日本国内における 920MHz 帯の ZigBee IP 仕様

岡庭　勝広　　福永　　茂　　川本　康貴
野崎　正典　　八百　健嗣

920MHz帯無線は、電波到達性と伝送速度のバランスの良いことで知られている[1]。OKIではこの920MHz帯無線を利用して、家庭やビルのエネルギー管理システムであるHEMS/BEMS(Home/Building Energy Management System)、スマートメータリング、モノとモノの通信を実現するM2Mネットワーク(Machine to Machine)等のサービスに利用できる無線マルチホップネットワークプラットフォームを開発した。

本プラットフォームはIEEE.802.15.4g, ZigBee IP等の国際的な標準に準拠しており、多様な機器・センサとの相互接続を可能とする。またネットワークへの参加認証と暗号化によりセキュアなネットワークを実現している。本稿では、920MHz無線プラットフォームのベース技術となるZigBee IPの技術仕様に関して概説する。

920MHz帯 ZigBee IPの概要

ZigBee®*1) は、センサネットワーク等向けに国際的に普及している通信方式であり、低速な無線伝送路上でのマルチホップ動作を特徴としている。これまでZigBee Allianceでは、世界的に広く利用可能な2.4GHz帯を採用してきたが、日本での920MHz帯の周波数移行を機会にサブギガ ZigBeeの審議を2012年8月に開始した。ここでのサブギガとは、1GHz帯より少し下の周波数帯(Sub GHz)を表す用語である。ZigBee Allianceでは、アプリケーションごとにプロファイルを規定しており、HEMS向けにSEP (Smart Energy Profile)が欧米で普及しつつある。一方、日本市場では、経済産業省がHEMSの標準化を推進しており、JSCA (日本スマートコミュニティアライアンス)では、2012年2月にアプリケーション・インタフェースとしてECHONET Liteを推奨方式として決めた。そこでZigBee Allianceでは、サブギガZigBeeの上位のアプリケーション層としてECHONET Liteにも対応し、またJSCAではネットワーク層にIPv6を推奨していることから、IPv6に対応しているZigBee IPをベースに審議を進めている。

ZigBee IPは従来のZigBee標準とは異なり、ネットワーク層やトランスポート層にIEEEやIETFで標準化されたオープンな規格を採用している。そのため、ZigBee IP仕様書には、各種プロトコルの利用手順やパラメータ、各デバイスのブートシーケンスなどが記載されている。ZigBee Allianceでは、技術規格の標準化において、複数ベンダによる相互接続試験を必須条件としており、現在、920MHz帯のZigBee IP（以降、920ZIPと呼ぶ）の認証プログラムを制定中である。一方、ZigBee Allianceとリエゾン関係にあるTTC（情報通信技術委員会）では、ECHONET Liteの下位層の通信インタフェースのガイドラインをTR-1043として制定しており、920MHz帯の通信方式に関しては、JJ-300.10[2] としてTTC標準を発行している。920ZIPも「方式B」として公開されており、本稿ではこのTTC標準に基づいて920ZIPの仕様を説明する。920ZIPのプロトコルスタックの構成を **図 1**に示す。

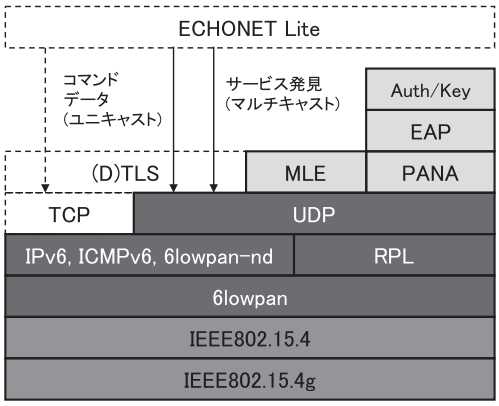

図 1　JJ-300.10 における 920ZIP のプロトコルスタック

920ZIPは物理層にIEEE802.15.4g[3] を採用しており、MAC層には従来のIEEE802.15.4のCSMA/CA方式を採用している。IP層はIPv6を採用しているが、IPv6ではIPv4よりもヘッダサイズが大きくなるため、低速な回線では伝送効率が悪くなる。そこでIEEE802.15.4のような低速な無線伝送路上にIPv6パケットを送受信するための規格と

＊1）ZigBee は、ZigBee Alliance の登録商標です。

して6lowpan[4]がIETFで標準化され、920ZIPでもアダプテーション層として採用している。6lowpanは、IPv6パケットを複数のフレームに分割するフラグメントや、IPv6のヘッダ情報を削減するヘッダ圧縮の機能などを備えている。

