

# Bluetooth over DTLSによる 宅内 Bluetooth 機器向け遠隔接続システムの評価

岡田 真実<sup>1,a)</sup> 鈴木 秀和<sup>1,b)</sup>

概要：宅内の情報家電機器を制御するための短距離無線通信規格の1つとして Bluetooth がある。しかし、Bluetooth は通信可能範囲が限定されているため、宅外から宅内の機器を Bluetooth の仕組みで直接遠隔制御することができない。筆者らは遠隔地にある Bluetooth 機器を近傍に存在しているように仮想的に認識することにより、どこからでも遠隔接続可能なシステムを提案している。本稿では提案システムにおける Bluetooth 制御メッセージの伝送の安全性を向上させるために、ユーザ認証機能および DTLS (Datagram Transport Layer Security) を用いた暗号化通信機能を新たに定義する。プロトタイプ実装により動作検証を行った結果、モバイルインターネット環境を利用して宅内の Bluetooth 機器を Bluetooth で規定されているタイムアウト時間より十分に短い範囲で探索できることを確認した。

## Evaluation of Remote Connection System for Home Bluetooth Devices with Bluetooth over DTLS

OKADA MAMI<sup>1,a)</sup> SUZUKI HIDEKAZU<sup>1,b)</sup>

### 1. はじめに

情報家電機器や電化製品をはじめとする我々の身の回りにあるあらゆるモノがインターネットに繋がり、人々の生活をより便利にしたり、産業をより効率化したりすることが期待されている IoT (Internet of Things) が注目を集めている。文献 [1] によると、2021 年には 1 兆 4000 億ドル規模の市場に拡大する予測が示されている。IoT は用途や対象により様々な通信規格が存在するが、ユーザのスマートフォンと連携することで様々なサービスを展開可能な短距離通信規格として、Bluetooth が主流となっている。

Bluetooth には初期に登場した BR (Basic Rate) の規格の他、伝送速度を向上させた EDR (Enhanced Data Rate) の規格がよく採用されていた。現在は Bluetooth version 4.0 で新たに追加定義された LE (Low Energy) 規格が主

流となっており、従来の BR/EDR と比較して超低消費電力で通信できるという特徴を有している。Bluetooth プロトコルスタックはホストとコントローラから構成されており、両者の間に定義されている HCI (Host Controller Interface) 層に含まれる HCI ドライバ (ソフトウェア) と HCI コントローラ (ハードウェアのファームウェア) 間で HCI コマンド、HCI イベントと呼ばれる制御メッセージおよび HCI データを交換することにより、他の Bluetooth 機器との通信を実現している [2]。本稿では HCI 層で交換されるこれらの制御メッセージおよびデータをまとめて HCI メッセージと呼ぶ。

しかし、Bluetooth は通信可能範囲が物理的に制限されているため、ユーザは宅内に設置された Bluetooth 機器を制御する場合は、その機器の近傍に位置していなければならない。そのため、Bluetooth 機器が宅内のホームゲートウェイ等に接続してインターネットに間接的に繋がっていたとしても、ユーザは宅外から宅内の機器を Bluetooth 対応アプリケーションで直接操作することができない。Bluetooth 4.2 ではスマートフォンなどとペアリングするこ

<sup>1</sup> 名城大学大学院理工学研究科  
Graduate School of Science and Technology, Meijo University

a) mami.okada@ucl.meijo-u.ac.jp

b) hsuzuki@meijo-u.ac.jp

と無く、ルータを介して直接インターネット接続することが可能な IPSP (Internet Protocol Support Profile) [3] と呼ぶインターネット接続用プロファイルが定義されているが、Bluetooth 機器およびスマートフォン等の操作機器にインストールされるソフトウェアがこのプロファイルを利用した仕様で開発されていなければならないこと、また宅内に設置するルータが 6LoWPAN (IPv6 over Low power Wireless Personal Area Networks) over BLE [4] をサポートしていなければならないなど、特定の条件が揃わなければ宅外から直接接続することはできない。

遠隔地に存在する Bluetooth 機器を操作するために、Bluetooth とは異なる別のプロトコルを連携することにより、Bluetooth 機器に制御メッセージを送信したり、通信結果を受信するサービスや技術が登場している [5-9]。さらに、Bluetooth 通信自体を遠隔地へ伝送することにより、ユーザは宅外先からでも宅内と同じ操作アプリケーションで Bluetooth 機器を操作できる手法も研究されている [10,11]。しかし、従来の遠隔制御システムや既存研究では、ユーザは自身の位置に応じて操作アプリケーションを使い分けたり、専用の装置を常に携帯していなければならないなど、ユーザの利便性がよいとは言えない。

