Computer Security Symposium 2020
26 - 29 October 2020

Bluetooth Low Energyに対する攻撃手法の発見と対策

石井 健太郎[1,a)]　白石 善明[1]　森井 昌克[1]

概要：Bluetooth Low Energy（BLE）は，短距離無線通信技術として，身の回りのデバイスにおいても広く使われるようになった．スマートロックなどのBLEを用いたデバイスは，重要な情報を取り扱うため，そのセキュリティは重要である．BLEにはセキュリティ機能が用意されているが，デバイス製作時のコストなどの理由により，多くのデバイスがその機能を十分に利用していない．そのようなデバイスは，容易に攻撃が可能となってしまう．BLEに対する攻撃のひとつに，中間者攻撃がある．中間者攻撃とは，攻撃者が正規の通信者になりすまし，攻撃者を経由した通信を行わせるものである．中間者攻撃が成功すると，データの盗聴や改ざんが行われてしまう．本稿では，BLEに対する攻撃手法として，アドレス偽造中間者攻撃を提案する．これは，攻撃用デバイスのアドレスを，攻撃対象デバイスのアドレスに偽造することで行われる．これにより，攻撃対象デバイスに接続したいユーザを，攻撃用デバイスに接続させ，中間者攻撃を行うことが可能となる．

キーワード：Bluetooth，Bluetooth Low Energy，中間者攻撃

A Discovery of a Method for Attacking against Bluetooth Low Energy and its Prevention

Kentaro Ishii[1,a)]　Yoshiaki Shiraishi[1]　Masakatu Morii[1]

Abstract:
With the spread of the Internet of Things, Bluetooth Low Energy (BLE) has been widely used and become more important as a short-range wireless communication technology. A BLE device transfers sensitive data. Therefore, BLE security is highly important. Unfortunately, despite the fact that BLE supports several security features, a lot of devices do not implement them due to cost problems, which means those devices are vulnerable to attacks. A Man-in-the-Middle, or MitM, attack is one of the attacks against BLE. A MitM attack involves an attacker impersonating two legal devices and forces them to connect to the attacker's device. Successful MitM attack allows a malicious actor to get secret information or unlock a door at will. In this paper, we propose a noble way to attack against BLE, which involves cloning the address of a victim's BLE device as that of an attacker's device.

Keywords: Bluetooth, Bluetooth Low Energy, Man-in-the-Middle Attack

1. はじめに

IoTの普及とともに，Bluetooth Low Energy（BLE）は，身の回りのデバイスにおいても広く使われるようになった[1]．ワイヤレスキーボードやスマートロックなどのBLEデバイスは，重要な情報を取り扱うため，そのセキュリティは重要である．BLEにはセキュリティ機能が用意されているが，デバイス製作時のコストなどの理由により，多くのデバイスがその機能を十分に利用していない．そのようなデバイスは，容易に攻撃が可能となってしまう．

BLEに対する攻撃のひとつに，中間者攻撃がある．中間者攻撃とは，攻撃者が正規の通信者になりすまし，攻撃者を経由した通信を行わせるものである．中間者攻撃が成功すると，データの盗聴や改ざんが行われてしまう．

[1] 神戸大学大学院工学研究科電気電子工学専攻
Graduate School of Engineering, Kobe University
[a)] ishii@stu.kobe-u.ac.jp

© 2020 Information Processing Society of Japan

本稿では，BLE に対する攻撃手法として，アドレス偽造中間者攻撃を提案する．これは，攻撃用デバイスのアドレスを，攻撃対象デバイスのアドレスに偽造することで行われる．これにより，攻撃対象デバイスに接続したいユーザを，攻撃用デバイスに接続させ，中間者攻撃を行うことが可能となる．

実際の BLE アプリケーションに対する攻撃検証として，スマートロックに対する中間者攻撃を行った．スマートロックは，住宅の扉の鍵に取り付けて，BLE や Wi-Fi などの通信を介して操作し，鍵の開閉を可能にするデバイスである．スマートロックに対する中間者攻撃に成功した場合，攻撃者が，正規ユーザによる鍵の開閉を不可能にし，任意に鍵の開閉が可能となる恐れがある．本稿では，アドレス偽造中間者攻撃によって，スマートロックが操作不可能になる事例を述べる．

