

将来 IoT/M2M のための ID ベース通信

福島裕介 Ved P. Kafle

モノのインターネット (IoT) は、我々の生活を豊かにする革新的な ICT サービスを提供する。マシン・ツー・マシン (M2M) は、IoT に求められる、異種通信環境に接続するデバイス間の安全かつ柔軟な通信を実現する。本稿では、デバイスの位置情報に依存しない M2M を実現する ID ベース通信に基づいたモバイルセンサネットワークの設計と実装について述べる。

1 まえがき

安価で低消費電力な無線通信デバイスの流通により、機器同士がネットワークを介して自律的に情報をやりとりすることで実現する様々な M2M (マシン・ツー・マシン) サービスが生み出されている。これらのサービスで使われる端末数は、2020 年までに 500 億に達すると目されており^[1]、膨大な数のデバイス間で安全に M2M を実現するフレームワークが国際的な標準化機関である国際電気通信連合 (ITU) で議論されている^[2]。このフレームワークでは、インターネットを介して端末を管理し、探しだす仕組みや、端末同士が互いを識別して安全に通信を開始し、ネットワークを切り替えても通信継続する仕組み、端末を遠隔制御する仕組み、そして異種通信プロトコルを用いるマシン間の通信サポートが盛り込まれている。現在の M2M では、センサデータを定期的にクラウドサーバへアップロードするなど、一方向の通信で 1 回の通信量が比較的少ない。しかしながら、M2M 技術がエンドユーザ向けアプリケーションに浸透する将来の IoT/M2M では、サービスが個々のデバイスを遠隔から管理し、ユーザの周囲の状況に基づいて、デバイスを安全に制御するための継続した通信など、ITU の M2M フレームワークで定義されるような機能が求められる。このような機能を実現するには、個々のデバイスをデータ通信開始前に認証し、識別しながら通信を行う必要がある。しかしながら、インターネットを介した通信では、IP アドレスをはじめとするデバイスの位置情報 (ロケータ) は、端末の識別子 (ID) として利用される。この場合、ネットワーク接続切替え等で、ロケータが通信中に変わると、通信先のデバイスを識別することができなくなる。加えて、デバイスの安全な遠隔制御実現のため、デバイス間の相互認証機構が不可欠になる。

これらの課題を解決する手段として、ID・ロケータ

分離ネットワークアーキテクチャ技術の研究開発が行われている^{[3][4]}。一般に ID・ロケータ分離ネットワークアーキテクチャでは、端末を識別する手段として新たにホスト識別子 (以下、ID) を導入し、端末識別機能をネットワーク層から分離することで、ロケータの変化に影響を受けず通信継続できる仕組みを提供する。中でも、我々が研究開発を行っている HIMALIS (Heterogeneity Inclusion and Mobility Adaptation through Locator ID Separation)^[5] 技術は、将来の IoT/M2M で有用と考えられる、インターネットを介して端末を見つける仕組み、端末同士が相互に認証を行う仕組みを提供する^[6]。本稿では、大規模オープンテストベッド JOSE^[7] の設備の 1 つとして設計・開発した HIMALIS をベースとした IoT/M2M 実現に向けた取組について述べる。

2 HIMALIS ネットワーク概要

本節では、HIMALIS ネットワークと、ID を用いた通信方式 (ID ベース通信) について述べる。

2.1 ネットワークアーキテクチャ

HIMALIS ネットワークは、複数のエッジネットワークと、それらを接続するトランジットネットワークで構成される (図 1)。トランジットネットワークは、ロケータを相互に変換可能な専用のゲートウェイ (HIMALIS ゲートウェイ) で各エッジネットワークと接続し、異なるロケータ種別 (例えば、IPv4、IPv6) で構成されるエッジネットワーク間の通信を中継している。また、トランジットネットワークには、ドメインネームサーバ (DNS) と同様の階層的なドメイン管理機構を持つドメイン管理サーバと、ホスト情報 (ホスト名、ホスト ID、ロケータ、公開鍵) を管理する ID・ロケータ管理サーバが設置されている。ホスト ID と鍵は、ホストの初期接続処理の際に自動生成さ

