAC レイヤでは source アドレスとして任意のアドレスを指定できないので, NWK レイヤから完全に透過にはできないためである。

そのため, トンネルの両端でそれぞれのネットワークトポロジのルートを交換する必要がある。ZigBee ではノードが PAN に参加する際には, NWK レイヤが MAC レイヤに MLME-Associate.request を発行する。トンネルの両端がそのリクエストを受信し, MLME-Associate.indication を受けた場合は, 上流のノードと自分を代理としてアソシエーションを行う。

ZigBee (Stack Profile 0x01) における Cskip ルーティングについては 2.3 にて述べた。トンネルの両端のノードは Cskip に基づきアドレス範囲の割り当てを他のノードが受けた際, そのアドレス範囲が無線ネットワークに存在するノードのものか, トンネルの先に存在するノードのものか記憶する。図 3.4 にトンネル間でのルートの確立とデータの中継について示す。この例では, 右端のノードがトンネル端のノードにアソシエーションを要求し, 右端のトンネルのフィルタである R-Filter がそのアソシエーションを代理で行うとともに, 上流のノードがトンネルの先にあることを記憶する。そしてルートを確立した後, フレームの中継を行う。

ルート解決の方法はもう一つの方法が考えられる。トンネル両端のノードのセッションイニシエーションとルーティングを独自のプロトコルで行い, トンネルを含めて単一のルータとして動作させる手法である。この手法ではネットワークのアドレス資源を若干節約できる利点があるが, 既存の ZigBee システムを用いる場合, スタックに大幅に手をいれる必要があるため, 既存の ZigBee システムとの親和性を確保するのが難しい。

3.5 PAN 間通信フレームのフィルタリング

PAN トンネリングによりすべてのフレームを中継すると, トンネルが PAN の速度やパケットレートを律速してしまう場合がある。特に, 組み込み機器とのインターフェイス

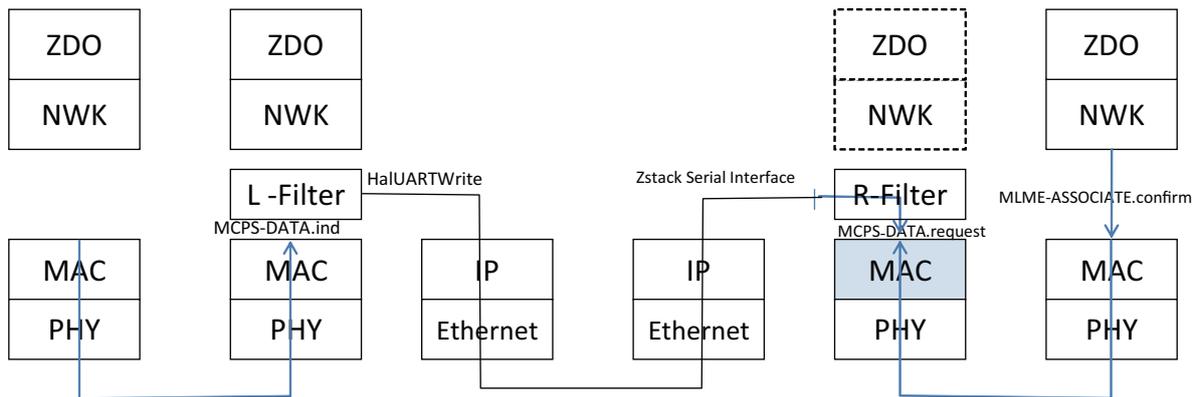


図 3.4 トンネル両端のルートの確立とデータ伝送

であるシリアル通信のインターフェイスは、割り込みなどが発生するためボトルネックになりやすい。そのため、 unnecessary パケットはフィルタして PAN トンネルを通るデータの量を制限する必要がある。PAN トンネルでフィルタすべきフレームの例を次に示す。

- BEACON.request と BEACON (レスポンス)。ノードが他のノードとアソシエーションする際に用いられるが、トンネルの間は必ずそのホップを経由することが明らかでないため転送する必要がない。
- ブロードキャストパケット。地理的に近隣のノードに対する通信であるため、フィルタする。
- 地理的位置に依存するアプリケーションのフレーム。位置計測など、地理的位置に依存するアプリケーションのフレームは、トンネルを超えると意味を持たないためフィルタする。