そこで、筆者らはこれらの課題を解決すべく、ユーザビリティに優れた Bluetooth 機器の遠隔接続手法を提案してきた [12-14]。本稿では提案システムに対してユーザ認証機能および DTLS (Datagram Transport Layer Security) [15] を用いた暗号化通信機能を追加し、その概要と実装について述べる。また、提案システムのプロトタイプ実装、および実環境における性能評価の結果について報告する。

以下、2 章で既存研究とその課題を示し、3 章でセキュリティを向上させた提案システムの概要について述べる。4 章で実装、5 章で評価について述べ、6 章でまとめる。

## 2. 既存研究

遠隔地に存在する Bluetooth 機器を制御する手段として、異なるプロトコルを連携して遠隔地にある専用の装置に制御メッセージを伝送し、遠隔地の Bluetooth 機器との通信結果を連携プロトコルにより取得する方法がある。東芝 HEMS (Home Energy Management System) [5] では、東芝 Web サービスとして「フェミニティ倶楽部」を構築し、ユーザに様々なサービスを提供している。図 1 に示すように、外出先のユーザは HTTPS (Hypertext Transfer Protocol Secure) を用いて Web サービスにアクセスし、宅内に設置されているホームゲートウェイに宅内の Bluetooth 機器に対して制御命令を送信する。ホームゲートウェイは受信した命令に従って制御対象の機器と Bluetooth 通信を行い、制御結果を HTTPS により応答する。この他にも PUC (P2P Universal Computing Consortium) アーキテクチャ [6-8] や UbiGate [9] も第三のプロトコルを連携す

ることにより、同様の仕組みで遠隔地にある Bluetooth 機器を制御することができる。

しかし、ユーザは自身の位置に応じて操作アプリケーションを使い分ける必要がある。宅内にいる場合は Bluetooth で直接操作するアプリケーションを利用し、宅外では HTTPS で Web サービスにアクセスするアプリケーションを利用しなければならないため、ユーザビリティが高いとは言えない。また、Bluetooth 機器の遠隔操作履歴が Web サーバに残ってしまう可能性があり、プライバシー侵害の懸念が残されている。さらに、アプリケーション提供者は Web サービスと 2 種類のアプリケーションを開発し、さらに Web サービスを提供するサーバを継続的に運用しなければならず、遠隔制御を実現するためのコストが高い等の課題がある。

ユーザの位置に関わらず、常に Bluetooth 通信を行う操作アプリケーションだけで遠隔地にある Bluetooth 機器を制御することが可能な手法として、図 2 に示す UbiPAN [11] が提案されている。この手法は UbiGate を拡張したものであり、遠隔地に存在する UbiGate Gateway (UGW) がその近隣に存在する Bluetooth 機器を探索し、その結果をユーザの近隣に設置した UGW まで SIP (Session Initiation Protocol) [16] を用いて伝送する。この状態でユーザが近隣の Bluetooth 機器を探索すると、近隣の UGW が遠隔地に存在している Bluetooth 機器の情報を返信することにより、遠隔地の Bluetooth 機器を発見することができる。物理的な距離の制約に縛られず、Bluetooth ネットワークが遠方まで拡大したように認識できることが、前述した既存サービスや既存研究にはない特徴である。この他に、有線回線により Bluetooth ネットワークを拡張する手法 [10] も同様の考え方で遠隔制御できることを提案している。

しかし、ユーザは常に UGW を携帯しなければならないことや、どの UGW 配下にどのようなサービスを実行できる Bluetooth 機器が存在するかなどの情報を収集および管

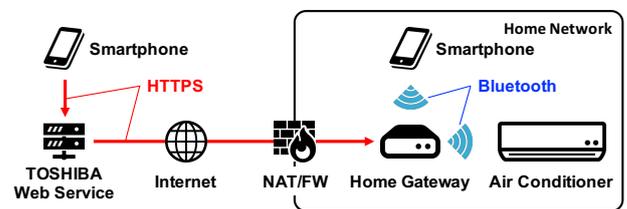


図 1 東芝 HEMS の概要

Fig. 1 Overview of Toshiba HEMS.