本稿の構成は以下の通りである． 基礎知識として，2 章では Bluetooth Low Energy，3 章では中間者攻撃について述べる．4 章では，BLE に対する従来の中間者攻撃を紹介し，その限界について述べる．5 章では BLE に対する攻撃手法を提案する．6 章では，BLE アプリケーションに対する攻撃検証を行う．最後に 7 章では，まとめと今後の課題について述べる．

2. Bluetooth Low Energy

Bluetooth Low Energy（BLE）は，近距離無線通信規格である Bluetooth の一部であり，Bluetooth 4.0 より追加された方式である．従来からの方式である Bluetooth Classic に比べて，低消費電力・低コストを目的として開発された．このため，短時間で容量の小さいデータを扱う場合に適しており，IoT デバイスに多く用いられる [9]．なお，BLE と Bluetooth Classic に互換性はない．

2.1 Bluetooth アドレス

BLE 通信を行う際に，デバイスを識別するためのアドレスとして，48 ビットの Bluetooth アドレスが用いられる．Bluetooth アドレスは，次の 2 つのタイプがある．

Public Address

図 1 のように，上位 24 ビットの企業識別番号と，下位 24 ビットの個体識別番号から構成されるアドレスである．企業識別番号は，IEEE への登録が必要となる [7]．

Random Static Address

図 2 のように，上位 46 ビットのランダム値と，下位 2 ビットの 11 から構成されるアドレスである．ランダム値の部分は，デバイスの起動時に変更される．アドレス取得にかかる費用を抑えるため，Public Address に代わって用いられる場合がある．

Public Address もしくは Random Static Address を，デバイスの真のアドレス Identity Address （IA）と呼ぶ．BLE では，プライバシー保護のため，Random Address と呼ばれるアドレスを用いることで，IA を秘匿することができる．これにより，悪意のある第三者からの IA によるデバイス追跡を困難にする．

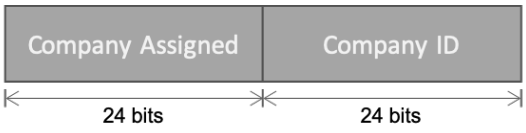


図 1 Public Address のフォーマット
Fig. 1 Format of Public Address

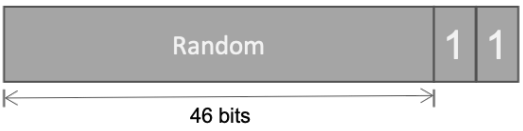


図 2 Random Static Address のフォーマット
Fig. 2 Format of Random Static Address

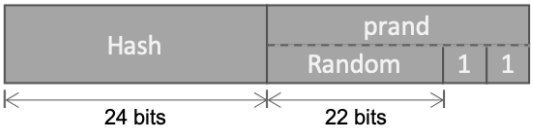


図 3 Resolvable Private Address のフォーマット
Fig. 3 Format of Resolvable Private Address

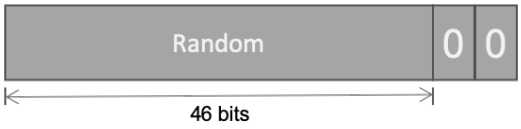


図 4 Non-Resolvable Private Address のフォーマット
Fig. 4 Format of Public Address

Random Address には，次の 2 つのタイプがある．

Resolvable Private Address (RPA)

下位 24 ビットがランダム値（prand）で，上位 24 ビットに prand をハッシュ化して 24 ビットに切り詰めたものが入る．Bluetooth Core Specifications[5] によると，prand は 15 分毎に変更することが推奨され，そのたびに RPA は更新される．prand をハッシュ化する際，Identity Resolving Key （IRK） と呼ばれる 128 ビットの鍵が使用される．IRK は，後述する Bonding 時に相手デバイスによって保存される．IRK を知るデバイスだけが，RPA を解決して IA を得て，アドレス更新後も同一デバイスであると判断することができる．

