

# 無線周波数の特徴量を用いた Physical Layer Authentication の実装及び評価

海江田 洋平<sup>1</sup> 国井 裕樹<sup>1</sup> 魚住 俊弥<sup>2</sup> 三輪 昌也<sup>2</sup>

**概要:** 無線通信におけるセキュリティは IoT デバイスへの攻撃増加等に伴い、今後はさらに高いセキュリティを確保することが求められる。無線通信におけるセキュリティを高める手法として、受信した無線信号の特徴量を利用し認証を行う PLA(Physical Layer Authentication) が提案されている。PLA の一手法である周波数オフセット量による認証は、送受信機の位置の影響を受けにくいこと、既存の無線トランシーバに適用可能なことから有効である。本稿では、無線トランシーバ RL78/G1H の AFC 機能により取得した周波数オフセット量を用いた PLA を提案、実装及び評価を行い、有効性を示す。

**キーワード:** 無線通信, 物理層, IoT セキュリティ, ソフトウェア無線

## Physical layer authentication using correction value of carrier frequency offset

YOHEI KAIEDA<sup>1</sup> HIROKI KUNII<sup>1</sup> TOSHIYA UOZUMI<sup>2</sup> MASAYA MIWA<sup>2</sup>

**Abstract:** With the rapid growth of IoT device attacks, wireless security becomes important concerns for IoT networks. Physical Layer Authentication(PLA) is proposed to enhance security in wireless networks using characteristics of received radio signals. In PLA, Carrier frequency offset is used to authenticate wireless devices. This method excels in that it is not affected by environments of wireless communications, and can be done with existing wireless transceivers. In this paper, we propose the way to authenticate wireless devices using AFC function of RL78/G1H. In addition, we developed and evaluated our PLA methods.

**Keywords:** wireless communications, physical layer, IoT security, software defined radio

### 1. はじめに

今後さらなる普及が予測される IoT (Internet of Things) において、多数の端末を収容するために無線通信の利用は必須である。IoT には警備やヘルスケア、医療といった分野があり、人命に関わるものやプライバシーの観点から高いセキュリティを担保することが求められる。

近年、セルラーネットワークやセンサーネットワーク、車載システム等の無線システムに対して、ソフトウェア無線 (SDR: Software Defined Radio) を用いて攻撃する手法

が報告されている [1], [2]。ソフトウェア無線とは、変復調方式や搬送波周波数等をソフトウェアで変更可能とする技術である。一つのハードウェアで多数の無線プロトコルに対応できることから、無線プロトコルの試作・検証等に用いられる他、スプーフィングやジャミング、盗聴等の攻撃の手段として用いられることもある。ソフトウェア無線機が安価に入手可能になったことや、オープンソース SDK の GNURadio[4]、関連ライブラリが普及したことにより、レガシーな独自無線プロトコルやオープンソースを利用した IEEE802.11, GSM 等の無線標準規格に対する攻撃がより容易となっており、無線システムへの攻撃の対策強化が求められている。無線通信におけるセキュリティを高める手法として、受信した無線信号の特徴量を利用し認証を行

<sup>1</sup> セコム株式会社 IS 研究所  
SECOM CO., LTD. Intelligent Systems Laboratory

<sup>2</sup> ルネサスエレクトロニクス株式会社  
Renesas Electronics Corporation

う PLA (Physical Layer Authentication) が提案されている [7], [8], [9], [10]. 本稿では, 高い無線セキュリティを担保するための PLA 手法の提案, 既存の無線トランシーバを用いた実装及び評価実験について述べる.

## 2. 既存研究

PLA の手法として, これまでに送受信機間の無線通信の環境や, 無線機自体の個体差等の物理層の特徴量を用いた認証手法が提案されている.

送受信機間の通信環境を用いるものには, チャンネル情報 (CSI:Chanel State Information) を用いるもの [10], 電波強度 (RSSI:Received Signal Strength Indicator) を用いるもの [9] がある. これらは, 端末間距離や遮蔽, マルチパス等による無線通信環境の影響を認証に用いる手法である. 無線機の個体差を用いるものには, IQ インバランシングを使用するもの [7], 周波数オフセット量を使用するもの [8] がある. これらは, 無線機の低雑音増幅器やローパスフィルタ等, アナログフロントエンドの個体差に起因する特徴量を認証に用いる手法である.