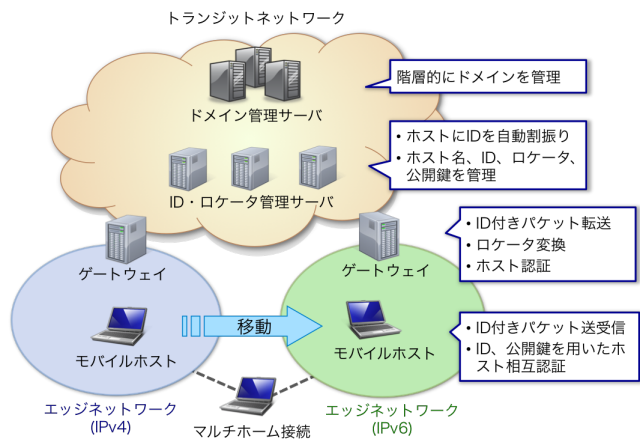


図1 HIMALIS ネットワークアーキテクチャ

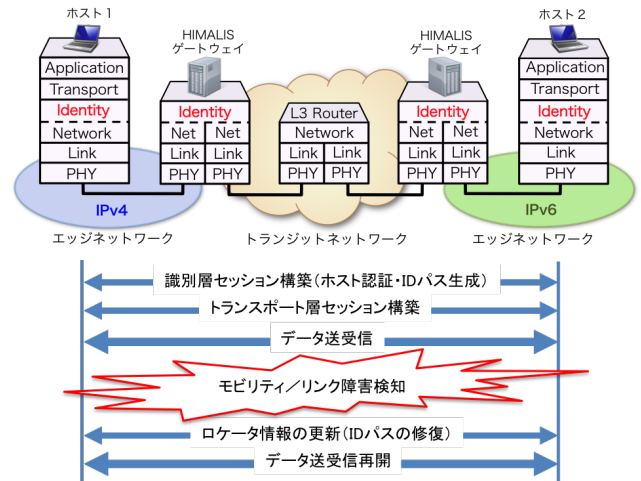


図2 HIMALIS のプロトコル・スタックと ID ベース通信

れ、ホスト名、ロケータとともに ID・ロケータ管理サーバに登録される。ネットワーク切替え等でロケータが変わったときに、ホスト自身がロケータ情報を更新することで、他のホストから検索可能になる。

2.2 プロトコル・スタックと ID ベース通信

HIMALIS では、ロケータに依存しない通信を実現するため、トランスポート層とネットワーク層の間に新たに識別層を挿入し、トランスポート層の機能をネットワーク層から完全に分離する。識別層では、ホスト ID とロケータの対応を管理する ID テーブルを持ち、ロケータが変化しても通信継続できる仕組みを実現している。自身のロケータが変化する度に通信相手にロケータ変化を通知することでモビリティに対応する。HIMALIS の通信では、通信開始前に通信相手を相互に認証する機構を有する。この認証機構は、ID・ロケータ管理サーバから取得できる通信相手の公開鍵で暗号化したメッセージを対応する秘密鍵を持つホストで復号できる仕組みを利用している。通信開始処理時に識別層でセッション (ID セッション) を構築し、通信路障害の検知や端末移動時の ID テーブルの更新を自動的に管理する。本稿では、このような識別層の機能を用いた通信を、ID ベース通信と呼ぶ。

ID ベース通信の流れを図2に示す。IPv4 エッジネットワークに接続するホスト1がIPv6 ネットワークに接続するホスト2への通信を開始する場合、宛先ホスト名 (host2 #himalis.net) をドメイン管理サーバ、ID・ロケータ管理サーバに問い合わせ、ホスト2のホスト ID、ロケータ、公開鍵を取得する。次に、ホスト1は、通信開始要求メッセージをホスト2と交換し、ID セッションを構築する。このメッセージは、公開鍵暗号方式を用いて交換されるので、相互のホスト認証も兼ねている。ID セッション構築後は、デー