Non-Resolvable Private Address

このアドレスは，定期的に変化するものの，解決して IA を得ることはできない．そのため，アドレス更新の前後で同一デバイスと判断することはできない．

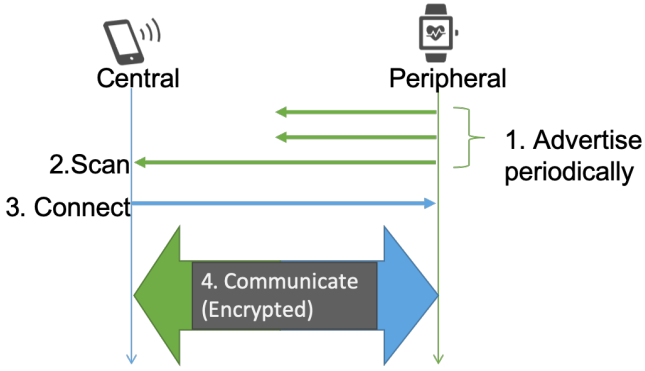


図 5　BLE における接続までの流れ
Fig. 5　BLE Connection Flow

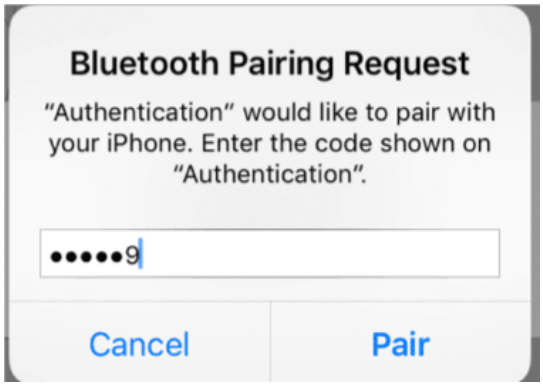


図 6　Passkey Entry の入力画面
Fig. 6　Passkey Entry Input Screen

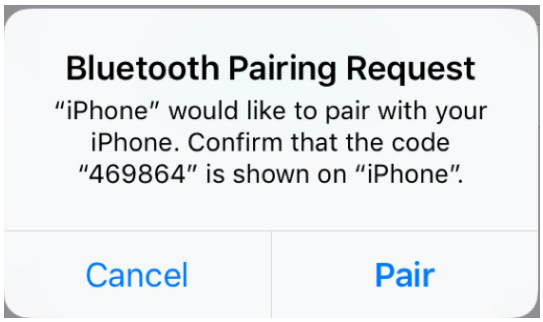


図 7　Numeric Comparison の確認画面
Fig. 7　Numeric Comparison Confirmation Screen

2.2　BLE 通信の手順

BLE におけるデバイス接続までの流れを**図 5** に示す．BLE で通信を行うデバイスは，Peripheral か Central どちらかの役割を担う．

Peripheral

Peripheral は，1.）自身の提供するサービスを周囲の Central にブロードキャスト（アドバタイズ）し，Central からの接続を待つ．

通常，ワイヤレスキーボードやスマートロックがこの役割を担う．

Central

Central は，2.）Peripheral のアドバタイズをスキャンしてアドレスやサービスを読み取り，目的の Peripheral である場合，3.）接続を行う．

通常，PC やスマートフォンがこの役割を担う．

この手順を行うことにより，4.）通信が開始される．また，暗号化通信を行う場合には，次の Pairing による認証が行われる．

2.3　Pairing

Pairing は BLE で暗号化通信を行う際の認証である．Pairing を行おうとする 2 つのデバイスは，まず，それぞれが備えている入出力装置の情報を交換する．交換した情報をもとに，次の 4 つの方式から，実行可能なものを選択する．

