Vol.2018-CSEC-83 No.4
2018/12/13

LoRaWANの脆弱性の実証とDoS攻撃の提案

壇 慶人[1,a)]　瀧田 愼[1]　仲野 有登[2]　清本 晋作[2]　森井 昌克[1]

概要：様々なモノがインターネットにつながるIoT（Internet of Things）において，一度のバッテリー交換で長期間稼働するデバイスを実現できれば，管理にかかる人的コストや労働負担を削減できる．デバイスの消費電力を抑えるために，低電力かつ長距離通信可能な通信方式（LPWA：Low Power Wide Area）が提案されている．LPWAを実用化する上ではLPWAを用いた通信の安全性を十分に評価する必要がある．本稿では，LPWAの一つであるLoRaWANを扱い，指摘されている脆弱性を実環境で検証し，その結果を利用してLoRaWANに対する新たな攻撃を提案する．まずLoRaWANに対するリプレイ攻撃を実環境で検証する．さらに，リプレイ攻撃で取得したパケットに含まれるLoRaのカウンタ値を容易に改ざんできることを明らかにし，アプリケーションサーバのカウンタ値を引き上げる攻撃を提案する．提案攻撃により，アプリケーションサーバは引き上げたカウンタ値より小さいカウンタ値を持つパケットの受付が不可能となり，DoS（Denial of Service）状態が長期間継続される．

キーワード：LoRaWAN，LPWA，Dos攻撃，リプレイ攻撃，IoT

1. はじめに

インターネット技術や各種センサの技術が進歩し，パソコンやスマートフォンだけでなく，家電や自動車，ビルや工場など，様々なモノがインターネットにつながるIoT（Internet of Things）時代が到来している[1]．IoT時代では多様なアプリケーションの通信ニーズに対応することが求められている．例えば，北海道石狩市ではLoRaを活用した社会インフラシステムの運用を開始している[2]．

IoTの普及により，各種センサで取得したデータを遠く離れた環境からリアルタイムで把握することが容易になった．一方で，センサなどの多数設置されるIoTデバイスは，安定した電源が確保できる場所に設置できるとは限らない．そこで，LPWA（Low Power Wide Area）と呼ばれるIoT向けの無線通信技術の研究開発が進められている．LPWAの通信速度は携帯電話システムとして用いられるセルラ方式と比較して低速ではあるが，一般的な電池で数年以上運用可能な省電力性や，数kmから数十kmもの通信が可能な広域性を有している[1]．

代表的なLPWAの規格として，LTEベースの規格，LoRaWAN[8]，Sigfox[3]がある[4], [5]．LTEベースの規格は，通信事業者が全国でサービスを提供し，通信事業者がデバイスを販売することを前提としており，LPWAの中でも比較的ハイスペックな用途を対象としている．LoRaWANやSigfoxは免許不要で利用可能な周波数帯（日本では920MHz帯）を使用しているため，サービス提供者がエンドデバイスやゲートウェイなどの機器を自由に設置・提供する．特に，LoRaWANは個人でエンドデバイスを購入することが可能であり，山間部や沿岸部などのLTEベースの規格でサービスが提供されにくい地域への活用が期待される．

IoTを活用したサービスが普及する一方で，IoT機器は，管理が行き届きにくいこと，ウイルス駆除ソフトのインストールなどの対策が難しいことなどの理由から，サイバー攻撃の脅威にさらされることが多く，その対策強化の必要性が指摘されている[6]．LPWAにおいては，省電力化，広範囲化，また利便性の確保のために，セキュリティ対策が犠牲になっている場合がある．実際に国内外で注目され，利用が進められているLoRaWANにおいても，多数の脆弱性及びそれを用いた攻撃の危険性が多く指摘されている[11], [12]．LPWAを実用化する上で，その通信の安全性を十分に評価することが求められている．