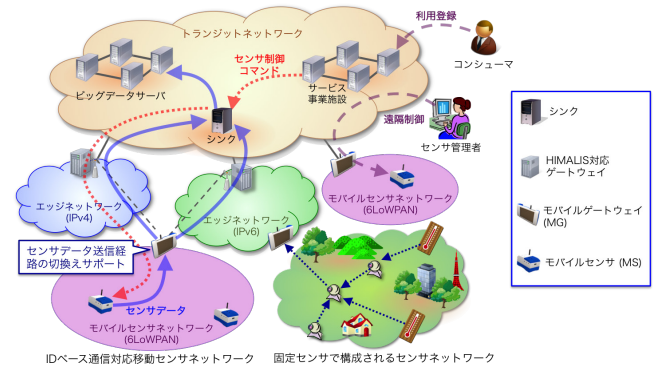


図3 HIMALIS のプロトコル・スタックと ID ベース通信

タ送受信が開始できる。ハンドオーバ等により、通信中にロケータが変化すると、最新のロケータ情報を交換し、互いの ID テーブルを更新する。

3 センサ群を収容する ID ベース通信ネットワーク

ネットワーク層の変化に関わらずインターネットを介して安全な通信継続を可能とする ID ベース通信の導入により、インターネットを介した移動体間の M2M や、端末配置後の管理が実現できる。本節では、ID ベース通信を用いた M2M の例として、モバイルセンサ群を収容する HIMALIS ネットワークについて述べ、ユースケースについて紹介する。

3.1 ネットワーク構成

センサが接続するネットワークに ID ベース通信を導入することにより、移動体に取り付けたセンサが接続するネットワークを切り替えても、センサ端末同士の M2M やセンサ管理者から制御することが可能になる。このネットワークでは、HIMALIS ネットワー

クに、新たにモバイルセンサ、モバイルゲートウェイ、シンクの3種類の端末が接続する(図3)。

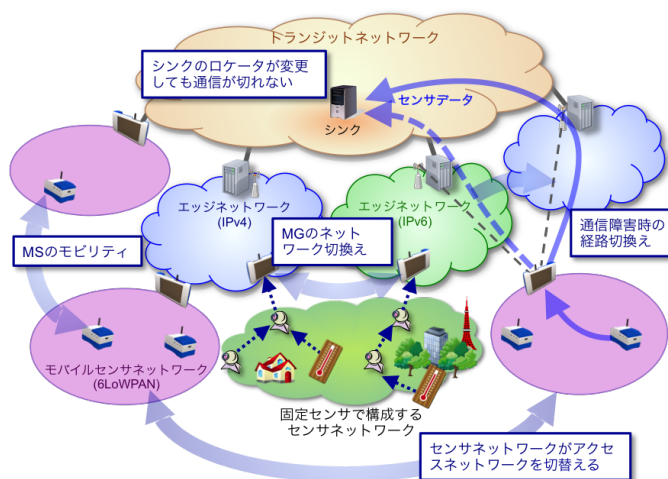
- モバイルセンサ (MS) は、小型のセンサモジュール、無線通信モジュール、演算モジュール、バッテリーで構成される。演算モジュールには、ID 通信スタックが実装され、ネットワーク接続を切り替えながらセンサデータを宛先に送信することや、遠隔から他の ID 通信対応端末から直接通信することが可能となっている。無線通信モジュールは、IEEE 802.15.4 等の電力消費の少ない通信規格が用いられ、通信プロトコルには、通信オーバーヘッドが少なく、IPv6 ネットワークに接続可能な 6 LoWPAN (IPv6 over Low power Wireless Personal Area Network) が用いられる。センサモジュールは、複数のセンシング機能の搭載が可能で、必要に応じて個々のセンサ機能の ON/OFF を行う。
- モバイルゲートウェイ (MG) は、複数の MS を收容するセンサネットワークに接続し、センサネットワークとエッジネットワーク間のロケータ変換を行う。MG 自身も ID ベース通信機能を持ち、モビリティやマルチホームをサポートする。また、接続する MS 群のハンドオーバーリングを集約し、センサネットワーク全体を別のエッジネットワークに切り替えることが可能である。また、移動に対応していない従来の固定型センサネットワークに接続することで、固定型センサから送られるデータをまとめ、宛先へ送ることも可能である。

- シンクは、センサデータを保存するデータサーバ機能を持つモバイルホストである。このため、シンクは、トランジットネットワーク、エッジネットワークのどちらにも設置できる。ID ベース通信のホスト認証・直接通信により、管理対象の MS から安全にセンサデータを受け取ることができる。また、シンクは、HIMALIS の通信機能を持たない一般的な端末からアクセスできる Web ベースのセンサ制御インタフェースを持ち、人間やマシンが遠隔の MS を制御することが可能である。