920ZIPの特徴であるマルチホップ機能に関しては、RPL(IPv6 Routing Protocol for Low-Power and Lossy Networks)[5]が採用されている。RPLはツリートポロジーとして1対多の接続形態を前提としており、複数の装置からのデータ収集などに適している。RPLでは、IPv6パケットの中継に必要となるルーティングアルゴリズムを規定している。また920ZIPでは、装置の認証や暗号鍵の配布などの機能が必要となるため、セキュリティ機能としてPANA (Protocol for carrying Authentication for Network Access)[6]を採用している。また隣接ノードとのセキュリティ情報の取得や、リンク品質測定のためにUDP上で動作するMLE (Mesh Link Establishment)[7]も用いられる。なお、920ZIPではRPLのrootノードをZC(ZigBee Coordinator)、RPLの機能を有する装置をZR(ZigBee Router)、RPLの機能を持たない装置をZH(ZigBee Host)と呼んでいる。次章では各層の詳細機能について説明する。

IEEE802.15.4g機能の詳細

IEEE802.15.4gはPAN(Personal Area Network)向けに作られた規格であるIEEE802.15.4のPHY部分の規格を、SUN(Smart Utility Network)向けに修正したものである。IEEE802.15.4g規格の特徴を以下に示す。

- 日本の920MHz帯を含む、世界各国のサブギガ帯域に対応(欧州：863MHz,米国：915MHz,中国：780MHz etc)
- 最大2047バイトのロングフレーム対応
- 最大1000バイトのロングプリアンブルにより、アンテナダイバシティ―に対応
- データホワイトニングに加えて誤り訂正符号に対応

変調方式は、従来の2.4GHz帯向けのDSSS方式、長距離伝送向けのGFSK方式、高速通信向けのOFDM方式が規定されており、920ZIPではGFSK方式が採用されている。GFSK方式の伝送レートは50kbps, 100kbps, 200kbps, 400kbpsの4種類が規定されているが、920ZIPでは100kbpsを採用している。

また日本国内では、920MHz帯のシステム共用性を高めるため、電波法やARIB標準で以下のような制限が定められている。

- キャリアセンス時間は128usec以上
- 最大連続送信時間は200msec以下
- 送信時間が3msec以上になるフレームを送信する場合、フレーム送信後2msecは送信禁止
- 1時間当たり送信時間の合計は360秒以下

なお上記のような制限はアプリケーションやネットワーク層で実装することは難しいため、OKIではMAC層の機能として上記制限を順守できるよう実装している。

RPL機能の詳細

RPLはDAG(Directed Acyclic Graph)と呼ばれる非循環有向グラフにより、1対多のツリートポロジーを形成する。RPLでの上りデータは、rootからの相対的な位置を示すrankと呼ばれる指標によってルーティングされる。このrank値は、小さいほどrootへの中継コストが低いものとされ、各ノードは自身よりrankの小さいノードを中継先の親候補として選択する。一方、rootからの下りデータは、パケットのヘッダに下りの経路表を記載するソースルーティングと呼ばれる手法により中継される。これにより各ノードは下りの経路表を維持する必要がなくなり、ノードの省メモリ化が実現できる。この様子を **図 2**に示す。

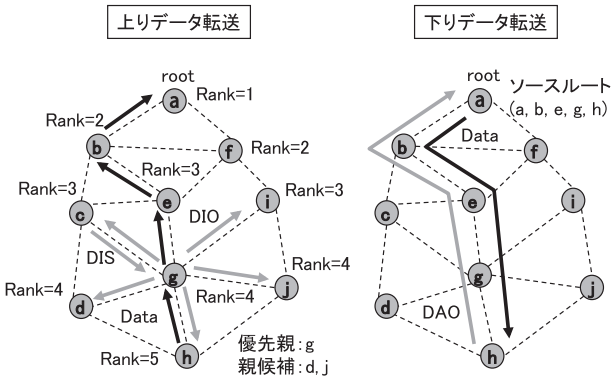

図 2　RPL の動作概要

まずRPLに参加したいノードは、DIS(DODAG Information Solicitation)を送信し、隣接ノードへDIO(DODAG Information Object)の送信を要求する。DIOにはrootのIPv6アドレスやrank、シーケンス番号などが記載されており、rank情報から優先親と親候補を選択する。ノードhの場合、優先親g、親候補d,jを選択している。次にノードは自身の親情報をrootに伝えるため、DAO(Destination Advertisement Object)をrootに送信する。DAOには優先親や親候補情報が記載されており、rootは各ノードの優先親を辿ることで、下り経路を確立することが出来る。