Passkey Entry

Pairing を行うとする 2 つのデバイスのうち，片方が入力装置を，他方が出力装置を備えている場合に使用される．この方式では，入力装置を備えたデバイスに表示された 6 桁の数字を，**図 6** のように，出力装置を備えたデバイス側で入力することにより，認証が行われる．この 6 桁の数字をもとに，128 ビット暗号化鍵 Long Term Key （LTK）が作成される．

Numeric Comparison

Bluetooth 4.2 より導入された方式で，Pairing を行うとする 2 つのデバイスのうち，少なくとも片方が入力装置，両方が出力装置を備えている場合に使用される．この方式では，2 つのデバイスに出力された 6 桁の数字が一致していることを確認して，問題がなければ，**図 7** のように，入力装置を持つデバイスが，確認ボタンを押すことにより認証が行われる．この 6 桁の数字をもとに，暗号化鍵が作成される．

Out of Band

USB や NFC などの別通信手段を用いた認証を行う．

Just Works

Pairing を行うとする 2 つのデバイスのうち，片方が入出力装置を持たない場合に使用される．この方式では認証機能を伴わず，Passkey Entry における，数字が 000000 の場合と同様の処理となる．

次回以降の Pairing を省略するために，次の Bonding によって，暗号化鍵 LTK の保存が可能である．

2.4　Bonding

Bonding をすることで，Pairing によって作成された暗号化鍵 LTK を保存し，次回以降の Pairing を省略することができる．また，真の Bluetooth アドレスを秘匿し，追跡から守るためのアドレスである Resolvable Private Address を解決するための鍵 IRK も保存することができる．そのため，BLE デバイスのアドレスが更新されても，過去に

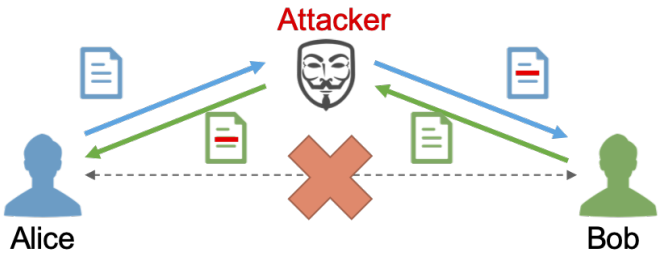


図 8　中間者攻撃の構造
Fig. 8　Architechture of Man-in-the-Middle Attack

Pairing を行った（信用された）デバイスと判断でき，自動接続が可能となる．

3. Bluetooth Low Energy に対する中間者攻撃とその対策

中間者攻撃とは図 **8** のように，攻撃者が，正規通信者両名とそれぞれ独立した通信経路を確立し，通信を自身に中継させることで，データを盗聴および改ざんする攻撃である．この際，攻撃者は正規通信者になりすまして，両名が互いに直接通信をしていると思わせることができる．

BLE では，1 台のデバイスで同時に 2 台のデバイスに接続することができないため，2 台の攻撃用デバイスを用いる．片方の攻撃用デバイスは攻撃対象 Central になりすまし，攻撃対象 Peripheral に接続する．他方の攻撃用デバイスはその逆を行う．2 台の攻撃用デバイス間でのデータのやり取りには双方向通信のプロトコルである WebSocket[4] が用いられる．

中間者攻撃対策として，通信者が本当に意図した相手かどうかを確かめる，認証がある．Bluetooth は独自の認証方式を備えており，片方のデバイスに表示された 6 桁の数字を他方で入力するなどして，認証を行う．

しかし Bluetooth における認証は，通信者両名のデバイスに，ボタンなどの入力装置もしくは，ディスプレイなどの出力装置を必要とする．そのため，入出力装置をもたないデバイスは認証をすることができず，中間者攻撃が容易に可能となる．

4. 従来の中間者攻撃とその限界

従来の BLE に対する中間者攻撃として，GATTacker [2] がある．GATTacker は，BLE に対する中間者攻撃の実装であり，Node.js のパッケージとして開発された [6]．