本稿では，代表的なLPWAの一つであるLoRaWANの安全性について議論する．LoRaWANはSemtech社によって開発されたLoRa変調を物理層の規格として用いている[7]．LoRaWANの仕様は非営利団体であるLoRa Allianceが標準化を推進している[8]．標準化を進める中で複数の脆弱性

[1] 神戸大学大学院工学研究科
Graduate School of Engineering, Kobe University
[2] KDDI 総合研究所
KDDI Research, Inc.
[a)] dan@stu.kobe-u.ac.jp

が指摘され，対策が進められている．LoRaWAN v1.0 に対して，文献 [11] では，LoRaWAN のネットワークにエンドデバイスを参加する際の脆弱性を利用したリプレイ攻撃が提案されている．文献 [12] では，LoRaWAN で用いられる暗号化の脆弱性を利用したビットフリッピング攻撃が提案されている．2018 年 11 月現在では，LoRaWAN v1.1[13] が最新の仕様であるが，エンドデバイスのバージョンアップが進んでおらず，v1.0.2 に基づいたデバイスが用いられている．

本稿では LoRaWAN v1.0.2 に基づくデバイスを用いて，LoRaWAN に対して指摘されている脆弱性を実環境で検証する．さらに，その結果を利用して LoRaWAN に対する新たな攻撃を提案する．まず，研究室内に LoRaWAN のネットワーク環境を構築し，正常に動作することを確認する．ネットワーク上に流れるメッセージを盗聴，取得し，ある条件のもとでそのメッセージを再送信することで，アプリケーションを提供するサーバを DoS （Denial of Service）状態にするリプレイ攻撃 [11] を実際に行い，成功することを確認した．また，別の脆弱性を利用して，リプレイ攻撃の条件を緩和し，DoS 状態を長期間継続させる攻撃を提案する．提案攻撃は，攻撃者の任意のタイミングで DoS 状態を引き起こすことが可能であり，必要なデータが長期間入手できないなどの問題を引き起こす可能性がある．

なお本稿で公開する脆弱性及びそれを用いた攻撃について，対応とともに LoRaWAN の規格団体である LoRa Alliance[8] に報告を済ませている．

2. LoRaWAN

本章では LoRaWAN v1.0.2 の仕様，特に暗号化に関する部分について概説する．

2.1 LoRa と LoRaWAN

LoRa は，チャープ拡散技術を改良した LoRa 変調を物理層の規格として用いている [7]．チャープ拡散は Semtech 社が開発した変調方式でスペクトル拡散方式の一つで，出力電圧を抑えて周波数を増加または減少させながら通信することで干渉に耐性をもたせている．LoRa では，拡散率（Spreading Factor）と呼ばれるパラメータで，どの程度信号を拡散させて，雑音耐性を高めるかを調節している．拡散率が上げると，伝送距離と雑音耐性が大きくなるが，伝送速度が小さくなる．

LoRa の上で動作する MAC 層プロトコル LoRaWAN の仕様は，LoRa Alliance[8] により定められている．LoRaWAN は IoT （Internet of Things）向けの無線技術である LPWA （Low Power Wide Area）の一つとして国内外で注目されている無線技術である [1]．IoT では携帯電話を中心に用いられているセルラ方式と同等かそれ以上の距離で通信可能であり，管理コスト削減のために一度のバッテリー交換で数年間動作し続けることが求められている．LPWA は文字通り低消費電力かつ広範囲で通信が可能な通信方式であり，その規格は上記の要件を満たすように設定されている．LoRaWAN では用途に応じてクラス A から C まで 3 種類の方式が定められている．どの方式も図 1 のように，エンドデバイス，ゲートウェイ，ネットワークサーバ，アプリケーションサーバで構成されるネットワークモデルで考えることができる．