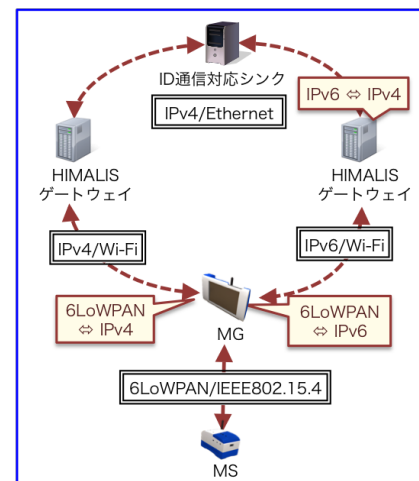
HIMALIS の通信機能を持つ MS、MG、シンクは、通信中に接続するネットワークを切り替えても通信を継続することができる(図4)。例えば、MS が、任意のタイミングで別のモバイルセンサネットワークに接続を切り替えることにより、移動体の周囲の状況をモニタリングすることが可能である。MG がエッジネットワークの接続を切り替える場合、接続する MS がネットワーク接続処理をすることなく、モバイルセンサネットワークを別のエッジネットワークに切り替えることができる。ID ベース通信技術により、MG が複数の MS を收容してネットワーク接続を切り替える状況においても個々の MS に対してアクセスが可能であるので、様々な移動体への設置が可能である。

3.2 モバイルセンサ群を收容する HIMALIS を用いたユースケース

端末固有の識別子を用いた HIMALIS 通信の特徴である移動端末の位置情報を管理する仕組み、安全に通信を継続する仕組みを活かし、移動体周囲のリアルタ



HIMALISセンサーネットワークでの端末の移動シナリオ



モバイルセンサからシンクへの通信

図4 モバイルセンサ、モバイルゲートウェイの移動シナリオ

イムモニタリング、移動体に取り付けたデバイスに対して遠隔から制御・管理など様々な利用用途が考えられるが、主な例を2つ示す。

3.2.1 どこでも医療サービス

現在利用可能なセンサを用いた健康管理サービスの多くは、デバイスとサービスが一体となっており、サービスを受けるには、対応するデバイスの購入が必須であり、購入後にサービスを変更することが難しい。また、スマートフォンや時計等のデバイスに搭載されるセンサで計測可能な身体情報は物理的に限られてしまう。継続的な身体モニタリングを実現するには、身体に取り付ける不特定多数のセンサを必要に応じて追加、制御し、適切なサーバへ情報送信を行う必要があるが、設定が複雑で現実的でない。

一方、HIMALISを導入すると、個々のデバイスの発見、識別、制御が遠隔から可能となる。これにより、デバイスの制御をサービスに任せることで、サービス提供に必要な各デバイスの設定の自動化や、起動するセンサや取得間隔変更など身体状態に応じた動的な制御が可能になる。これにより、サービスが最適な設定で、24時間利用者の身体状況をモニタすることができるだけでなく、サービスから利用者への動的なフィードバックが実現できる。例えば、生活習慣病等の未病の治療に働きかけたり、持病が重篤化する前に医療機関の受診を促したり、救急の際は、救急車や受け入れ先医療機関にリアルタイム身体情報を提供するなど、長期的なケアが必要なものから、緊急を要する事態に対しても幅広く利用できる。

3.2.2 車いす支援サービス

肢体に障害を持つ人にとって車いすは、他人の手を借りず移動を実現する最も簡単な手段の1つである。しかしながら車いす移動には、段差、傾斜、歩行者との接触、路面凹凸による不快な振動など、視認が困難な路面状況や時々刻々と変化する道の混み具合など、様々な障害があり、毎年車いす利用による重大事故が発生しており、車いす移動に不安を感じる利用者が少なくない。この問題の解決手段として、車いすに取り付けたセンサから、走行ログを分析し、目に見えない危険の可視化や、危険を予測し車いす利用者にフィードバックを返す仕組みが考えられている^[8]。このようなシステムを実現するには、車いす走行時の路面状況や位置情報、運転者の姿勢や操作情報の個人情報や安全にサーバにアップロードし、かつ、サーバから利用者へフィードバックを返す仕組みが必要になる。このような仕組みを利用者自身が所有する車いすに作り込むことは既存の技術でも可能と考えられるが、新しい車いすを購入した、1つの車いすを複数の利用者で利用する、旅行先で一時的に車いすを借りる等、作り込