無線通信中の環境や無線機の個体差の特徴量は物理層の情報であり, 従来用いられる上位層の暗号技術とは独立に認証を行うことができる. そのため, これら二つの要素を組み合わせた認証としてさらに強固なセキュリティを実現できる. また, 攻撃者がなりすまし等の攻撃を行う際, 物理層の情報はオリジナルの無線機と異なるため, なりすましが困難という点で優れる.

従来研究では, 理論やソフトウェア無線による試作により有効性を示しているものは存在するが, 既存の無線トランシーバを用いて PLA を行っているものは無い.

## 3. 目的と提案手法

既存の無線トランシーバを用いて, 無線機の個体差の一つである, 周波数オフセット量を利用した PLA の有効性を検証することを本稿の目的とする. 周波数オフセット量とは, アナログフロントエンドの個体差に起因した無線機毎に存在する搬送波周波数のずれの量である. 無線機が送信する無線信号の周波数には, アナログ回路の個体差により一定の誤差が生じる. そのため, 標準規格や各国電波法では, 周波数許容偏差として, 誤差の許容される範囲が定められている. 例えば, IEEE802.15.4g [5] の 920MHz 帯を日本国内で使用する場合は,  $\pm 20\text{ppm}$ , IEEE802.11 [6] の場合, 5GHz 帯を使用する場合は  $\pm 20\text{ppm}$ , 2.4GHz 帯を使用する場合は  $\pm 25\text{ppm}$  と定められている. 例えば, 中心周波数 920MHz で周波数許容偏差が  $\pm 20\text{ppm}$  の場合

$$920[\text{MHz}] \cdot 20 * 10^{-6} = 18.4[\text{kHz}]$$

となり,  $\pm 18.4\text{kHz}$  の範囲に収まるように無線機は製造される. 本稿では, 許容される範囲内で存在する, 無線機毎

に異なる周波数オフセット量を認証に用いる手法を提案する. 無線機の個体差を利用する手法は, 通信環境を用いる手法と比較すると, 端末の位置やノイズ等の通信環境の変化による影響を受けにくいという利点がある. また, 攻撃者が送信機の正確な周波数オフセット量を取得するには, スペクトラムアナライザ等を使用する必要があり, 実際の無線システムに対する攻撃コストは大幅に高まる. 本節では, 使用する既存の無線トランシーバ RL78/G1H を用いた周波数オフセット量取得の手法と, その事前検証について述べる.

### 3.1 検証に用いる無線トランシーバ

無線トランシーバには, ルネサスエレクトロニクス社の RL78/G1H を用いる. RL78/G1H は, 無線通信機能を搭載した RL78 マイコンである. RL78/G1H を図 1, 主な仕様を表 1 に示す.

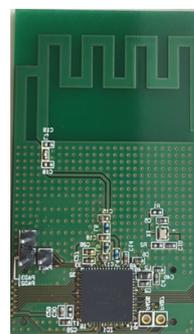


図 1 RL78/G1H  
Fig. 1 RL78/G1H

表 1 RL78/G1H 仕様  
Table 1 RL78/G1H specification

項目	
中心周波数	863MHz ~ 928MHz
変調方式	2GFSK/4GFSK
データレート	10kbps ~ 400kbps
対応標準規格	IEEE802.15.4g Wi-SUN ECHONET-Lite B ルート Wi-SUN シングルホップ HAN PHY Layer for JUTA Profile

RL78/G1H のフレームフォーマットを図 2 に示す.