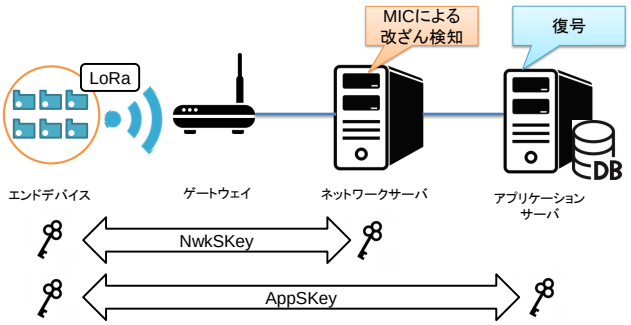

図 1 ネットワークモデル
Fig. 1 Network model

LoRaWAN は免許が必要ない周波数帯を利用しているため，個人が LoRa の通信モジュールを購入して LoRaWAN のネットワークを自由に構築できる．ネットワークサーバやアプリケーションサーバはモジュールを含めた商用サービスが提供されている．また，LoRa Server project[9] では，個人でネットワークサーバやアプリケーションサーバを構築できるように，オープンソースプロジェクトを展開している．ネットワークサーバやアプリケーションサーバを個人で構築する場合，LoRaWAN の仕様上だけでなく，実装方法による脆弱性が含まれる可能性がある．

2.2 LoRaWAN における暗号化

LoRaWAN では，暗号化プロトコルに AES-128[10] を採用している．暗号鍵は，アプリケーションキー（AppKey），ネットワークセッションキー（NwkSKey），アプリケーションセッションキー（AppSKey）の三種類があり，AppKey と AppSKey はエンドデバイスとアプリケーションサーバが共有しており，NwkSKey はエンドデバイスとネットワークサーバが共有している．エンドデバイスが LoRaWAN ネットワークに参加する際にはこれらの鍵を生成，共有するための Key Activation を実行する必要がある．その方法として，ABP （Activation By Personalization）と OTAA （Over The Air Activation）が用意されている．ABP は工場出荷時に予め二つの鍵をエンドデバイスに格納しておき，それを変更せずに使い続ける方式である．ネットワークの状態に依らず容易に接続できるが，デバイスを再起動したとしても二つの鍵は変更されないため，長期間使い続けると鍵が漏洩するなどセキュリティ上の問題が起こりや

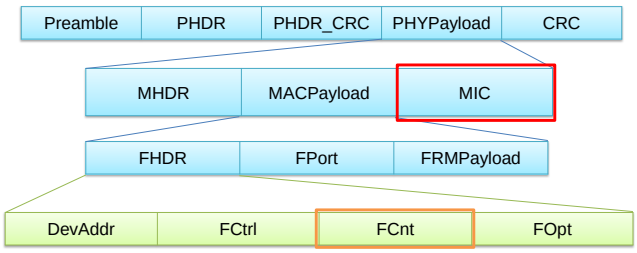

図 2　メッセージフォーマット
Fig. 2　Massage format

すい．OTAA は予め AppKey を共有しておき，それとデバイス情報などの追加の情報を用いて，セッションの開始時に新しい AppSKey と NwkSKey を共有する方式である．ネットワークへの参加にかかる時間はゲートウェイからの応答に依存するが，デバイスを再起動することでセッションキーを更新できるため，セキュリティを強化できる．

OTAA などの方法で，ネットワークに参加した後，エンドデバイスは LoRaWAN のプロトコルに従い，ゲートウェイにメッセージを送信する．メッセージにはアップリンクメッセージとダウンリンクメッセージの二種類があり，前者はエンドデバイスによりゲートウェイ経由でアプリケーションサーバに送信される．図 2 は LoRaWAN のメッセージフォーマットである．メッセージは，プリアンブル，物理層ヘッダ，ヘッダ CRC，物理層ペイロード，メッセージ全体の完全性を保護するための CRC で構成される．物理層ペイロードには，MAC 層ヘッダ，MAC ペイロード，メッセージ完全性コード（MIC）が含まれる．ここで，MIC の値の導出には NwkSKey が用いられ，メッセージがネットワークサーバに到達したときに MIC のチェックが行われる．さらに，MAC ペイロードには，フレームヘッダ，フレームポート，フレームペイロードが含まれている．LoRaWAN で送信したいデータはフレームペイロードに格納されており，AppSKey を用いて暗号化される．メッセージがアプリケーションサーバに到着したら，共有している AppSKey を用いてフレームペイロードを復号し，データを得る．