みが困難な場合にも利用できる柔軟なシステムの構築が望ましい。

HIMALISを導入すると、車いす、個々のセンサ、利用者所有の端末はそれぞれサーバで識別され、管理される。これによりサーバは、利用者の情報(体力、運転の癖、疾患など)を元に個々のデバイスを遠隔から再設定し、サービス提供に最適な状態にすることができる。

4 システム設計と実装

4.1 モバイルセンサ群を収容する HIMALIS ネットワークの実装

ID ベース通信を用いた IoT/M2M の例として前節で述べた、センサ群を収容する HIMALIS ネットワークの評価を行うため、MS、MG の実装を行った(図5)。

MS は、様々なセンサボードを取付け、移動体に設置することを想定し、Raspberry Pi をベースに開発した。Raspberry Pi に、HIMALIS スタックを追加実装した Raspbian OS 3.2.27 をインストールし、MS から直接 ID ベース通信できるようにしている。通信モジュールには、IEEE802.15.4 対応 XBee モジュールを採用し、6 LoWPAN プロトコルで IP 通信を可能としている。複数のセンサの動的制御機能を確認するため、温度、湿度、照度、気圧の4種のセンサを搭載したセンサボードを取り付けた。センサボードは、USB ケーブルで Raspberry Pi に接続し、必要に応じて別のセンサボードに付け替えることができる。

MG は、移動体への設置が容易で、GUI と直感的な操作が可能な Android タブレットをベースに開発した。エッジネットワークへの接続には、内蔵無線 LAN アダプタを用いるが、外付け無線 LAN アダプタを付けることにより、ハンドオーバー中のパケット損

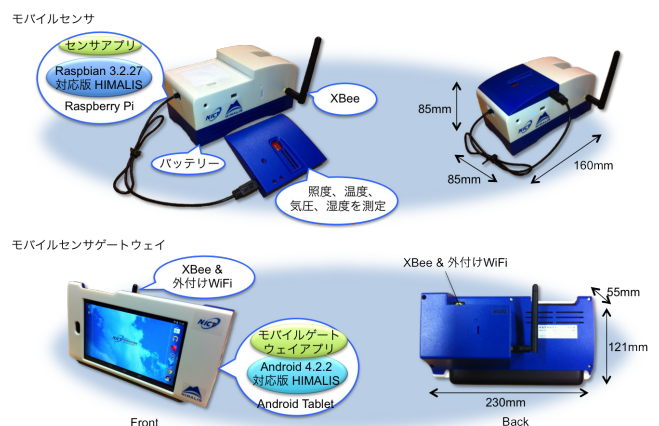


図5 モバイルセンサ、モバイルゲートウェイの実装

失が少ない make-before-break ハンドオーバをサポートする。また、MS の通信パケットを中継し、ID ヘッダを見て適切にパケット転送を行うため、MG には、HIMALIS スタックを追加実装した AndroidOS 4.2.2 をインストールした。そして、MS と接続するため、XBee 無線モジュールを搭載し、6 LoWPAN プロトコルの実装を行った。XBee を用いた通信でパケット衝突を低減するため、XBee 標準の Digi Mode 通信ではなく、CSMA/CA (Carrier Sense Multiple Access/ Collision Avoidance) を用いた。

モバイルセンサ群を収容する HIMALIS ネットワークのシステム構成を図 6 に示す。MS、MG は、図のように接続する。MG に 2 つの無線 LAN アダプタを持つ場合、複数のエッジネットワークにマルチホー

ム接続できる。これにより、移動中のパケット損失が少ない make-before-break ハンドオーバをサポートするので、MG がネットワークを切り替える最中でも、MS のセンサデータを中継することが可能になっている。6 LoWPAN モジュールは、ユーザランド実装し、TUN モジュールを介して HIMALIS スタックから送られる IPv6 パケットのヘッダ圧縮を行う。ヘッダ圧縮されたパケットは、XBee のシリアル伝送モジュールを介してモバイルセンサネットワークへ送信される。シンクは、センサからのデータを集めるデータベース・サーバアプリケーションと MS のセンサ制御を行うためのセンサアプリケーションが動作するモバイルホストとして実装し、エッジネットワーク、トランジットネットワークのどちらかに接続する。