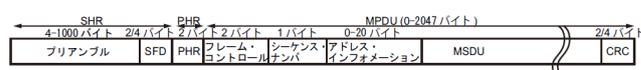


図 2 フレームフォーマット  
Fig. 2 Frame Format

RL78/G1H のフレームは, 同期を行うためのプリアン

ブル, 物理層ヘッダ, コントロール情報, フレームレンゲス等の PHR (PHY Header), デバイスアドレスや, ペイロード等からなる MPDU (Mac Protocol Data Unit) から構成される。プリアンブルは, 指定された変調方式による 1,0 の繰り返しであり, 信号長は 4 ~ 1000byte の可変長である。PHR 長は 2byte 固定, MPDU 長はペイロード長に依存する可変長である。

### 3.2 周波数オフセット量を用いる認証の手段

認証のために周波数オフセット量を取得する必要がある。これに, RL78/G1H の AFC (Auto Frequency Control) 機能を用いる。AFC 機能とは, 入力された受信信号の搬送波周波数オフセット量を, 自動的に設定値に補正する機能である。周波数オフセット量は受信性能の低下につながるため, AFC 機能を用いて補正する。AFC 機能は, 受信信号を復号可能な低い周波数に変換するダウンコンバージョンの過程で機能する。ダウンコンバージョンによる周波数変換を図 3 に示す。

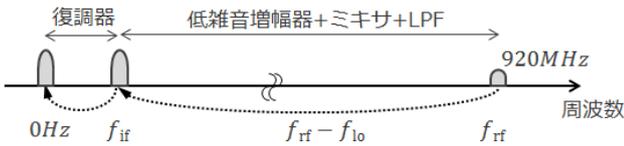


図 3 ダウンコンバージョン  
Fig. 3 Down conversion

RL78/G1H に入力された, 周波数  $f_{rf}$  の入力信号は周波数  $f_{lo}$  の局部発振器とミキシングされ, 中間周波数  $f_{if}$  にダウンコンバートされる。その後, ローパスフィルタにより不要な帯域の信号をフィルタし, ADC でデジタルに変換される。ここで,  $f_{rf}$  が受信機の基準周波数  $f_{ref}$  から計算される期待値からずれている場合, 受信信号に含まれる既知のデータの変調信号であるプリアンブル (同期用信号) を用いて, 周波数差分を計算し, これを補正してから復調する。本提案手法で用いる周波数オフセット量と送受信機の個体差の関係について RL78/G1H のブロック図 (図 4) を用いて説明する。

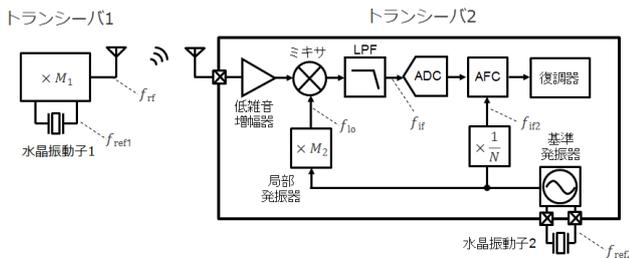


図 4 RL78/G1H ブロック図  
Fig. 4 RL78/G1H block diagram

受信機 1 から出力される信号の周波数  $f_{rf}$  は水晶振動子 1

の周波数  $f_{ref1}$  を  $M_1$  倍して生成される。ここで  $M_1$  は RF チャンネルによって決まる定数である。また, 周波数  $f_{ref1}$  は水晶振動子 1 の製造ばらつき等により, 理想的な周波数よりずれる。この周波数ずれを  $f_{\Delta_1}$ ,  $f_{ref0}$  は理想的な基準発振器の周波数,  $f_{rf0}$  は理想的な RF の周波数とすると下記式が成り立つ。

$$\begin{aligned} f_{ref1} &= f_{ref0} + f_{\Delta_1} \\ f_{rf1} &= M_1 \cdot f_{ref1} \\ &= M_1 \cdot (f_{ref0} + f_{\Delta_1}) \\ &= f_{rf0} + M_1 \cdot f_{\Delta_1} \end{aligned}$$