3. LoRaWAN の脆弱性

LoRaWAN には複数の脆弱性が指摘されており，それを利用した攻撃が提案されている [11], [12]．文献 [11] では，エンドデバイスに対する物理的な攻撃，ジャミング攻撃，リプレイ攻撃などが提案されている．文献 [12] では，鍵管理の脆弱性を利用したビットフリッピング攻撃や鍵生成の脆弱性を提案，指摘している．

リプレイ攻撃はセキュリティプロトコルに対する攻撃であり，悪意のあるエンティティが有効なデータ送信を再送信もしくは繰り返す攻撃である．LoRaWAN では，そのデータが暗号化されているため，エンドデバイスとゲートウェイ間を流れるメッセージを取得したとしても，AppSKey なしではデータを復号することはできない．また，データを改ざんすると MIC チェックが失敗するため，NwkSKey なしではデータを改ざんできない．さらに，正規のメッセージを連続して再送信したとしても，フレームカウンタ（FCnt）を用いてそれを検知することができる．メッセージに含まれる FCnt は，エンドデバイスがメッセージを送信するごとにインクリメントされる．サーバは前回受け取ったメッセージの FCnt を記憶しておき，その値より大きい FCnt を持つメッセージのみを正規のメッセージとして受け取る．それ以外の場合はそのメッセージを破棄する．しかしながら，ABP による Key Activation を使用してネットワークに参加するデバイスに対しては，リプレイ攻撃の危険性がある．

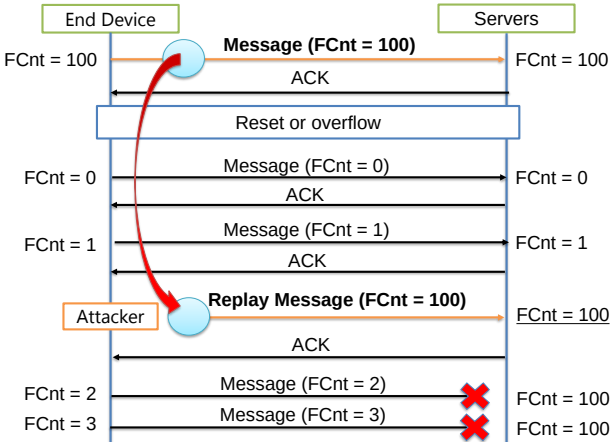

図 3　LoRaWAN におけるリプレイ攻撃
Fig. 3　Replay attack in LoRaWAN

FCnt はエンドデバイスが再起動されたとき，あるいは，カウンタがオーバーフローしたときに 0 にリセットされる．そして，ABP ではエンドデバイスが再起動されたとしても，AppSKey 及び NwkSKey が変更されない．そのため，再起動前に送信されたメッセージは，再起動後に再送信したとしても MIC が正しいメッセージとなる．そして，その FCnt がサーバに記録された値よりも大きければ正規のメッセージとして受理される．そこで，攻撃者はエンドデバイスが送信したメッセージを取得しておき，カウンタ値のリセットを待ってそれを再送信することで，サーバに記録されるカウンタ値を意図的に大きい値に変更できる．正規のメッセージの FCnt が，攻撃者が送信したメッセージの FCnt よりも小さい間は，そのメッセージがアプリケーションサーバに届いたとしても破棄され続ける．図 3 はリプレイ攻撃のシナリオを図示したものである．

OTAA を利用する場合，カウンタ値が 0 にリセットされるとき，すなわちセッションが再度確立される度に鍵が更新される．そのため，セッションの再確立後に再送信すると，NwkSKey が変更されているため MIC の値が一致しな