GATTacker で攻撃対象となる Peripheral のアドレスを指定することで，その Peripheral のアドバタイズパケットをコピーして，攻撃用デバイスでも同じアドバタイズを行う．これにより，攻撃対象 Peripheral になりすまし，攻撃対象 Central が自身に接続してくるのを待つ．攻撃対象 Central が接続してきた場合，中間者攻撃の準備が整い，攻撃対象 2 台のデバイス間のデータを，攻撃者が盗聴および改ざんして送信などが可能となる．

GATTacker による攻撃は，攻撃対象となるデバイスが Bonding している場合には成立しない．これは，RPA の解決による IA を用いた接続が行われることと，初回 Pairing 時に作成された暗号化鍵 LTK を再利用した暗号化通信が行われるためである．BLE デバイスは，利便性のために，Bonding を行って，Central から Peripheral に自動接続できるようにする場合が多く，そのような場合は GATTacker による攻撃は不可能となる．

5. アドレス偽造中間者攻撃

関連研究による BLE に対する中間者攻撃は，攻撃対象デバイス同士が Bonding している場合には成立しない．BLE デバイスを利用する際は，利便性のため，Bonding を行って自動接続することが多い．自動接続する場合は，予め決められたアドレスに対して接続するようになっているため，そのアドレスと異なる攻撃用デバイスを準備しても，攻撃対象が接続してくることはない．

本章では，Bonding を行っている自動接続するデバイスにおいても，ある条件下において，中間者攻撃が成立する攻撃手法について述べる．

5.1 アドレス偽造

コンピュータに搭載されている Bluetooth アダプタには，予め Bluetooth アドレスが割り当てられているが，このアドレスは任意に変更することができる．本研究では，hcitool[8] と呼ばれるツールを用いて，攻撃用デバイスの Bluetooth アドレスを指定したアドレスに変更している．アドバタイズパケットのコピーに加え，アドレス偽造を組み合わせることで，より高いレベルで攻撃対象 Peripheral になりすますことができる．

5.2 攻撃成立条件

攻撃対象デバイス同士が Bonding している状態で，アドレス偽造を行って攻撃が成立するための条件は 2 つある．

1 つ目は，2 章で述べた，攻撃対象 Peripheral の RPA と IA が一致することである．通常，RPA は IA を秘匿するために用いられるランダム値をもとにしたアドレスであり，図 **9** のように，RPA と IA は一致しない．しかし，BLE デバイスには，製作コストなどの理由から，図 **10** のように，RPA と IA が一致するものが存在する．また，そのようなデバイスは，RPA が定期的に更新されることもない．

2 つ目は，攻撃対象 Central が，攻撃対象 Peripheral と Bonding して，いるのにも関わらず，アドレス偽造した攻撃用 Peripheral と平文通信を行うことである．通常，Bonding したデバイスとは，保存された暗号化鍵 LTK を用いた暗号化通信を行う．しかし，アドレス偽造した攻撃

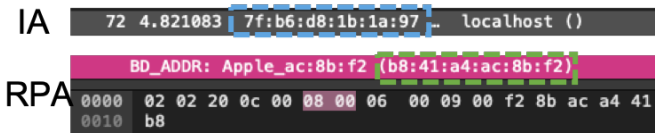


図 9　RPA と IA が不一致
Fig. 9　RPA NOT matching with IA

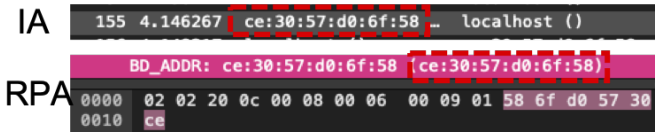


図 10　RPA と IA が一致
Fig. 10　RPA matching with IA

用デバイスのように，Bonding したデバイスとは異なるが，アドレスが一致する場合，暗号化鍵 LTK を用いた暗号化通信を行わないものが存在する．

5.3　攻撃シナリオ

提案手法を用いた攻撃シナリオとして，まず，攻撃成立条件 1 である，RPA が IA と一致する Peripheral を探し出す．これは，流通している BLE デバイスの様々な機種を購入して，そのデバイスと Bonding し，RPA と IA を比較することで達成できる．そのようなデバイスを見つけた場合，同じ機種のデバイスでも同様に RPA と IA が一致すると考えられる．