受信機 2 では, 入力信号は低雑音増幅器で増幅された後, 局部発振器出力とミキサで混合され, ローパスフィルタを通して, デジタルで処理可能な周波数領域  $f_{if}$  にダウンコンバートされる。局部発振器出力の周波数  $f_{lo}$  は周波数  $f_{ref2}$  を  $M_2$  倍して生成される。ここで  $M_2$  は RF チャンネルによって決まる定数である。周波数  $f_{ref2}$  は水晶振動子 2 の製造ばらつき等により, 理想的な周波数よりずれる。周波数ずれを  $f_{\Delta_2}$ , 局部発振器出力の理想的な周波数を  $f_{lo0}$ , ダウンコンバート後の信号の理想的な周波数を  $f_{if0}$  とすると下記式が成り立つ。

$$\begin{aligned} f_{ref2} &= f_{ref0} + f_{\Delta_2} \\ f_{lo} &= M_2 \cdot f_{ref2} \\ &= M_2 \cdot (f_{ref0} + f_{\Delta_2}) \\ &= f_{lo0} + M_2 \cdot f_{\Delta_2} \\ f_{if} &= f_{rf1} - f_{lo} \\ &= (f_{ref0} + M_1 \cdot f_{\Delta_1}) - (f_{lo0} + M_2 \cdot f_{\Delta_2}) \\ &= f_{if0} + (M_1 \cdot f_{\Delta_1} - M_2 \cdot f_{\Delta_2}) \end{aligned}$$

ダウンコンバートされた信号は ADC でデジタル信号に変換され, AFC 機能を持つブロックに入力される。ここで, 自身の基準周波数  $f_{ref2}$  から計算される  $f_{if2}$  に対して, 入力信号の周波数差分を計算し, これを補正する。 $f_{if2}$  は実際には水晶振動子 2 の製造ばらつき等の影響を受けるため, 下記式となる。

$$\begin{aligned} f_{if2} &= \frac{1}{N} \cdot f_{ref2} \\ &= \frac{1}{N} \cdot (f_{ref0} + f_{\Delta_2}) \\ &= f_{if0} + \frac{1}{N} \cdot f_{\Delta_2} \end{aligned}$$

ここで  $N$  は  $f_{if0}$  と  $f_{ref0}$  で決まる定数である。AFC により計算される周波数差分は下記となる。

$$\begin{aligned} f_{afc} &= f_{if} - f_{if2} \\ &= f_{if0} + (M_1 \cdot f_{\Delta_1} - M_2 \cdot f_{\Delta_2}) - (f_{if0} + \frac{1}{N} \cdot f_{\Delta_2}) \\ &= M_1 \cdot f_{\Delta_1} - M_2 \cdot f_{\Delta_2} - \frac{1}{N} \cdot f_{\Delta_2} \end{aligned}$$

RL78/G1H では  $M_1, M_2$  は 20 前後の値,  $N$  は 100 前後の値となるため, 入力周波数のずれから自身の周波数ずれの差分が支配項となるため, 以下に近似できる.

$$f_{afc} \approx M_1 \cdot f_{\Delta_1} - M_2 \cdot f_{\Delta_2}$$

本 AFC 補正值は入力信号に含まれる既知のデータの変調信号であるプリアンプル(同期用信号)を用いて行い, 毎回の受信の初めに行う. 通常, AFC 機能で補正した値は外部に出力されないが, 実験のために AFC で補正した値を取得する機能を持つカスタムファームウェアを開発した. 実験は開発したファームウェアで読みだした AFC 値を利用する. 補正值は 2 の補数値で格納され, これを AFC 値とすると, データレートに基づく定数  $\alpha$  を用いた下記式で, 周波数オフセット量を求めることができる.

$$f_{afc} \approx \alpha \cdot AFC$$

本提案手法では, 各無線機の  $f_{afc}$  を周波数オフセット量として扱い, その値の違いを認証に用いる.

### 3.3 AFC 機能の事前検証

RL78/G1H の AFC 機能による周波数オフセット量取得の精度を評価するために, 受信機のみ精度を調査としてシグナルジェネレータによる性能評価実験を, 送受信機対向での精度を評価として RL78/G1H 2 台での対向試験を行った. これら事前検証実験について説明する.

#### 3.3.1 シグナルジェネレータによる性能評価実験

RL78/G1H の開発用キットであるテセラ社の TK-RLG1H+SB, キーサイト社のシグナルジェネレータ E4438C を用い, AFC 機能の読み出し機能の性能評価を行った. 実験の構成を図 5 に示す.