セキュリティ機能の詳細

920ZIPではセキュリティ機能として、1）NW参加認証、2）NW鍵の配信、3）MLE暗号化認証、および、4）MAC暗号化認証を規定している。これら機能により、権限のないノードが不正にネットワークに参加することを防止でき、第三者による盗聴や不正アクセスを防ぐことができる。以下に各機能を説明する。

1）NW 参加認証機能

参加ノードと認証サーバとの間で、認証メッセージを交換し、互いに正当な認証情報を保有するかどうかを確認する。認証プロトコルは、以下の2種類のプロトコルから構成されている。

EAP-TLS(Extensible Authentication Protocol – Transport Layer Security)[8]：TLSに基づき、認証・鍵交換するプロトコルであり、920ZIPでは事前共有鍵を用いて認証する方式を採用している。

PANA：UDP上で動作し、EAP-TLS認証メッセージを運ぶプロトコルとして利用される。また920ZIPでは、ZRにおいて、参加ノードと認証サーバ間で送受信されるEAP-TLS認証メッセージをリレーさせる機能や、NW鍵を暗号化配信する機能を規定している。

認証サーバ機能はZC内に実装され、参加ノードが事前共有鍵などの正当な認証情報を保有するかどうかを確認する。また、ブラックリスト／ホワイトリストを事前に管理しておくことにより、参加ノードを制限することも可能である。

2）NW 鍵の配信機能

NW鍵は、NWで共通の秘密情報であり、後述するMAC/ MLE暗号化認証に利用する鍵を生成するためのシードとして利用される。NW鍵の配信には、参加認証時の初期の配信と、NW鍵の更新に伴う配信とがあり、共にPANAを用いて配信される。認証サーバは、任意のタイミングで権限のあるノードのみに新しいNW鍵を配信することが出来る。新しいNW鍵を配信されなかったノードは、その後のNW鍵の切り替えにより、NWへの参加資格を失う。

3）MLE 暗号化認証機能

NW鍵より生成したMLE鍵を利用して、MLEの暗号化と認証を行う。MLEの暗号化認証には、128-bit鍵長のAESを利用しており、隣接ノードとの制御パラメータの交換を安全に実施することが出来る。

4）MAC 暗号化認証機能

NW鍵より生成したMAC鍵を利用して、MACの暗号化と認証を行う。MACの暗号化認証には、128-bit鍵長のAESを利用し、マルチホップの転送毎にMACフレームの暗号化と認証を実施する。NW鍵を知らない第三者が暗号化されたMACフレームを解読したり、認証が通るMACフレームを生成することは困難であるため、第三者による盗聴や、不正アクセスを防ぐことができる。

ZIPルータの動作シーケンス

本章では、上述したプロトコルがどのような手順で動作するかについて説明する。920ZIPのルータ装置（以下、ZR）における動作シーケンスを **図 3**に示す。

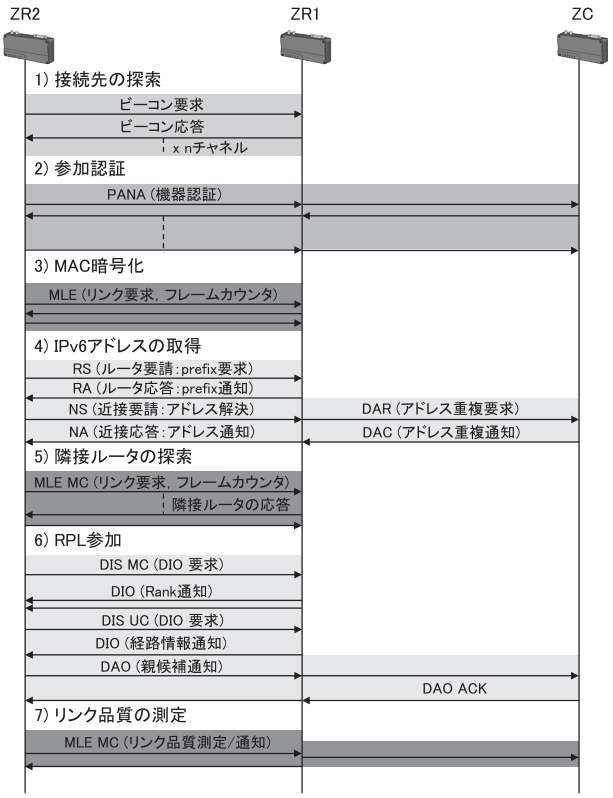

図 3　ZIP ルータの動作シーケンス

1）NWに参加しようとするルータ(ZR2)は、周辺ノードに対してビーコン要求をブロードキャストで送信する。ビーコン要求を受信した周辺ZRは自身の存在を知らせるためにビーコンを送信するが、この時、ビーコンペイロードにZIP NetworkIDを記載する。これにより新規にNWに参加するZRはどのNWに加入すれば良いかを知ることができる。