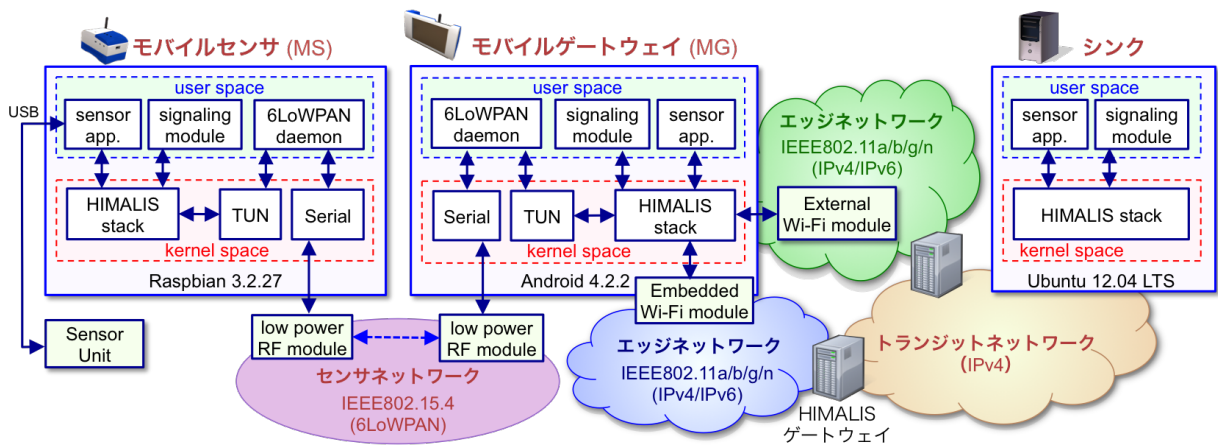
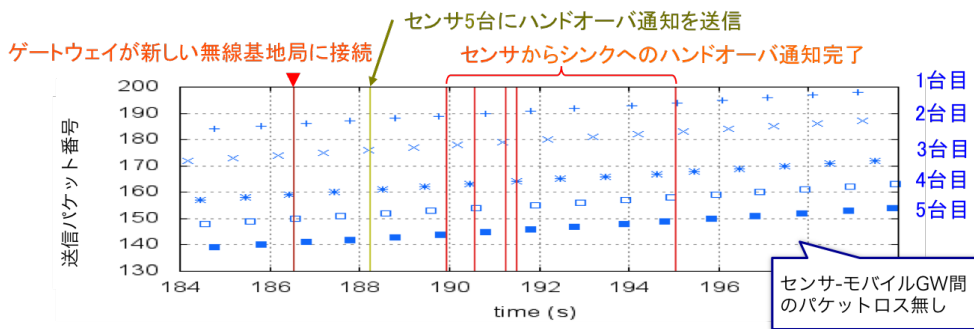