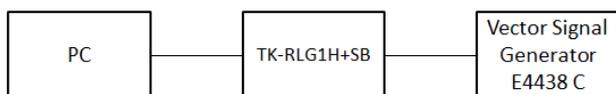


図 5 シグナルジェネレータを用いた試験

Fig. 5 Experimental evaluation using signal generator

シグナルジェネレータの中心周波数を 925.6MHz とし, -10ppm ~ 10ppm の範囲で 5ppm 刻みで変更し, それぞれ AFC 値を読み出す実験を行った. 検証時の入力信号 925.6MHz, 信号強度 0dBm, ペイロード 20byte, 繰り返し回数 1000 回, データレート 10kbps に設定し, RL78/G1H の  $f_{afc}$  を取得した. シグナルジェネレータ設定値が 0ppm 時の周波数オフセット量が本試験で使用する RL78/G1H の周波数オフセット量に相当するため, その値を補正值として, 各試験の結果から補正する. この手順で得た周波数と, シグナルジェネレータの生成した周波数を比較するこ

とで, 精度を検証した. AFC 機能の事前検証で得られた結果を表 2 に示す.

表 2 シグナルジェネレータ試験結果

Table 2 Experimental evaluation using signal generator results

SG 設定		評価結果			
設定値 [ppm]	kHz 換算 [kHz]	$f_{afc}$ -	換算値 [kHz]	補正後の値 [kHz]	誤差 [kHz]
10	9.256	3224	9.900	8.533	0.723
5	4.628	1976	6.030	4.663	0.035
0	0	448	1.367	0.000	0.000
-5	-4.628	-1048	-3.198	-4.565	0.063
-10	-9.256	-2575	-7.858	-9.225	0.031

10ppm を設定した際の誤差が 0.723kHz となりやや誤差が大きいが, それ以外では 0.1kHz 以下の誤差に収まるという結果となった. 3 節で示した通り, 標準規格の許容偏差は約 18kHz であること, 送信機と受信機が逆方向に基準周波数がずれた場合に誤差は最大となるが, その際の誤差が 36kHz 程度であること考慮すると, 十分な性能を持つと判断した.

#### 3.3.2 RL78/G1H 対向試験

RL78/G1H 同士で, 周波数オフセット量を AFC 機能で取得可能かの実験を行った. 対向試験の構成を図 6 に示す.

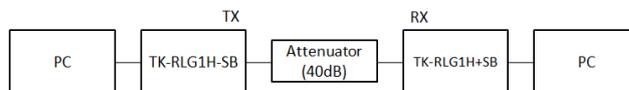


図 6 対向試験

Fig. 6 Experimental evaluation of opposite test system

送受信機は, アッテネータを介して有線で接続する. アッテネータの減衰量は 40dB とした. RL78/G1H をそれぞれ PC に接続し, 送受信のコマンド操作及び受信した値の取得を行った. 中心周波数は 925.6MHz, 信号強度 0dBm, ペイロード 5byte, 繰り返し回数 1000 回, データレート 10kbps, 変調指数  $m=0.5$  と設定し, 実験した. 事前に, 使用する送受信機の周波数オフセット量をスペクトラムアナライザで計測し, 補正を行った. その状態で, 1000 回分の送信を行い, 周波数オフセット量を計測した. 測定の結果, 平均は -6Hz, 標準偏差は 79Hz となった. 周波数オフセット量は 18kHz 前後発生することを考慮すると, 十分な精度を持つと判断した.

次に, -10ppm ~ 10ppm の範囲で送信機の周波数を変化させ, 受信側でのずれが正常に検出できるかの実験を行った. 例えば, 10ppm の場合, 理論値は 9256Hz となるが, 実際は平均で 9300Hz となったため, 44Hz の誤差となる. 結果を図 7 に示す.

