LPWAとセキュリティに関する調査

A study of LPWA and security

亘理克好・ネットワーク分科会・情報セキュリティ大学院大学

Abstruct:

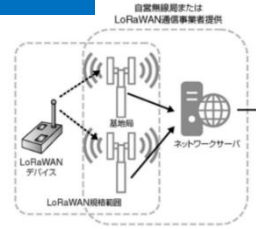
With IoT, various devices such as sensors, home appliances, factory facilities, automobiles will be connected to the Internet. The number of these devices is expected to more than 30 billion units by 2020. For these devices, low power wide area (LPWA) technology is becoming popular. In this study, we describe overviews of major LPWA technology that are LoRaWAN, SIGFOX, and NB-IoT. Then, we also consider it's security.

1. はじめに

IoTにより、これまでインターネットに接続していなかったようなセンサーや家電、工場設備や自動車など様々な機器がインターネットに接続され、新たな価値をもたらす。IoTデバイスの数は急速に増加しており、2020年には世界で300億個以上の機器が接続されるとの予測もある。
IoT機器の中でも特に産業用途のものは、通信容量は小さいが接続数が大量、さらに長期間稼働のため低消費電力であることが求められる。そのような要求のために現在開発・提供が進んでいるのがLPWA(Low Power Wide Area)である。メジャーな3方式であるLoRaWAN、SIGFOX、NB-IoTについて調査を行った。

2.方式概要

LoRaWAN

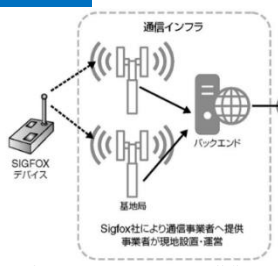


出典: IoTネットワークLPWAの基礎 鄭立

①誰でもサービス提供可能
プライベートネットでも使用可
②用途に応じてA/B/Cのデバイスクラス
③小さいメッセージ
256バイト/250-50kbps/
通信回数制限なし
④長距離通信
チャープスペクトラム拡散/
帯域500-125kHz

→採用例：登山者位置情報、農業センシングなど

SIGFOX

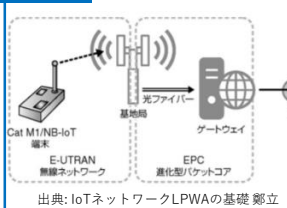


出典: IoTネットワークLPWAの基礎 鄭立

①通信はデバイス側から開始
②極小メッセージ
12バイト/1日140回/100bps
③郊外では50km超：
1メッセージの帯域100Hz
④メッセージはクラウドに保管
外部アプリと連携可

→採用例：ピザ冷蔵庫監視、スマート駐車場など

NB-IoT



出典: IoTネットワークLPWAの基礎 鄭立

①ライセンスバンド使用
既存LTEと共用運用可
②既存基地局のソフト更新で対応可能
③カバレッジは既存LTEの4-5倍
④PowerSaveMode搭載
⑤1セル当たり20万のデバイスサポート

→採用例：レンタル自転車、スマート駐車場など検討中

3. セキュリティ対応

LoRaWANとSIGFOXにのセキュリティ項目を以下に示す。

	LoRaWAN	SIGFOX
認証	デバイスID	デバイスID
暗号化	AES-128による暗号化 (MAC層はネットワークキー、 ユーザデータは アプリケーションキー使用)	オプション
デジタル署名	ネットワークキーにて メッセージ認証(MAC)	メッセージ認証 (MAC)と メッセージシーケンス番号(replay回避)
暗号鍵	ネットワークキーと アプリケーションキーの 2種類使用	ネットワークキーのみ
鍵配布	ABP(※)又はOTAA(※)にて キーを配布 (デバイス製造と回線提供が 別の場合はOTAA)	デバイス製造時に デバイス毎にキーを 割り当て ABP(※)のみ

※ABP(Activation By Personalization): 直接活性化
OTAA(Over the Air Activation): 無線活性化

4.考察

LPWAについては多種の方式があり今後の普及につれて新たな脆弱性が発見される可能性がある。LPWAといってもそれぞれ特徴を持ち違いがあり、例えば、SIGFOXはペイロードを暗号化しない。
IoT機器は台数が多く後付けのセキュリティ対策は難しいこともあり、仕様を確認してから利用する必要がある。
LoRaWANについては一部脆弱性が指摘されている[7]。鍵の取り扱いやアクティベーション、ack再送や偽の基地局など、セキュリティの問題を再度考察する必要があるのではないかと考えている。

5.今後

他の脆弱性についての考察(特に仕様の公開されているLoRaWAN)、およびNB-IoTについての現状を調査し、必要なセキュリティ対策を検討したい。

参考文献

[1] LoRaAlliance, "LoRaWAN 1.1 Specification", 2017
[2] SIGFOX, "Sigfox Technical Overview", 2017
[3] K.Moinuddin, "A Survey on Secure Communication Protocols for IoT Systems", 2017
[4] 鄭立, "IoTネットワークLPWAの基礎", 2017
[5] 日経コンピュータ, "すべてわかる 5G/LPWA大全 2018", 2017
[6] 総務省, "平成29年版情報通信白書", 2017
[7] Xueying Yang, "LORAWAN: VULNERABILITY ANALYSIS AND PRACTICAL EXPLOITATION", Delft University of Technology, 2017