次に，RPA と IA が一致するデバイスのアドバタイズパケットを解析する．これにより，アドバタイズパケットの機種共通のデータを得る．

最後に，アドバタイズパケットの機種共通データをもとに，町中などで稼働している同じ機種のデバイスを探索する．そのようなデバイスが見つかった場合，その付近で，アドレス偽造中間者攻撃を実行し，ユーザの接続を待つ．もし，ユーザが，攻撃成立条件 2 に該当する BLE デバイスを使用していた場合，アドレス偽造中間者攻撃が成立することとなる．

6.　Bluetooth Low Energy アプリケーションに対する攻撃

本章では，アドレス偽装中間者攻撃による実例をあげる．

6.1　実験環境

攻撃対象 Peripheral として，商用化されているスマートロックの一製品を対象とする．なお，攻撃対象における RPA は IA と一致しており，5.2 節で述べた攻撃成立条件 1 を満たしている．

攻撃対象 Central として iPhone 8 （iOS 13.1.3）（以下 iPhone）を用いる．iPhone は，5.2 節で述べた攻撃成立条

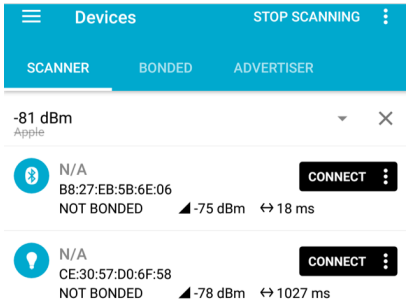


図 11　アドバタイズの確認（従来の攻撃時）
Fig. 11　Advertising (under attack by the existing way)

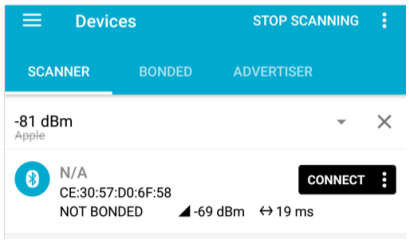


図 12　アドバタイズの確認（アドレス偽装した場合）
Fig. 12　Advertising (under attack by the proposal way)

件 2 を満たすことを確認している．iPhone には，スマートロック操作用アプリをインストールしており，スマートロックと事前に Bonding している．iPhone で操作用アプリを開くと，鍵の開閉を行う画面が表れる．

攻撃用デバイスとして，2 台の Raspberry Pi 3 Model B+[3] を用いる．この Raspberry Pi モデルは，Bluetooth 4.2 に対応したアダプタを搭載している．

6.2　修正された中間者攻撃の適用とその効果

まず，中間者攻撃ツール GATTacker をそのまま用いた実験を行った．GATTacker を起動してアドバタイズを確認したところ，**図 11** に示すように，アドレスの異なるパケットが送信されていることが確認された．この状態で iPhone のスマートロック操作用アプリを起動すると，攻撃用デバイスではなく，スマートロックに接続され，攻撃は成立しなかった．

次に，攻撃用デバイスのアドレスを，スマートロックのものに設定した状態で，GATTacker を用いた．アドバタイズを確認すると，**図 12** のように，2 つあったアドバタイズが 1 つになっていることを確認した．この状態で iPhone のスマートロック操作用アプリを起動すると，攻撃用デバイスに接続された後，通常時とは異なる内容が表示され，スマートロックの操作が不可能となる DoS 攻撃が成立した．

6.3　原因の分析

修正された中間者攻撃によって，6.2 節で述べた DoS 攻撃が成立する原因は，5.2 節でも述べたとおり，スマートロックの RPA と IA が一致していること，iPhone とスマー