結果,  $\pm 10$ ppm の範囲で平均は最大で 57Hz の誤差, 標

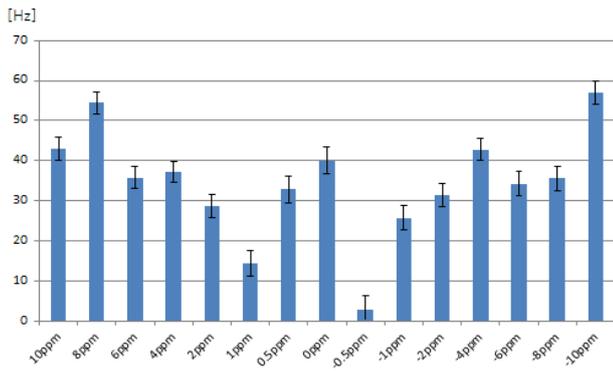


図 7 対向試験結果

Fig. 7 Experimental evaluation of opposite test system results

標準偏差は 3.31Hz であり、想定する 18kHz の範囲から比べると小さいと言えるため、AFC 機能を使った認証方式の実験に必要な精度を持つと判断した。

#### 4. 実験

前節で述べた装置を用い、AFC 機能による PLA の有効性を検証する実験を行った。実験は、(1) RL78/G1H の AFC 機能が認証に十分な特徴量を取得できるかを検証する実験、(2) ソフトウェア無線によるリプレイ攻撃がされた場合、元の送信機と異なる装置として判別可能かの実験、(3) 周波数オフセット量を用いるにあたり、端末が動いた場合にドップラーシフトの影響を受けるかを検証するための実験、3 種類の実験を行った。各実験の無線通信の送受信機には、評価試験と同様 TK-RLG1H+SB を用いた。各実験について説明する。

##### 4.1 AFC 機能による PLA 性能評価実験

センサーネットワークを想定した、AFC 機能による認証が正しく機能するかの評価実験を行う。被認証である送信機は 7 台、認証を行う受信機は 1 台とした。実験の構成を図 8 に示す。

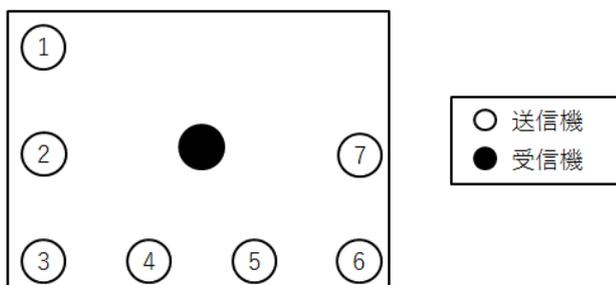


図 8 AFC 機能による PLA 評価実験

Fig. 8 Experimental evaluation of PLA using AFC function

実験は、各送信機から一台ずつパケットを送信し、それぞれ AFC 値を取得する。送信機の設定は使用チャネル 25

(925.6MHz)、信号強度-89dBm、ペイロード 20byte、繰り返し回数 100 回とした。AFC 値を基に、周波数オフセット量を計算し、送信機毎の周波数オフセット量の差で認証可能かを検証する。取得した周波数オフセット量は一定の分散を持つため、認証においては受信したパケットの周波数オフセット量がどの母集団に属するかで送信機を判別することが妥当である。よって、取得した周波数オフセット量に統計的に有意な差があれば本提案手法は PLA として有効であると判断することとした。取得した周波数オフセット量の結果を図 9 に示す。

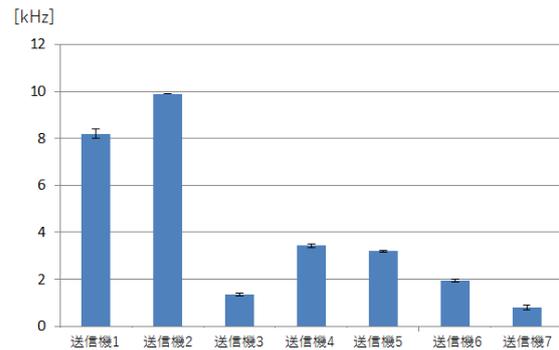


図 9 実験 (1) 結果

Fig. 9 Experimental evaluation(1) results

周波数オフセット量は各送信機毎に異なっており、平均で 1.353 ~ 9.899kHz の幅で周波数オフセット量がある結果が得られた。次に、取得したデータ群に差があるかの検定する。分散分析の結果、 $p\text{-value} \ll 0.01$  となり母集団に差があることを得たため、Tukey 法による多重比較を行った。多重比較の結果を表 3 に示す。