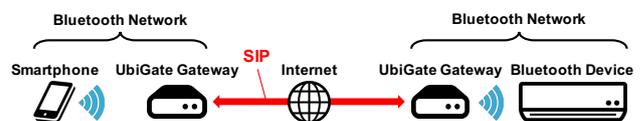


図 2 UbiPAN の概要

Fig. 2 Overview of UbiPAN.

理するための Register サーバを導入，運用する必要がある．

### 3. 提案システム

#### 3.1 概要

筆者らは2章で述べた既存研究の課題を解決するために，Bluetooth ネットワークを拡大するアプローチを採用した遠隔地にある Bluetooth 機器のシームレス接続システムを提案している [12–14]．図 3 に提案システムの概要を示す．提案システムは操作端末を CD (Control Device)，CD の近隣に存在する Bluetooth 機器を ND (Neighbor Device)，宅内に設置される専用の機器を BGW (Bluetooth Gateway)，BGW の近隣に存在し CD の遠隔制御対象となる Bluetooth 機器を RD (Remote Device) から構成されている．

提案システムでは，Bluetooth プロトコルスタックにおけるホストとコントローラの間で交換されている HCI メッセージのコピーを遠隔地に設置した BGW (Bluetooth Gateway) へ UDP トンネル通信により伝送する．これにより，遠隔地に設置されている BGW の Bluetooth コントローラに対して HCI メッセージを届けることができるため，CD は BGW の Bluetooth インタフェースを自身のインタフェースであるかのように操作することができる．BGW が近隣の Bluetooth 機器を探索または通信を行って RD からの応答を受信すると，Bluetooth コントローラからホストへ渡される HCI メッセージをフックし，自身の Bluetooth ホストではなく UDP トンネル通信により CD 側へ送り返す．CD は ND だけでなく BGW から受け取る RD からの情報を受け取ることができる．

これにより既存研究のようにユーザは専用の装置を携帯する必要が無く，かつ場所の違いに影響されことなく常に単一の操作アプリケーションで同じように Bluetooth 機器を探索，操作することができる．なお，文献 [12–14] では CD と BGW 間は UDP トンネルを構築していたが，本稿ではセキュリティを向上させるために DTLS (Datagram Transport Layer Security) を適用し，ユーザ認証処理を新たに追加することとした．

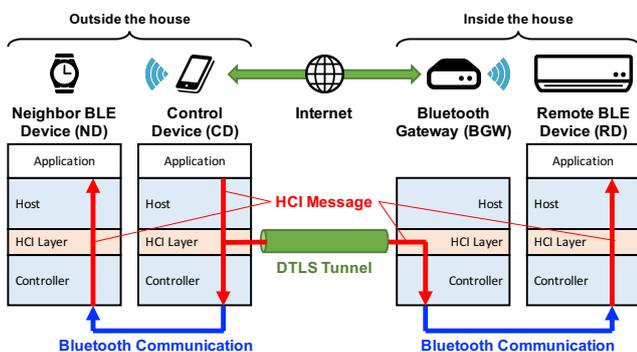


図 3 提案システムの概要

Fig. 3 Overview of the proposed system.

#### 3.2 通信シーケンス

事前の準備として，ユーザはあらかじめ BGW との間で 3.2.1 項で述べるユーザ認証処理を行う．なお，自宅の NAT/ファイアウォール (FW) に対して宅外から BGW に対して DTLS 通信ができるよう，ポートフォワードリングの設定を行っているものとする．

##### 3.2.1 ユーザ認証フェーズ

提案システムでは CD と BGW の双方向認証を行うため，公開鍵証明書およびパスワードを用いた 2 種類のユーザ認証モードをサポートする．なお，以下に示すユーザ認証処理はユーザが宅外のネットワークに移動した際に 1 回だけ実施するものであり，宅内に存在する場合は必要としない．

###### (1) 公開鍵証明書によるユーザ認証モード

この認証モードでは，BGW において CA (Certification Authority) を構築し，BGW 用にサーバ証明書を，CD 用にクライアント証明書を発行する．図 4 に公開鍵証明書を用いたユーザ認証シーケンスを示す．CD が宅外のネットワークに接続すると，BGW に対して DTLS ハンドシェイクを開始し，両者は自信の公開鍵証明書を交換して共通鍵を生成する．CD および BGW は DTLS の枠組み内で双方向認証が行われ，DTLS ハンドシェイクが完了するとユーザ認証も完了し，DTLS トンネルが生成される．