フレームのフィルタは ZigBee モジュールに接続した計算機内のソフトウェアで行う手法と、ZigBee のハードウェア内のファームウェアで行う手法がある。今回の実装では計算機内のソフトウェアで行った。

3.6 PAN トンネリング実験

実装した PAN トンネリングの検証のために実験を行った。トンネル両端の 2 つ分のノードを実装し、周波数チャンネルを 11 と 26 の 2 つに分けて直接通信できないようにした。そして、周波数チャンネル 26 でフレームを出力し続けるノードを稼働させ、周波数チャンネル 11 に同じフレームが出力されていることを確認した。フレームを出力しつづける

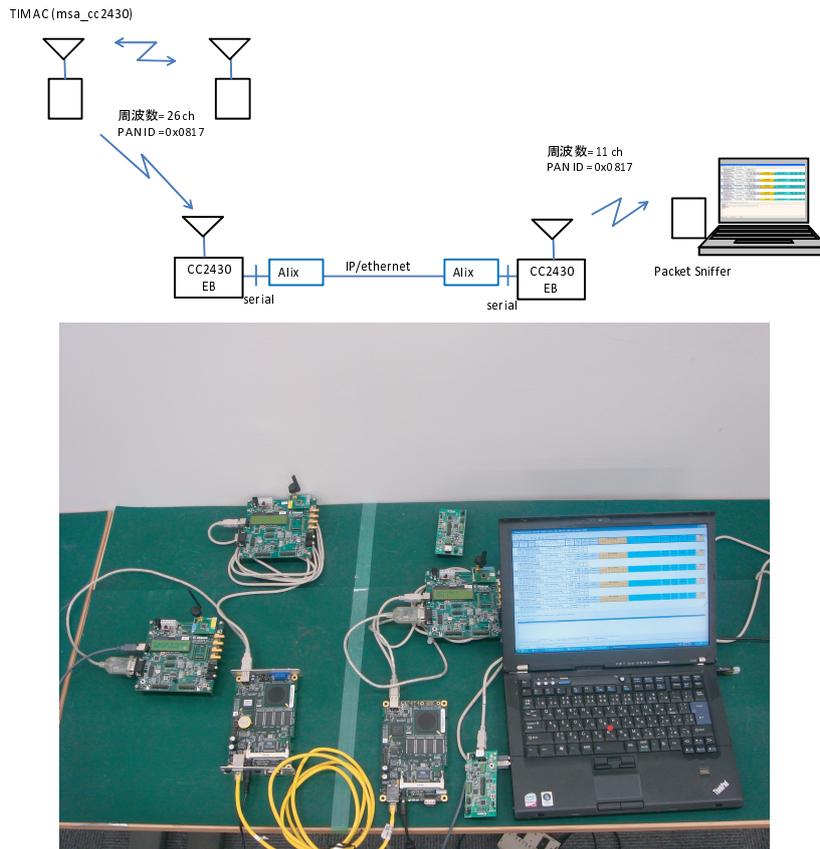


図 3.5 PAN トンネリング実験システム

ノードのプログラムは、IEEE802.15.4 実装である TIMAC msaCC2430 を用いて作成した。図 3.5 に実験システムの構成と実験の様子を示す。

TIMAC msaCC2430 ノードが周波数チャンネル 26 で送信するパケットフレームは図 3.6 に示すように MAC ペイロードが 20byte、フレーム全体では 31byte である。このパケットを一定間隔で送信した。