表 3 多重比較

Table 3 multiple comparison

比較対象	diff [kHz]	p adj	比較対象	diff [kHz]	p adj
t2-t1	1.660	1.53e-11	t7-t2	-9.153	1.53e-11
t3-t1	-6.899	1.53e-11	t4-t3	2.065	1.53e-11
t4-t1	-4.835	1.53e-11	t5-t3	1.851	1.53e-11
t5-t1	-5.049	1.53e-11	t6-t3	0.600	1.53e-11
t6-t1	-6.299	1.53e-11	t7-t3	-0.594	1.53e-11
t7-t1	-7.493	1.53e-11	t5-t4	-0.214	2.43e-11
t3-t2	-8.559	1.53e-11	t6-t4	-1.465	1.53e-11
t4-t2	-6.495	1.53e-11	t7-t4	-2.659	1.53e-11
t5-t2	-6.709	1.53e-11	t6-t5	-1.251	1.53e-11
t6-t2	-7.959	1.53e-11	t7-t5	-2.445	1.53e-11
			t7-t6	-1.194	1.53e-11

表の比較対象の t1 ~ t7 は、送信機 1 ~ 7 に対応する。評価試験の結果、全てにおいて  $p\text{-value} \ll 0.01$  となり、母集団に差があるという結果が得られた。この結果から、今回用意した送受信機においては、本提案手法は PLA として利用可能であるという結果となった。

## 4.2 ソフトウェア無線によるリプレイ攻撃実験

1 節で述べた通り，ソフトウェア無線による攻撃の脅威が高まっており，対策が必要である．ソフトウェア無線によるリプレイ攻撃を受けた場合，誤認証とすることがないかを確認するための実験を行った．実験の構成を図 10 に示す．

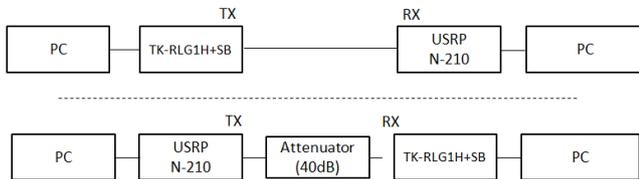


図 10 ソフトウェア無線によるリプレイ攻撃実験

Fig. 10 Experimental evaluation of Replay attack with SDR

ソフトウェア無線の攻撃の実験のために，ソフトウェア無線機 USRP-N210[3]，N210 に装着するドーターボードに WBX，GNURadio をインストールした PC を用意した．WBX 装着時の USRP N210 のスペックを表 4 に示す．

表 4 USRP N210・WBX仕様

Table 4 USRP N210,WBX specification

項目	
対応周波数	50 ~ 2200MHz
ADC/DAC 分解能	16bit
サンプリングレート	最大 40MHz
送受信	全二重

リプレイ攻撃を行うために，無線信号の受信・送信を行うソフトウェア無線のプログラムをそれぞれ開発した．受信用に，任意の中心周波数，サンプリングレートを 2MHz で受信し，PC にデータを保存するプログラムを開発した．送信用に，受信プログラムで保存したデータを読み出し，同中心周波数・サンプリングレートで送信するプログラムを開発した．プログラムの開発には，それぞれ GNURadio を用いた．設定は使用チャンネル 25 (925.6MHz)，信号強度 0dBm，ペイロード 5byte，繰り返し回数 100 回とした．USRP で受信・送信する際の使用周波数を決定するために，スペクトラムアナライザを用いて周波数オフセット量を計測したところ，RL78/G1H が 3.368kHz，USRP が 0.593kHz であった．この結果を考慮し，中心周波数を 926MHz と補正し，その周辺の周波数でリプレイ攻撃を試したが，RL78/G1H では受信失敗となった．そのため，周波数 500Hz 刻みで送信・受信を行ったところ，926.65 ~ 926.6525MHz 帯でリプレイ攻撃が成功した．そこで，前後 500Hz 刻みで受信・送信を行い，周波数オフセット量を取得した．また，RL78/G1H の周波数オフセット量と USRP の周波数オフセット量に違いがあるかそれぞれ t 検定した．これらの結果を表 5 に示す．