###### (2) パスワードによるユーザ認証モード

公開鍵証明書を用いたユーザ認証モードでは，CD に対してクライアント証明書を発行してインストールする作業が必要となり，ユーザにとって負担となることが考えられる．そこで，CD にクライアント証明書を発行したり，インストールする手間を省略する代わりに，ユーザ名とパスワードを用いて CD を認証する方法を選択することができる．この認証モードでは，BGW にはサーバ証明書のほか，ユーザ名とパスワードを記載したユーザ認証情報を準備しておく．

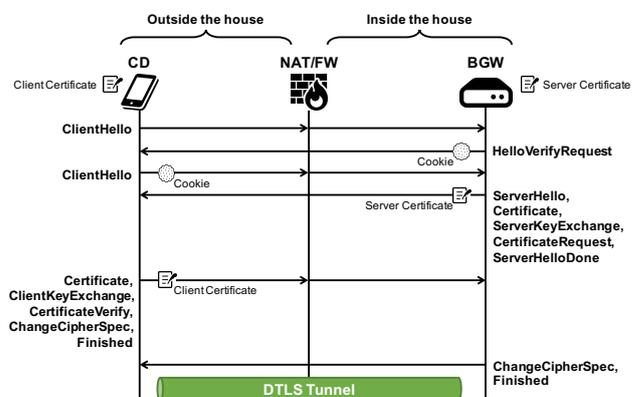


図 4 公開鍵証明書を用いたユーザ認証シーケンス

Fig. 4 Sequence of the user authentication using public key certificates.

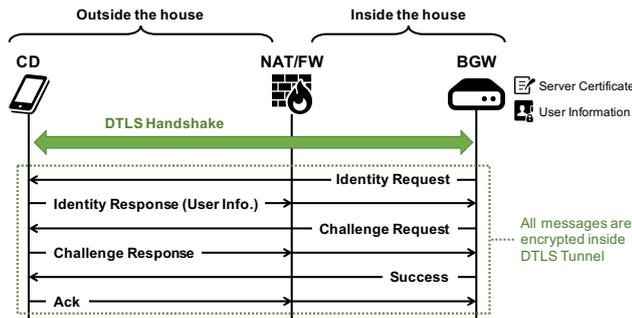


図 5 パスワードを用いたユーザ認証シーケンス

Fig. 5 Sequence of the user authentication using the password.

図 5 にパスワードを用いたユーザ認証シーケンスを示す。まず、CD が BGW に対して DTLS ハンドシェイクすることは変わらないが、DTLS ハンドシェイクでは BGW 側のみサーバ証明書により認証することができる。そのため、DTLS ハンドシェイクが完了して DTLS トンネルが構築された後、クライアント認証処理に移る。

まず、BGW が CD に対して Identity Request メッセージを送信し、ユーザ認証を要求する。CD はユーザ名とパスワードを入力し、Identity Response メッセージにより返信する。さらに再送攻撃によるなりすまし行為を防止するために、BGW は CHAP (Challenge-Handshake Authentication Protocol) [17] で採用されているチャレンジを CD へ行い、CD はそれに対する応答を返す。以上の処理により、CD と BGW 間で DTLS による暗号化トンネルが形成され、かつ双方向認証が完了する。

なお、この双方向認証手順については、EAP-TTLSv0 (Extensible Authentication Protocol Tunneled Transport Layer Security Authenticated Protocol Version 0) [18] および PEAPv0 (Protected EAP) [19] などのユーザ ID とパスワードを用いた認証プロトコルに準じて定義したものである。

### 3.2.2 Bluetooth 通信フェーズ

3.2.1 項で示したユーザ認証フェーズの完了後、CD で Bluetooth 通信を行う場合は図 6 に示す流れで Bluetooth 通信が行われる。まず、CD 側で Bluetooth 通信を行う操作アプリケーションを起動して近隣の Bluetooth 機器の探索を開始すると、Bluetooth ホストからコントローラに向けて HCI メッセージが渡される。ここで、HCI 層において HCI メッセージを複製し、元の HCI メッセージはそのままコントローラに渡して、CD は自身の Bluetooth インタフェースを用いて近隣の Bluetooth デバイス ND を探索する。ND を発見した場合は通常の Bluetooth プロトコルスタックの処理手順により探索結果がアプリケーションに渡される。