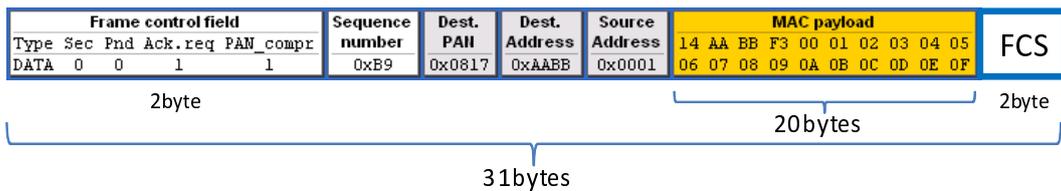


図 3.6 PAN トンネリング試験フレーム

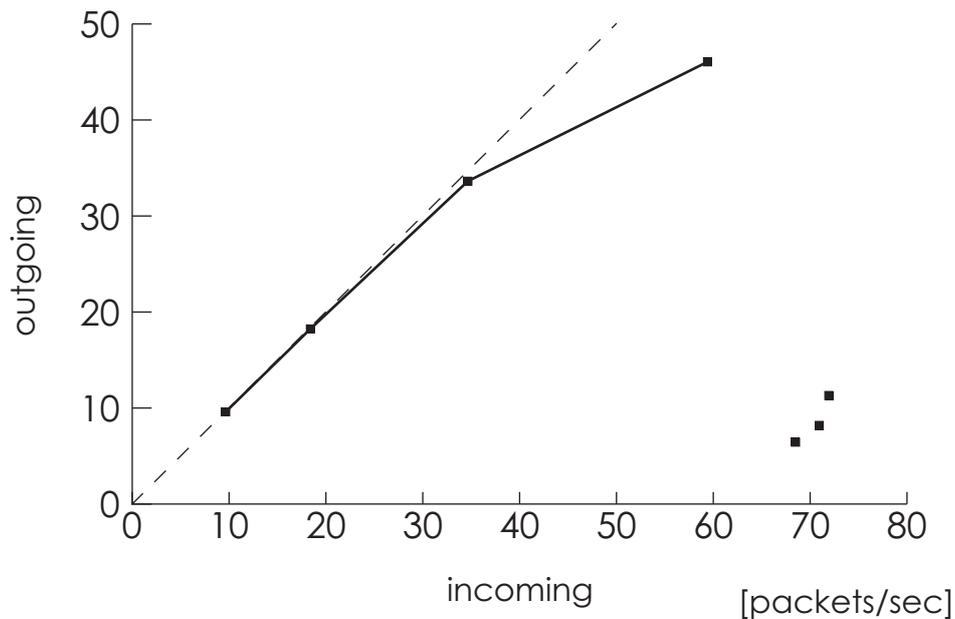


図 3.7 PAN トンネリングによるパケットロス

3.7 PAN トンネリングの性能評価

実験の際、トンネルを通る際にどの程度フレームがロスするか計測した。そのために、ペイロード 20byte の MAC フレームを送信間隔を変えながら 120 秒間送信し、トンネルを通過したフレームの数を測定した。図 3.7 に、トンネルへの入力のパケットレートとトンネルの逆端から出力されたパケットレートの比較を示す。

40 packets/sec 程度のフレームレートでは、トンネルを通過することによるフレームロスは 5% 未満であった。この程度のロスは通常の無線通信によるホップでも発生するため、実用可能なレベルと考えられる。この場合のヘッダを含めた MAC のビットレートは 9.9 kbps である。しかし、それ以上のフレームレートではロスが大きくなり、70 packets/sec 程度のフレームレートでは、60 packets/sec の程度のフレームレートのときよりもさらにフレームレートが悪化した。

次に、トンネルを構成する要素のうち、どの部分が律速しているのか判断するため、トンネルの各段階でのパケット転送成功率を計測した。図 3.8 にその結果を示す。フレームを無線で受信した数を 1 とし、左から “Serial” はそのフレームをシリアルで出力できた率、“IP” はそのフレームが UDP によりトンネルの逆端の計算機に到達した率、“Radio”