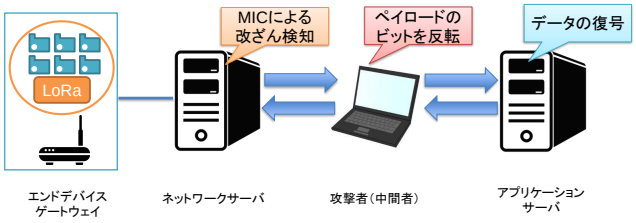

図 4　LoRaWAN におけるビットフリッピング攻撃
Fig. 4　Bit-flipping attack in LoRaWAN

い．したがって，ネットワークサーバでの MIC のチェックにより検知され，受理されることはない．

ビットフリッピング攻撃は，共通鍵暗号の CTR モードの脆弱性を利用した攻撃である．LoRaWAN では AES128 を CTR モードで利用しているため，この攻撃が実行される可能性がある．CTR モードでは，セッションキーから生成される鍵ストリームと平文の単純な XOR により暗号文が生成される．つまり，暗号文をビット反転すると，平文の対応するビットを反転させることができる．ビットフリッピング攻撃は任意のデータに改ざんすることはできないが，本来のデータとは異なるデータをアプリケーションサーバに復号させることができる．ただし，エンドデバイスとネットワークサーバ間でビットフリッピング攻撃をする場合，メッセージの改ざんが MIC により検知される．LoRaWAN において，ビットフリッピング攻撃を行う場合は，ネットワークサーバでの MIC のチェックを通過した後に，メッセージの改ざんを行う必要がある．図 4 はビットフリッピング攻撃の流れを図示したものである．

4. リプレイ攻撃の実証実験

本章では前章で概説したリプレイ攻撃 [11] を実装し，実際に攻撃が成功することを確認する．環境構築に使用した LoRaWAN プロトコルとアクティベーションは下記のとおりである．デバイスとゲートウェイは市販されているものを用いる．ネットワークサーバとアプリケーションサーバはクラウドサービスを利用する．本稿は脆弱性を実証するものであり，実験に用いた機器，サービスの実名を表記しないことが望ましいと判断している．

- アクティベーション: ABP
- LoRaWAN プロトコル: LoRaWAN v1.0.2

図 1 に対応するように LoRaWAN ネットワークを設計した．エンドデバイスとゲートウェイは LoRa により無線通信し，ゲートウェイとアプリケーションサーバ間は有線 LAN で通信する．

本実験では次のような能力を持つ攻撃者を仮定する．

- ゲートウェイとネットワークサーバ間のメッセージを盗聴でき，そのメッセージを取得できる．
- 取得したメッセージをアプリケーションサーバに対して，任意のタイミングで再送信できる．
- エンドデバイスを任意のタイミングで再起動できる．

本実験では次の手順でリプレイ攻撃の検証実験を行った．正規のエンドデバイスを LoRaWAN に参加させ，セッションを確立させる．攻撃用端末で，ゲートウェイとネットワークサーバ間のメッセージを盗聴し，取得する．その後，エンドデバイスを再起動しセッションを再確立させる．そして，攻撃用端末で取得したメッセージをネットワークサーバに対して送信する．

ABP による Key Activation が行われている場合，NwkSKey と AppSKey はデバイスの再起動の前後で変更されない．そのため，再起動前に取得したメッセージの MIC は，取得後に再送信したとしても正しいものであり，再送信したメッセージはネットワークサーバにおける MIC チェックを通過した．そして，アプリケーションサーバにおいても，再送信したメッセージは正規のメッセージとして受理され，サーバ内のカウント値が更新された．その後，正規のエンドデバイスが新たにメッセージを送信したとしても，FCnt がサーバのカウント値よりも小さい場合はそのメッセージが受理されることはなく，サーバは DoS 状態になった．