図 6 システム構成図

モバイルゲートウェイで受信したパケット



シンクで受信したパケット

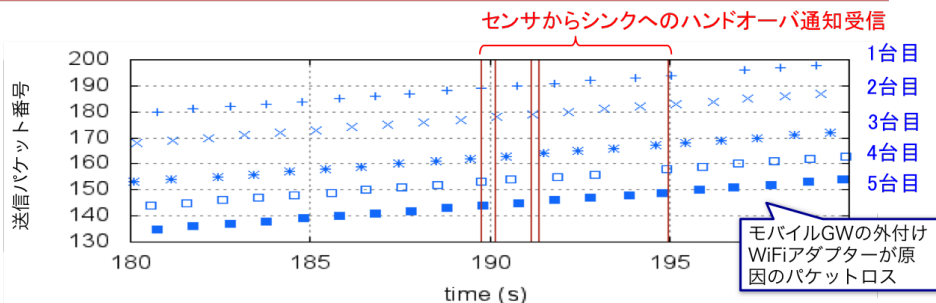


図 7 5 台の MS の通信を中継する MG が、ハンドオーバーしたときのパケット損失

4.2 モバイルゲートウェイによるモバイルセンサのハンドオーバーサポート

通信機能の動作確認ならびにハンドオーバー機能の評価を行うため、MGが任意のタイミングでエッジネットワークを切り替えたときに、MGに接続するMSの packets 損失量について調べた。まず、図6に示すネットワークを構築(青色のネットワークはIPv4、緑色のネットワークはIPv6ネットワークとした)し、MGに接続するMSを評価子やすさの観点から最大5台を増やした。5台のMSが1秒間隔で、UDPパケットをシンクへ送っているときに、MGがIPv4、IPv6エッジネットワークを切り替えた。図7は、この時にMGとシンクでそれぞれ受信できたパケットを示している。図7の横軸は各パケットの受信時間を示し、縦軸はMSが送信するときに1から順にパケットに付与するパケットIDを示す。これにより、いつ、どのMSのどのパケットが受信できたかひと目でわかるようにしている。5台のMSからMGへ送られたパケットは、IEEE802.15.4とIEEE802.11 b/gが混在している状況にも関わらず全て受信できていることがわかる。一方、MGとシンク間では、ハンドオーバー処理直後からパケット損失が認められた。このパケット損失は、外付け無線LANアダプタのドライバが原因であることがわかった。上記実験により、MSのデータ送信に影響なく、MGが任意のタイミングでネットワーク切替えが可能であることがわかった。

4.3 センサアプリケーション

シンクからMSを管理・制御する共通のプラットフォームとして、センサアプリケーションを開発した。IDベース通信の性質上、シンクからMSへ直接通信を行うアプリケーションの作成は容易であるが、本ア

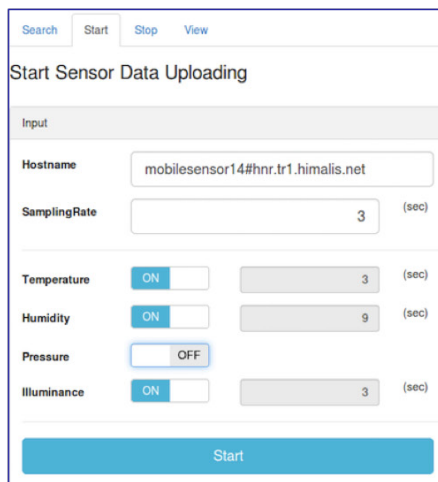
プリケーションは、センサの起動・停止など、共通のオペレーションに対する処理最適化や、M2MのためのAPI提供手段を目的として開発している。

シンク用のセンサアプリケーションは、Webベースのセンサ管理ツールである。MSの管理者は、Webブラウザでシンクにアクセスすることで、IDベース通信を用いたMSの検索、センサデータの送信開始や停止、アップロードされるセンサデータのモニタが簡易に実行できる。ブラウザベースのセンサ制御パネルを図8左に示す。この制御画面では、hostnameにMSのホスト名を入れ、起動したいセンサとサンプリングレートを選択する。これにより、必要に応じて特定のセンサのサンプリングレートを変える、消費電力削減のため不要なセンサデータの取得停止ができる。

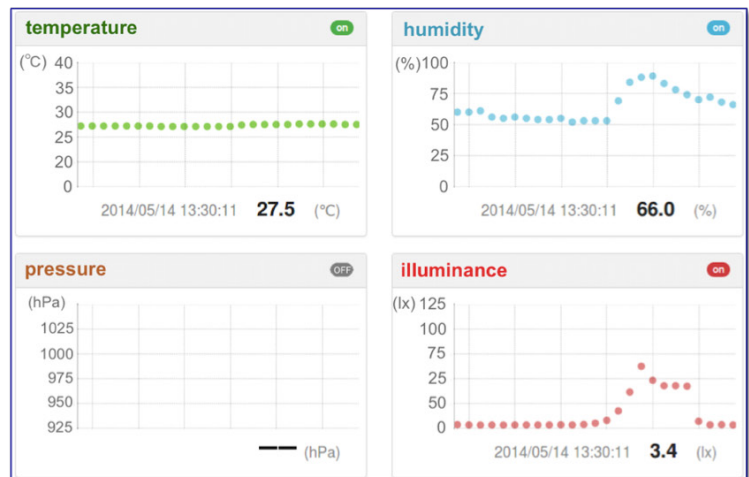
MS用のセンサアプリケーションは、シンクから送られる制御メッセージに基づいて、センサの起動状態を通知、指定されたセンサデータのアップロード開始、停止を制御する。センサが送るデータは、取得データ、取得時間を持ち、中間者からのデータ改ざんを防ぐため、シンクと予め交換した共有鍵で署名される。