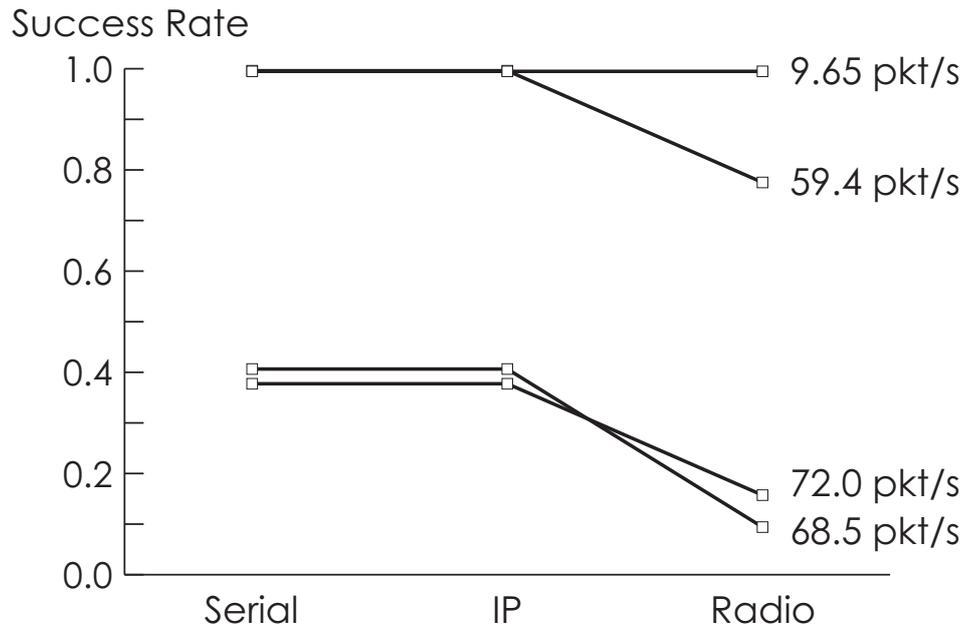


図 3.8 トンネルの各段階でのパケット転送成功率

は出力されたフレームの数である。

IP でのフレームロスが観測できなかったが、その他の段階で同じ程度のフレームロスが観測できた。そのため、シリアル通信の部分が律速していると考えられる。

しかし図 3.7 の 70 packets/sec 以上で極端にフレームがロスする現象については、無線でデータを出力する部分など、他の原因が考えられる。

第4章

結論

人やモノ、移動体などにワイヤレスセンサをとりつけた移動ノードを用いて、センシングを行う場合、物理的距離は離れていても、同一のセンサーネットワークとして扱いたい場所がある。たとえば職場と自宅、敷地内で離れた建物などである。移動ノードがある場合には、こうした離れた場所に移動したときにも同一のサービスや管理ポリシーが実現できることが望ましい。本論文は、離れた位置のセンサーネットワーク間を、移動ノードがその違いを意識しなくてすむようにインターネットで接続する方法、PAN (Personal Area Network) トンネリング、を提案し、ZigBee (IEEE 802.15.4) を用いた実装により提案方法の妥当性を示した。

PAN トンネリングは用途に応じて様々なレイヤーで行うことができる。本論文では、PAN トンネリング有無で、移動ノードの動作が変わることがないように、MAC 層でトンネリングする構成を選択した。この実現には、PAN トンネル側での MAC 層でのアドレス書き換えや、場合によっては過大となるトラフィックをフィルタリングする機能が必要である。ZigBee の代表的なプロトコルスタックである ZStack の Serial Interface および MAC 層のファームウェアおよび、外部組み込みコンピュータプログラムにより、PAN トンネリングを実現した。MAC ペイロード 20byte のフレームでは、40 packets/sec 以下であれば、現在の実装で PAN トンネルが実現できる。これ以上のレートでは SoC のシリアルインターフェイスがボトルネックとなり、無視できないパケットロスが発生する。

従来、離れた位置にセンサーネットワークを構成する際には、メッシュネットワークでセンサーネットワークを拡大するか、あるいは別々の複数の PAN を構成するしかなかったが、本研究によりインターネット接続があれば、離れた位置に PAN を拡大して設置できる。職場と自宅、本社と支社、同一敷地内での異なるビルにセンサーネットワークを敷設する際に有効である。

今後はフレームフィルタの再設計を行い、より柔軟、手軽にフィルタリングする手法について検討するとともに、および SoC とのインターフェイスを UART ではなく他の方式で行う手法について検討を進める。

謝辞

この論文はたくさんの方々にお世話になって提出に至ります。お世話になりすぎていて皆さんにお礼を申し上げることはできないくらいです。

慶應義塾大学環境情報学部 村井純教授には主査を，慶應義塾大学環境情報学部 中村修教授には副査を引き受けて頂きました。また，学部入学時から問題児だった私を研究会の指導教官としてここまで導いて頂きました。

慶應義塾大学環境情報学部 三次仁准教授には副査を引き受けて頂き，またこの論文のご指導を頂きました。ようやくここにきて“エンジニアリング”の何たるかが分かりかけてきた気がします。