文献 [11] では，リプレイ攻撃により，メッセージを再送信するために，カウンタ値（FCnt）のオーバーフロー，あるいはエンドデバイスの再起動を待つ必要があると説明している．カウンタ値は 16 ビットであり，カウンタ値がオーバフローするためには 2^{16} 回メッセージが送られる必要がある．一般社団法人電波産業会 (ARIB)[14] が定める電波利用に関する規定の中で運用する場合，最小でも 4.4 秒の送信間隔が必要となり，カウンタ値のオーバーフローを待つためには，約 80 時間必要となる．そのため，LoRaWAN に対するリプレイ攻撃を実行する場合，攻撃者はエンドデバイスを再起動できることが現実的である．また，このリプレイ攻撃は ABP による Key Activation を前提としており，OTAA により Key Activation が実行された場合は攻撃に成功しない．

5. フレームカウンタの改ざんによる DoS 攻撃の提案と検証

本稿では，異なる脆弱性を利用した DoS 攻撃を提案する．本章では，アプリケーションサーバで MIC チェックが行われないというセキュリティ上の問題を利用して，フレームカウンタ（FCnt）を任意の値に改ざんする攻撃を提案する．

5.1 FCnt の改ざん

LoRaWAN ネットワークではネットワークサーバのみで MIC によるメッセージの改ざん検知が行われる．そのため，ネットワークサーバからアプリケーションサーバに送信されるメッセージが改ざんされたとしても，アプリケー

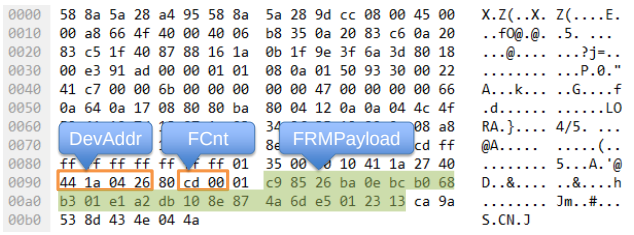

図 5　LoRaWAN におけるメッセージの例
Fig. 5　An example of message in LoRaWAN

ションサーバは改ざんされたメッセージを受理してしまう．また，FCnt は LoRaWAN ネットワークにおいて暗号化されていないため，メッセージフォーマットを知っていれば，盗聴したメッセージの FCnt を容易に知ることができる．したがって，ネットワークサーバとアプリケーションサーバ間に侵入することで，FCnt を任意の値に改ざんできる．図 5 は，LoRaWAN 上に流れるメッセージの一例であり，送信元を表す DevAddr やフレームカウントである FCnt は暗号化されておらず，データである FRMPayload は暗号化されている．

5.2　提案攻撃とその成立条件

本稿では FCnt の改ざんによる DoS 攻撃を提案する．攻撃対象のネットワークは，ネットワークサーバとアプリケーションサーバは有線あるいは無線により接続され，攻撃者がサーバ間に中間者として介入可能なネットワークであると仮定する．

攻撃は次の流れで実行する．まず，ネットワークサーバとアプリケーションサーバの間に中間者として侵入する．つまり，ネットワークサーバから送信されたメッセージは，攻撃用端末で中継されてアプリケーションサーバに送信される．そして，中継時に，そのフレームカウンタ値を大きな値に改ざんする．メッセージフォーマットは既知であり，フレームカウンタは暗号化されていないため，容易に改ざんを実行できる．

提案攻撃は攻撃者の任意のタイミングで実行可能であり，4 章のリプレイ攻撃のようにカウンタのリセットを想定する必要がない．また，ネットワークサーバによる MIC チェックを通過した後に，メッセージを改ざんするため，アプリケーションサーバで改ざんが検知されることはない．

5.3　検証実験と考察

検証環境は下記のとおりである．デバイス，ゲートウェイはリプレイ攻撃の実証実験で用いたものと同一である．

- アクティベーション：ABP
- LoRaWAN プロトコル：LoRaWAN v1.0.2
- ネットワークサーバ：LoRa Server [9]
- アプリケーションサーバ：LoRa App Server [9]
- 中間者攻撃ツール：Ettercap [15]