MG用のセンサアプリケーションは、中継するセンサデータにGPSで所得した位置情報を付与する機能を持つ。また、複数のシンクから同一MSへデータアップロード要求がある場合に、MSが同一センサデータを複数回送信するのを避けるため、MGが複数のシンクへ同時にセンサデータを送る機能も有する。

上記センサアプリケーションを実装し、遠隔のMSが持つセンサの動的制御及びモニタリング機能が実現できたことを確認した(図8右)。



ブラウザベースのセンサ制御パネル



センサの環境センサをモニタする可視化画面

図8 モバイルセンサを管理・制御するシンクのセンサアプリケーション画面

5 おわりに

異なる通信方式で接続する膨大な数の端末が M2M する将来 IoT では、インターネットを介した端末管理や安全に遠隔制御を行う仕組みが必要となる。このような将来 IoT/M2M 実現の例として、本稿は、端末管理の仕組みや、異種通信方式間で安全に通信継続できる仕組みを有する ID・ロケータ分離ネットワーク HIMALIS へのモバイルセンサ群収容の検討を行った。モバイルセンサ及びデータを中継するゲートウェイ、データを蓄積するシンクそれぞれに、HIMALIS の ID ベース通信方式を導入することで、異種通信方式で接続するモバイル端末間の M2M が実現可能であることを、実機実装を通して明らかにした。今後は、制御メッセージの最適化を行い、複数のデバイスで通信可能であることを実証する予定である。

6 謝辞

本研究は、原井洋明室長、藤川賢治主任研究員、寺西裕一研究マネージャー、戸室知二技術員、小針康永技術員らと実施した。また、研究開発にご協力いただいた関係各位に感謝する。

【参考文献】

- 1 Ericsson, "More than 50 billion connected devices," White Paper, Feb. 2011.
- 2 ITU-T Focus Group Technical Report on M2M Service Layer, "M2M service layer: Requirements and architectural framework," 2014.
- 3 R. Moskowitz and P. Nikander, "Host Identity Protocol (HIP) Architecture," RFC 4423, May 2006.
- 4 V.P. Kafle and M. Inoue, "HIMALIS: Heterogeneity inclusion and mobility adaptation through locator ID separation in new generation networks," IEICE Trans. Commun., Vol.E93-B, No.3, pp.478-489, March 2010.
- 5 大規模オープンテストベッド JOSE, <http://www.nict.go.jp/nrh/nwgn/jose.html>
- 6 V. P. Kafle, Y. Fukushima, and H. Harai, "Design and Implementation of Dynamic Mobile Sensor Network Platform for ID-Based Communication," IEEE Communications Magazine – Communications Standards Supplement, Vol.53, Issue 3, pp.48-57, March 2015.
- 7 福島 裕介, ベド カフレ, 原井 洋明, 次世代モバイルネットワークにおける M2M のための ID ベース通信, 電子情報通信学会技術報告 無線通信システム研究会, Vol.114, No.372, RCS2014-250, pp.177-182, 2014 年 12 月
- 8 Y. Iwasawa, H. Suzuki, and I.E.Yairi, "Detecting Exceptional Actions Using Wearable Sensors' Data for Developing Life-Log Database of Visually Impaired People," AAAI Spring Symposium: Data Driven Wellness 2013, pp.6-11, 2013.



福島裕介 (ふくしま ゆうすけ)

光ネットワーク研究所ネットワークアーキテクチャ研究室研究員
博士 (情報科学)
ネットワークアーキテクチャ、モバイルネットワーク、新世代ネットワーク



Ved P. Kafle

光ネットワーク研究所ネットワークアーキテクチャ研究室主任研究員
Ph.D.(Infomatics)
ネットワークアーキテクチャ、モバイルネットワーク、新世代ネットワーク