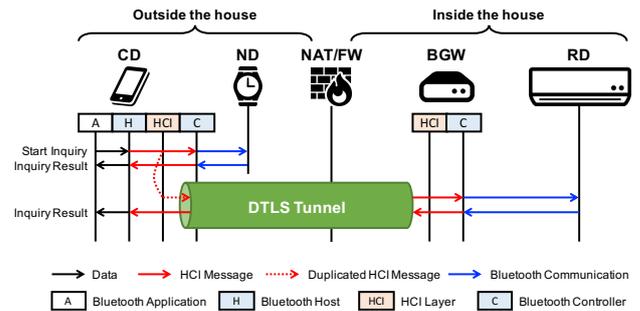


図 6 Bluetooth 通信シーケンス

Fig. 6 Sequence of the Bluetooth communication.

一方、複製された HCI メッセージはユーザ認証フェーズで構築した DTLS トンネルを利用して BGW へ伝送される。BGW は CD から HCI メッセージを受信すると、自身の Bluetooth コントローラへ HCI メッセージを渡し、近隣の Bluetooth 機器 RD を探索する。RD を発見した場合は逆の手順により HCI メッセージを CDS 側へ伝送する。CD は BGW から受信した HCI メッセージを自身の Bluetooth ホストへ渡す。以上の処理により、操作アプリケーションに RD の情報も渡される。

以後、発見したデバイスとの Bluetooth 通信についても Bluetooth ホストとコントローラ間で HCI メッセージをやり取りすることにより実現されるため、上記と同じ手順で処理することになる。このように Bluetooth over DTLS 通信を行うことにより、ユーザは自身の場所や Bluetooth で定められている通信可能範囲を考慮することなく、遠隔地にある Bluetooth 機器とシームレスに接続することができる。

## 4. 実装

提案システムを実現するためには、Bluetooth プロトコルスタックにおける HCI 層で HCI メッセージの複製を BGW へ伝送し、BGW 側から受け取った HCI メッセージを CD のプロトコルスタック戻す処理が必要である。そこで、提案システムを実現するために、Linux PC を利用し、Linux に実装されている Bluetooth プロトコルスタック BlueZ [20] のカーネルモジュールを拡張した。また、DTLS トンネルの構築、ユーザ認証処理および HCI メッセージの伝送を行うために HCI Forwarder デモンを実装した。図 7 にモジュール構成を示し、その詳細を以下に説明する。

### 4.1 Bluetooth プロトコルスタックの拡張

CD 側の BlueZ に実装されている HCI 層における HCI メッセージの送信処理部に HCI メッセージが格納されているソケットバッファを複製する処理を追加した。複製したソケットバッファは Bluetooth カーネルモジュールに新たに追加した関数へ渡し、Netlink ソケット [21] を用いてユーザランドで動作している HCI Forwarder デモンへ渡



ND 探索時間を測定したところ、589.18 ミリ秒であったことを踏まえると、提案システムでは ND 探索時間が増加していることがわかる。これは提案方式において HCI メッセージを複製した際、先に HCI Forwarder デーモンに複製した HCI メッセージを渡してから、元の HCI メッセージを Bluetooth コントローラへ渡す順序で実装を行っていることが原因であると考えられる。一方、RD の探索には ND の探索時間に加えて CD と BGW 間の通信遅延および DTLS に基づく暗号化および認証処理時間が加算されているが、Bluetooth の仕様で定義されている探索間隔 2.56 秒の範囲で収まっており、実用上問題ないと考えられる。

## 5.2 考察

本稿では BlueZ を利用して提案システムのプロトタイプを実装したが、今後は Android スマートフォンへの移植を検討している。Android は Linux カーネルを採用しており、バージョン 4.1 までは PC 向け Linux と同様に BlueZ が採用されていた。そのため、提案システムの機能をクロスコンパイルすることにより、Android スマートフォンへ移植することができる。ただし、現在市販されている Android スマートフォン（バージョン 4.2~5.1）は“Bluedroid”と呼ぶ新しい Bluetooth プロトコルスタック変更されている。さらに Bluedroid は“Fluoride”と名称を変更し、Android 6.0 以降に実装されている [23]。