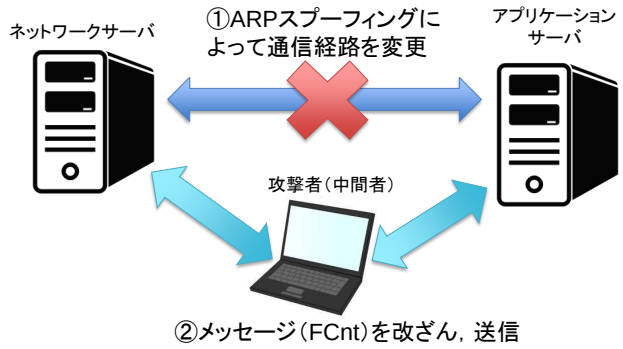

図 6　攻撃シナリオ
Fig. 6　Attack scenario

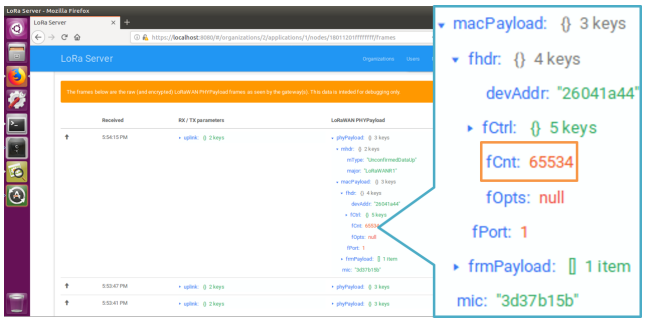

図 7　実験結果
Fig. 7　Result of experiment

4 章の実験ではネットワークサーバとアプリケーションサーバとしてクラウドサービスを利用したが，本章の実験では Lora Server project[9] がオープンソースで提供しているソフトウェアを用いて，ローカル環境にネットワークサーバとアプリケーションサーバを構築した．

図 6 に攻撃のシナリオを図示する．攻撃者は ARP スプーフィングによって二つのサーバ間の通信に割り込み，メッセージを中継し，その FCnt を改ざんする．ARP スプーフィングには Ettercap を用いた．Ettercap はネットワークに接続し，その内部の通信経路を自身を介するものに変更でき，その途中でメッセージを改ざんできる．攻撃用端末を経由するメッセージをリアルタイムで改ざんするために，予め改ざん方法を記述した設定ファイルを用意する．改ざん方法は，ある文字列を異なる文字列に置き換えるなど単純なものでよい．まず，メッセージを盗聴しその FCnt を把握する．そして，設定ファイルには FCnt+1 を任意の値に置換する処理を記述する．次のメッセージが流れたとき，そのメッセージは設定ファイルに従って処理され，FCnt が改ざんされる．

図 7 は，攻撃を実行した後に，アプリケーションサーバで GUI 表示されたペイロードデータである．カウンタ値を 16 進数 “0001” から “FFFE” に改ざんすることで，アプリケーションサーバでは 10 進数 “65534” と表示されている．つまりアプリケーションサーバが記憶するカウンタ値が “65534” に変更される．その後，正規のデバイスが新

しいメッセージを送信し続けたとしても，そのカウンタ値が “65534”より小さい場合，そのメッセージはアプリケーションサーバで受理されず破棄されることを確認した．

提案攻撃は，4 章のリプレイ攻撃と比較して，Key Activation の方式に依らず実行できる，また，エンドデバイスや FCnt のオーバーフローによるカウンタのリセットを想定する必要はなく，攻撃者の任意のタイミングで実行できる．本実験では，LoRaWAN v1.0.2 を対象としたが，最新の仕様である v1.1 においても，アプリケーションサーバでの改ざん検知は含まれておらず，提案攻撃は有効であると考えられる．

対策としては，ネットワークサーバとアプリケーションサーバをクラウドに設計することが考えられる．またサーバ間の通信のために SSL といった安全なチャネルを用意することも有効である．