トロックが Bonding しているのにも関わらず，iPhone が攻撃用デバイスと平文通信を行ってしまうことである．

本来，RPA は IA を秘匿するために用いられるアドレスであり，RPA と IA が一致していては，その意味をなさない．しかし，BLE デバイス製作時のコスト削減のため，RPA を用いるための処理が適切に行われておらず，RPA と IA が一致していると考えられる．

また，iPhone とスマートロックが Bonding している場合，iPhone が，RPA を解決するための鍵 IRK から得たスマートロックの IA 宛に，初回 Pairing 時に作成した暗号化鍵 LTK を用いて，暗号化通信を行わなければ，Bonding の意味をなさない．この iPhone の動作は，スマートロック操作用アプリか，iOS の不具合だと考えられる．iOS の不具合である場合，このスマートロック製品のみならず，他の BLE デバイスにおいても，同様の脆弱性が起こり得る．

6.4 対策の検討

修正された中間者攻撃の対策は，BLE デバイスの RPA と IA を一致させないこと，もしくは，Bonding しているアドレスを偽造したデバイスとの通信時に，平文通信を行わないことである．後者に関しては，今後，脆弱性の原因を解明およびベンダーへの報告をし，不具合の修正につなげたいと考えている．

6.5 さらなる被害の可能性

今回の攻撃では，6.2 節で述べたとおり，スマートロックが操作不可能になる DoS 攻撃となったが，それ以上の被害をもたらす攻撃も考えられる．例えば，iPhone からスマートロックに送信されている BLE パケットを解析し，スマートロックの鍵開閉に必要な情報を得られた場合，攻撃者によって任意に鍵開閉が可能となる．もしくは，スマートロック操作用アプリを解析し，iPhone からスマートロックに充てられた鍵を閉めるためのパケットを遮断し，予め攻撃者が準備した，鍵が閉まったことを示すパケットを iPhone に送信すれば，ユーザに問題なく鍵が閉まったと思わせることも可能となる．

7. まとめ

本稿では，BLE に対する攻撃手法として，アドレス偽造中間者攻撃を提案した．この手法により，従来の中間者攻撃では成立しない場合であっても，攻撃が可能となる．その効果の検証として，実際に，スマートロックに対する中間者攻撃実験を行った．その結果，従来の中間者攻撃では攻撃が成立しなかったが，提案手法では，中間者攻撃が成立し，スマートロックの操作ができなくなるという DoS 攻撃に繋がることを示した．

今後，提案手法による攻撃で，DoS 攻撃以上の被害の可能性の検証と，その対策方法を考案する．

謝辞 本研究は JSPS 科研費 20K11810 の助成を受けたものです．

参考文献

[1] Bluetooth SIG, Inc., “Bluetooth market update 2020,” https://www.bluetooth.com/bluetooth-resources/2020-bmu/, 参照 2020-07-16.
[2] Jasek, S., GATTacking Bluetooth Smart devices, Black-Hat USA, 2016
[3] Buy a Raspberry Pi 3 Model B+ Raspberry Pi, https://www.raspberrypi.org/products/raspberry-pi-3-model-b-plus/, 参照 2020-08-19.
[4] Fette, I. and Melnikov, A., The WebSocket Protocol. Internet Engineering Task Force, RFC 6455, 2011, https://tools.ietf.org/html/rfc6455, 参照 2020-08-19.
[5] Core Specifications — Bluetooth Technology Website, https://www.bluetooth.com/specifications/bluetooth-core-specification/, 参照 2020-08-19
[6] gattacker - npm, https://www.npmjs.com/package/gattacker, 参照 2020-08-19
[7] IEEE SA - Registration Authority, https://standards.ieee.org/products-services/regauth/index.html, 参照 2020-08-19
[8] hcitool(1): configure Bluetooth connections - Linux man page, https://linux.die.net/man/1/hcitool, 参照 2020-08-19
[9] The Difference Between Classic Bluetooth and Bluetooth Low Energy, https://blog.nordicsemi.com/getconnected/the-difference-between-classic-\\bluetooth-and-bluetooth-low-energy, 参照 2020-08-20