そこで、提案方式が Fluoride に適用できるかを検討した。図 9 に Fluoride の Bluetooth プロトコルスタックを示す [24]。Fluoride では HCI 層や HCI メッセージをトレースするためのカスタムエクステンションを追加するために、ベンダー拡張が可能な仕組みが用意されている。そのため、libbt-hci モジュールを開発することにより、提案システムの機能を実装できると考えられる。従って、最新の Android スマートフォンを CD として利用して、提案システムを実現することができる。

## 6. まとめ

本稿では、遠隔地にある Bluetooth 機器を仮想的に発見、接続および通信する手法にユーザ認証処理および DTLS による暗号化機能を追加した。提案システムでは Bluetooth プロトコルスタックにおけるホストとコントローラ間でやり取りされる制御メッセージを DTLS トンネルを用いて遠隔地の BGW に伝送することにより、BGW の近傍に存在する RD を CD の近隣に存在するように認識させることができることを示した。また、提案システムのプロトタイプ実装を行い、実環境において動作検証および通信遅延を評価した。その結果、Bluetooth で規定されているタイムアウト時間内に CD が遠隔地の RD を発見できることを確認した。また、現在市販されている Android スマートフォンに提案手法を適用できることを示した。

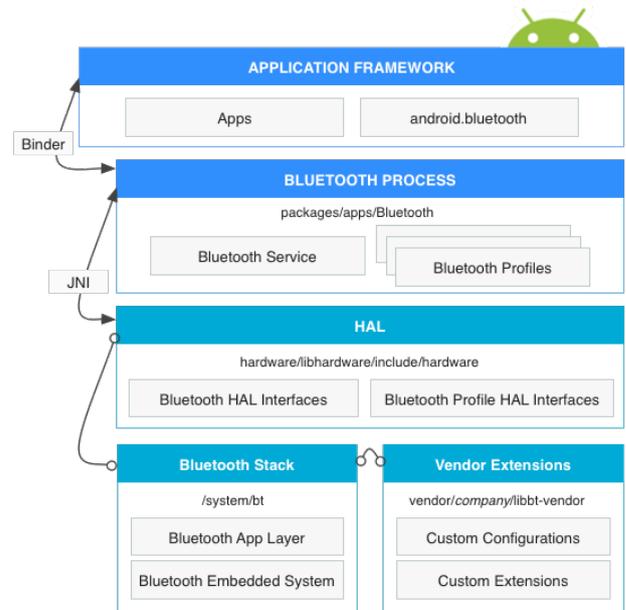


図 9 Fluoride の Bluetooth プロトコルスタック

Fig. 9 Bluetooth protocol stack of Fluoride.

今後は提案システムを Android へ移植し、スマートフォンでの実現を目指す。また、提案システムを応用として、Bluetooth の制御メッセージだけでなく、様々なデバイスの制御メッセージを遠隔地に設置したゲートウェイに送信することにより、ゲートウェイに装着されているデバイスをスマートフォンに仮想的に装着して遠隔制御する手法について検討する予定である。

謝辞 本研究の一部は、東北大学電気通信研究所における共同プロジェクト研究の支援によって行われた。

## 参考文献

- [1] Shirer, M. and Torchia, M.: Worldwide Spending on the Internet of Things Forecast to Reach Nearly \$1.4 Trillion in 2021, According to New IDC Spending Guide, IDC Research, Inc. (online), available from <http://www.idc.com/getdoc.jsp?containerId=prUS42799917> (accessed 2017-07-29).
- [2] Bluetooth SIG: BLUETOOTH SPECIFICATION Version 4.0, Vol. 1, Bluetooth SIG (2010).
- [3] Internet WG: Internet Protocol Support Profile Bluetooth Specification, Technical report, Bluetooth SIG (2014).
- [4] Nieminen, J., Savolainen, T., Isomaki, M., Patil, B., Shelby, Z. and Gomez, C.: IPv6 over BLUETOOTH(R) Low Energy, RFC 7668, IETF (2015).
- [5] 一色正男, 河口俊朗, 平原茂利夫: 広がる東芝ネットワーク家電“フェミニティ”シリーズ, 東芝レビュー, Vol. 60, No. 4, pp. 23-27 (オンライン), 入手先 [https://www.toshiba.co.jp/tech/review/2005/04/60\\_04\\_pdf/a07.pdf](https://www.toshiba.co.jp/tech/review/2005/04/60_04_pdf/a07.pdf) (2005).
- [6] Sumino, H., Ishikawa, N., Murakami, S., Kato, T. and Hjelm, J.: Pucc Architecture, Protocols and Applications, *Proceedings of the 4th IEEE Consumer Communications and Networking Conference, CCNC 2007*, pp. 788-792 (2007).