なお，現在提供されている LoRaWAN の商用サービスはサーバ間に中間者として侵入することは困難であるため，直ちにサービスへの影響はないと考えられる．今後個人で LoRa デバイスを購入し，ネットワークサーバ，アプリケーションサーバを構築する場合は，本稿で公開した脆弱性及び既存の脆弱性に対して十分対策を取る必要がある．

6. おわりに

IoT 時代において，省電力で広域の通信が可能な LPWA が注目されている．本稿では，代表的な LPWA の規格である LoRaWAN の脆弱性とそれを利用した攻撃を市販されている LoRa モジュールを用いて実際に検証した．ABP による Key Activation を前提としたリプレイ攻撃が成功することを確かめ，その脆弱性が放置されていることの危険性を確認した．また，アプリケーションサーバで MIC チェックが行われないことを利用して，ネットワークサーバとアプリケーションサーバ間で容易に FCnt の改ざんが可能であることを示した．FCnt の改ざんにより，アプリケーションサーバのカウンタ値を任意の値に変更でき，それ以下の FCnt を持つ正規のメッセージを受け付けない状態に移行させることが可能である．その結果，センサデバイスで取得したデータが長期間入手できず，データの活用に支障をきたす恐れがある．

今後 LoRa，LoRaWAN が IoT の普及とともに広まるにあたり，現在の商用サービスだけでなくユーザが独自に環境を設計するケースが増加すると考えられる．LoRaWAN ネットワークを独自で設計する場合は，本稿で公開した脆弱性及び既存の脆弱性に対して十分対策を取る必要がある．

参考文献

[1] 総務省，平成 30 年情報通信白書，2018 年.
[2] さくらインターネット，“LoRa を利用した河川水位計測システムの試行運用開始,” ニュースリリース，2018 年 3 月， https://www.sakura.ad.jp/information/pressreleases/2018/03/30/90212/,（参照 2018-11-13）.
[3] Sigfox, https://www.sigfox.com/en.
[4] 高橋 幹，垣内 勇人，“LPWA（Low Power Wide Area）の規格と技術動向,” 電子情報通信学会誌，Vol.100，No.9，pp.982-986，2017 年 9 月.
[5] 鈴木 一哉，森本 昌治，岩井 孝法，“IoT 技術の最新動向，” 電子情報通信学会 通信ソサイエティマガジン，2018-2019，12 巻，1 号，p.12-20，2018 年 6 月.
[6] IPA 独立行政法人 情報処理推進機構，情報セキュリティ白書 2018，2018 年.
[7] Semtech, “What is Lora”, https://www.semtech.com/lora,（参照 2018-11-13）.
[8] LoRa Alliance, https://lora-alliance.org/.
[9] LoRaServer, “LoRa Server, open-source LoRaWAN network-server”, https://www.loraserver.io/,（参照 2018-11-13）.
[10] AES, https://csrc.nist.gov/publications/detail/fips/197/final,（参照 2018-11-13）.
[11] E. Aras, G. S. Ramachandran, P. Lawrence, and D. Hughes, “Exploring the Security Vulnerabilities of LoRa,” 2017 3rd IEEE International Conference on Cybernetics (CYBCONF), Exeter, 2017, pp.1-6.
[12] R. Miller, “LoRa Security”, MWR Labs Whitepaper, https://labs.mwrinfosecurity.com/assets/BlogFiles/mwri-LoRa-security-guide-1.2-2016-03-22.pdf,（参照 2018-11-13）.
[13] LoRa Alliance, “LoRaWAN(TM) Specification v1.1,” https://lora-alliance.org/resource-hub/lorawantm-specification-v11,（参照 2018-11-13）.
[14] 一般社団法人 電波産業会, “標準規格概要（STD-T108)”, https://www.arib.or.jp/kikaku/kikaku_tushin/desc/std-t108.html,（参照 2018-11-13）.
[15] Ettercap, https://www.ettercap-project.org/,（参照 2018-11-13）.