2）ZR2は、ZCへのPANA参加認証を開始するために、ZR1に対してPCI (PANA Client Initiation)を送信する。このPCIを受信したZR1は、以降ZR2のPANA中継局として動作する。

3）PANAによる参加認証が完了したZR2は、通知されたNW鍵を用いてMAC層の暗号化通信を行うために、ZR1とのカウンタ値の交換を行う。このカウンタ値の交換にはMLEが用いられる。

4）ZR2は自身のIPv6アドレスを決定するために、RS/RA(Router Solicitation/Advertisement)によりZR1からIPv6アドレスのプレフィックスを取得する。この時、ZR2のIPv6アドレスは、16bitのショートアドレス(SA)から生成されるが、この値はノード自身がランダムに決定するため、同じNW内で重複する可能性がある。そこで、ZR2はNS/NA(Neighbor Solicitation/Advertisement)を用いて自身のSAをZCに通知し、ZCは過去に同じアドレスが使用されていないかのチェックを行う。このメッセージは、DAR/DAC(Duplicate Address Request/Confirmation)と呼ばれ6lowpan-nd[9] で規定されている。

5）SAが確定したZR2は、隣接ノードの探索を行うため、MLE Link Requestをマルチキャストアドレスで送信する。このメッセージを受信した隣接ノードは、自身の隣接テーブルに空きがあれば、MLE Link Accept and Requestを返信する。最後にZR2はMLE Link Acceptを返信することで隣接テーブルへの登録を完了する。以降、ZR2は隣接テーブルに登録されたルータ間とのみ暗号化された通信を行う。

6）次にZR2は、マルチホップ経路を構築するためにRPLの動作を開始する。ZR2は周辺の経路情報を取得するために、DISをマルチキャストで送信し、DISを受信した隣接ノードは，DIOを返信することでDODAG-IDやRPLインスタンスなどのRPL情報を通知する。ZR2は、隣接ノードの中から優先親ノードとして最適なノードに対して、ユニキャストのDISを送信し、返信されたDIOによって経路情報を取得する。最後にZR2は、親情報をDAOメッセージとしてZCに対して送信する。これにより、ZCは各ノードの親子関係を知ることが可能となり、ソースルーティングによる下り経路を確立することができる。

7）920ZIPでは、経路を決定するメトリックとして、パケット受信率の逆数を用いており、パケット受信率は、MLEの定期的な広告により隣接ノード間で測定される。また、rankの算出には、MRHOF[10] と呼ばれる算出方法が用いられ、ヒステリシスな特性によりパケット受信率の変化に対して頻繁に経路が変更されないような工夫が施されている。

ま と め

本稿では、日本国内における920MHz帯のZigBee IP仕様について紹介を行った。OKIではZigBee IPに準拠した製品を2013年1月から商品出荷している。

今後は、ZigBee IP製品の品揃えを強化し、お客様からの様々な要求に対応可能なスマートネットワークソリューションを提供していく。 ◆◆

■参考文献

1）福井, 福永,“センサネットワーク向け900MHz帯の標準化動向”, OKIテクニカルレビューNo.218, 2011年10月

2）TTC標準 JJ-300.10 ECHONET Lite向けホームネットワーク通信インタフェース(IEEE802.15.4/4e/4g 920MHz帯無線) 第1版, 2013年2月

3） IEEE Std 802.15.4g-2012, 2012.4

4）IETF RFC 6282, “Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks”, 2011.9.

5） IETF RFC 6550, “RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks”, 2012.3.

6） IETF RFC 5191, “Protocol for Carrying Authentication for Network Access”, 2008.5.

7） IETF draft-kelsey-intarea-mesh-link-establishment-05, 2013.02

8）IETF RFC 5216, “The EAP-TLS Authentication Protocol”, 2008.3.

9） IETF RFC 6775, “Neighbor Discovery Optimization for IPv6 over Low-Power Wireless Personal Area Networks”, 2012.11.

10） IETF RFC 6719, “The Minimum Rank with Hysteresis Objective Function”, 2012.9

●筆者紹介

岡庭 勝広：Katsuhiro Okaniwa. 通信システム事業本部 スマートコミュニケーション事業部

福永 茂：Shigeru Fukunaga. 通信システム事業本部 スマートコミュニケーション事業部

野崎 正典：Masanori Nozaki. 研究開発センタ スマート社会ビジネスイノベーション推進部

川本 康貴：Yasutaka Kawamoto. 研究開発センタ スマート社会ビジネスイノベーション推進部

八百 健嗣：Taketsugu Yao. 研究開発センタ スマート社会ビジネスイノベーション推進部