慶應義塾大学大学院政策・メディア研究科 羽田久一博士にはこの論文のご指導を頂きました。スクリプト言語で満足していた私に，組み込みの世界に足を少しだけ踏み入れるきっかけを頂きました。

慶應義塾大学徳田村井合同研究会，Auto-ID Lab. Japan，WIDE Project，嘉悦大学，などなど私が向かう先々の先生方に次々ご迷惑をおかけし，かつ大変お世話になりました。お一人ずつお名前を申し上げることができず大変恐縮です。

株式会社 IJ Innovation Institute 宇夫陽次朗博士，中央大学大学院戦略経営研究科 折田明子博士には，ボランティア的に論文や生活のご指導と頂きました。ボランティアなのにごはんまで頂きました。

“ZigBee チーム”こと慶應義塾大学大学院政策・メディア研究科 江村桂吾さん，慶應義塾大学総合政策学部 米村茂さん，富田千智さんには研究の相談と最後の追い込みのお手伝いを頂きました。定義上先輩ですが，だめな先輩ですみません……。

オンライン，オフラインともにたくさんの方々に励まされ和まされここまで来ました。ありがとうございました。

最後に，私の学生生活に全面的支援をしてくれた家族に感謝を申し上げます。なんとかなったっぽいですよ。

参考文献

- [1] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci. A survey on sensor networks. *IEEE Communications magazine*, Vol. 40, No. 8, pp. 102–114, 2002.
- [2] 斎藤洋, 梅比良正弘, 守倉正博. 広域ユビキタスネットワークインフラストラクチャ構築に向けた考察. *電子情報通信学会論文誌 B*, Vol. Vol.J88-B No.18, pp. 2128–2136, 2005.
- [3] Rolf Kistler, Marcel Bieri, Rolf Wettstein and Alexander Klapproth. Tunneling smart energy protocols over zigbee. *IEEE conference on Emerging Technologies & Factory Automation, ETFA 2009. IEEE Conference on 22-25 Sept.*, 2009.
- [4] R.-C. Wang, R.-S. Chang, and H.-C. Chao. Internetworking between zigbee/802.15.4 and ipv6/802.3 network. *SIGCOMM Data Communication Festival, August 2007*, 2007.
- [5] ZigBee Alliance. *Building Automation Profile Specification (Rev. 10)*. <http://www.zigbee.org/>, 2007.
- [6] ZigBee Alliance. *ZigBee Specification*, 17 edition, 2008.
- [7] 米村茂, 三次仁, 羽田久一, 中村修, 村井純. 移動する ZigBee センサーノードの位置推定アルゴリズム. *電子情報通信学会 2009 年度ソサイエティ大会*, 2009.
- [8] The Institute of Electrical and Electronics Engineers, inc. *IEEE Standard for Information technology Telecommunications and information exchange between systems Local and metropolitan area networks Specific requirements, Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs)*, 2006 edition, 2006.
- [9] Shahin Farahani. *ZigBee Wireless Networks and Transceivers*. Newnes, 2008.

- [10] Mikio MAEDA, Tsuyoshi NAKATOGAWA, and Kimiyuki OYAMADA. Optical fiber transmission technologies for digital terrestrial broadcasting signals. *IEICE TRANSACTIONS on Communications*, Vol. E88-B, No. 5, pp. 1853–1860, 2005.
- [11] Haruhisa ICHIKAWA, Masashi SHIMIZU, and Kazunori AKABANE. Ubiquitous networks with radio space extension over broadband networks. *IEICE TRANSACTIONS on Communications*, Vol. E90-B, No. 12, pp. 3445–3451.

付録 A

ZStack を利用したソフトウェア 開発

Texas Instruments ZStack は 2010 年現在次のバージョンが存在する。

CC2530 SoC 用 最新 Ver. 2.2.0, ZigBee 2006・ZigBee 2007・ZigBee Pro 利用可能。

CC2520 トランシーバチップ + MSP430 CPU 用 最新 Ver.2.2.0, ZigBee 2006・ZigBee 2007・ZigBee Pro 利用可能。