- [7] 伊藤崇洋, 加藤悠一郎, 峰野博史, 石川憲洋, 水野忠則: 異種デバイス連携基盤を用いたセンサ・家電制御アプリケーション, 情報処理学会研究報告コンピュータセキュリティ(CSEC), Vol. 2011-CSEC-52, No. 35, pp. 1-6 (2011).
- [8] 田中 剛, 伊藤崇洋, 加藤悠一郎, 峰野博史, 水野忠則: Android 端末を用いた異種ネットワークデバイス連携システムの開発, マルチメディア, 分散協調とモバイルシンポジウム 2011 論文集, DICOMO2011, Vol. 2011, pp. 1257-1264 (2011).
- [9] Bissyandé, T. F. d., Réveillère, L. and Bromberg, Y.-D.: UbiGate: A Gateway to Transform Discovery Information into Presence Information, *Proceedings of the 4th International Workshop on Services Integration in Pervasive Environments*, SIPE 2009, pp. 19-24 (2009).
- [10] 井波政朗, 丹 康雄: Bluetooth ネットワークの有線拡張方式に関する検討, 電子情報通信学会技術研究報告, CS2003, Vol. 103, No. 415, pp. 47-52 (2003).
- [11] Albert, J., Bissyandé, T. F., Bromberg, Y.-D., Chaumette, S. and Réveillère, L.: UbiPAN: A Bluetooth Extended Personal Area Network, *Proceedings of the 4th International Conference on Complex, Intelligent and Software Intensive Systems*, CISIS 2010, pp. 774-778 (2010).
- [12] Tsuda, K., Suzuki, H., Asahi, K. and Watanabe, A.: Proposal for a Seamless Connection Method for Remotely Located Bluetooth Device, *Proceedings of the 7th International Conference on Mobile Computing and Ubiquitous Networking*, ICMU 2014, pp. 78-79 (2014).
- [13] 岡田真実, 鈴木秀和: 遠隔地にある Bluetooth LE 機器のシームレス接続手法の検証, 情報処理学会研究報告コンシューマ・デバイス&システム(CDS), Vol. 2016-CDS-17, No. 13, pp. 1-7 (2016).
- [14] Okada, M. and Suzuki, H.: Implementation of Seamless Connection System for Bluetooth Low Energy Devices in Remote Locations, *Proceedings of the 35th International Conference on Consumer Electronics*, ICCE 2017, pp. 341-342 (2017).
- [15] Rescorla, E. and Modadugu, N.: Datagram Transport Layer Security Version 1.2, RFC 6347, IETF (2012).
- [16] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M. and Schooler, E.: SIP: Session Initiation Protocol, RFC 3261, IETF (2002).
- [17] Simpson, W.: PPP Challenge Handshake Authentication Protocol (CHAP), RFC 1994, IETF (1996).
- [18] Funk, P. and Blake-Wilson, S.: Extensible Authentication Protocol Tunneled Transport Layer Security Authenticated Protocol Version 0 (EAP-TTLSv0), RFC 5281, IETF (2008).
- [19] Kamath, V., Palekar, A. and Wodrich, M.: Microsoft's PEAP version 0 (Implementation in Windows XP SP1), Internet-draft, IETF (2002). draft-kamath-pppext-peapv0-00.txt.
- [20] BlueZ Project: BlueZ, available from <http://www.bluez.org/> (accessed 2016-07-26).
- [21] Salim, J., Khosravi, H., Kleen, A. and Kuznetsov, A.: Linux Netlink as an IP Services Protocol, RFC 3549, IETF (2003).
- [22] OpenSSL Project: Cryptography and SSL/TLS Toolkit, available from <https://www.openssl.org/> (accessed 2017-07-29).
- [23] Git at Google: Fluoride Bluetooth stack, available from <https://android.googlesource.com/platform/system/bt/> (accessed 2017-07-29).
- [24] Android Open Source Project: Bluetooth, available from <https://source.android.com/devices/bluetooth.html> (accessed 2016-07-29).