CC2430/CC2431 SoC 用 最新 Ver. 1.4.3, ZigBee 2006 のみ利用可能。

CC2420 トランシーバチップ + MSP430 CPU 用 最新 Ver. 1.4.3, ZigBee 2006 のみ利用可能。

本文中で使用した ZStack は CC2430/CC2431 用の Ver. 1.4.3 である。ZigBee 2006 は本文中における ZigBee Stack Profile 0x01 を意味する。以下、単に ZStack と記した場合は CC2430/CC2431 SoC 用を意味する。

A.1 IAR Embedded Workbench MCS-51 での ZStack のコンパイル

ZStack は 8051 プロセッサの統合開発環境である IAR Embedded Workbench MCS-51 (以下, IAR EW) にてコンパイルおよびインサーキットデバッグできる。しかし、最新版の IAR EW では互換性の問題が生じる場合がある。その場合は次の手順を踏む。

1. “f8w2430.xcl” に “-D_EXTENDED_STACK_END=0x0000” の定義を追加

2. “chipcon_banked_code_support.s51” をコンパイル時に含まない設定にするか削除する
3. デバッガの Device Description File のパスの “chipcon” を “Texas Instruments” に変更する

A.2 MAC フレームの入力

ZStack では Z-Tool Maintenance Tool (MT) / Serial Port Interface (SPI) を用いて MAC フレームを UART ポートから NWK レイヤへ入力できる。ZTOOL を利用するには、次のコンパイルオプションを利用して、MT-MAC デバイスとしてスタックをコンパイルする。

コンパイルオプション

```
NONWK  
MT_TASK  
MT_MAC_FUNC  
MT_MAC_CB_FUNC  
ZTOOL_P1
```

その後、UART ポート経由で ZMAC_DATA_REQUEST(0x0083) コマンドを発行し、任意のフレームを送信する。

MT-MAC デバイスとして動作させる場合は、ZDO が動作しないため、アプリケーションは動作せず、また NWK レイヤのネットワーク構成は利用できない。

A.3 MAC フレームの出力

前節と同じ手法で MT-MAC デバイスを構築し、SYS_CALLBACK_SUBSCRIBE (0x0006) コマンドにて NLDE_DATA_INDICATION (0x0181) のコールバックを設定すれば、MAC フレームを出力させることが可能に思われるが、正常な動作を確認できていない。

しかし、MAC レイヤ中でのイベントハンドリングを強制的にフックし、フレームを UART で出力することが可能である。MAC の MLME-DATA.indication をハンドリングしている箇所は zmac_cb.c の次の箇所である。

```

zmac_cb.c
void MAC_CbackEvent(macCbackEvent_t *pData)
{
#ifdef MT_MAC_CB_FUNC
    zmacSendMTCallback ( pData );
#elif !defined NONWK

    uint8 macEvent = pData->hdr.event;
    uint16 msgLen = zmacCBSizeTable[macEvent] + getZMacDynamicSize
(macEvent, pData);
    macCbackEvent_t *msgPtr;
    ... snip ...
        case MAC_MCPS_DATA_IND:
    ... snip ...
        /* Store parameters */
        event = pData->hdr.event;
        status = pData->hdr.status;
        len = pData->dataInd.msdu.len;
        msdu = pData->dataInd.msdu.p;

```

A.4 Promiscuous モード

MAC レイヤで Promiscuous モードを利用するためには、MAC レイヤの初期化関数 `MAC_Init()` が呼ばれた後に、`MLME-SET.request` を発行し、MAC レイヤのプロパティを変更する事で行う。具体的には `zmac.c` を次のように変更すればよい。

```

zmac.c
#include "mac_low_level.h"
... snip ...
ROOT uint8 ZMacInit( void )
{
    uint8 stat;

    MAC_Init();
    MAC_InitDevice();

#ifdef ( RTR_NWK )
    MAC_InitCoord();
#endif

    macRxPromiscuousMode(MAC_PROMISCUOUS_MODE_COMPLIANT); // HERE!!

```

変更履歴と成果の公開について

本論文の変更履歴は次の通りである。

2010年1月12日 慶應義塾大学湘南藤沢メディアセンター収蔵版。

2010年2月12日 本版。

- 図 2.8 を変更
- p.29 の S_n の式を訂正
- 図 3.2 を追加
- その他, 体裁と誤字の修正

また, 本論文と研究の成果は次の URL にて公開する。

<http://www.autoidlab.jp/pantun/>