表 5 実験 (2) 結果

Table 5 Experimental evaluation(2) results

送受信周波数 [MHz]	average[kHz]	p-value
925.6525	-0.377	5.417e-16
925.6520	-2.720	2.2e-16
925.6515	7.906	2.2e-16
925.6510	6.048	1.397e-10
925.6505	3.837	2.911e-09
925.6500	2.787	2.039e-15

全ての結果で， $p\text{-value} \ll 0.01$  となり，有意となった．そのため，USRP N210 による受信・送信によるリプレイ攻撃は現実的には困難という結果となった．

## 4.3 ドップラーシフトの影響調査実験

実環境では，無線機は固定，可動の 2 種類が想定される．ウェアラブルデバイスや窓の開閉センサーのような可動式の場合，送信機に動きがあることが想定され，ドップラー効果により周波数が変動することが考えられる．提案方式では認証に周波数オフセット量を用いるため，周波数の変動が発生すると認証精度に問題が生じる可能性がある．本仮定を検証するために，実験した．構成を図 11 に示す．

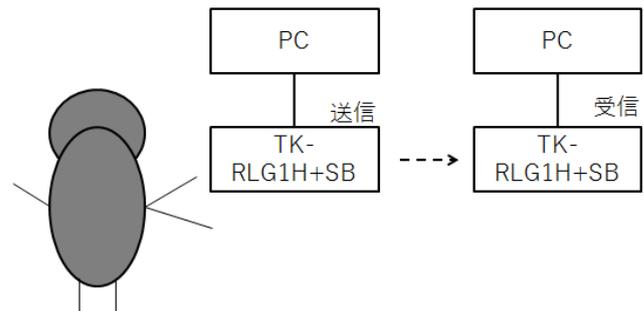


図 11 ドップラーシフトの影響実験

Fig. 11 Experimental evaluation of the influence of doppler shift

前節の実験に用いた送信機 4,5,6,7 を，それぞれ動かしながら信号を送信し，周波数オフセット量を取得する実験を行った．前節の実験と同様に受信機で周波数オフセット量を読み取る．また，各送信機において，動きのある場合とない場合での平均の差を検証するために t 検定を行った．結果を表 6 に示す．

表 6 実験 (3) 結果

Table 6 Experimental evaluation(3) results

	平均 [kHz]	平均 (動)[kHz]	p-value
送信機 4	3.134	3.293	2.89e-08
送信機 5	3.195	3.366	3.83e-05
送信機 6	1.974	2.011	0.18
送信機 7	0.702	0.641	2.78e-07

送信機 4,5,7 で動きがある場合とない場合で有意となった。また、送信機 6 では有意とならないが、一定の変化が見られた。この結果から、動きの有無で周波数オフセット量は異なる値域となる可能性が高いという結果となった。このことから、可動式の場合 AFC 機能による認証は困難という結果を得た。

## 5. まとめ

本稿では、RL78/G1H の AFC 機能で取得した周波数オフセット量を用いた PLA の手法を提案し、実機による有効性の検証を行った。RL78/G1H の AFC 機能を検証するために、シグナルジェネレータ、送受信機 2 台による対向、2 種の事前試験を行い、AFC 性能評価の結果、十分な精度があるという結果を得た。本試験では異なるトランシーバにおける AFC 機能の検証、SDR を用いたリプレイ攻撃の実験を行い、PLA での利用可能性を示した。一方、端末を動かすことによる発生するドップラー効果によって周波数に変動が起こり、可動型のトランシーバにおける本手法での PLA には課題があることを示した。

多数の端末での認証を行う場合には、提案手法単体では確率的に異なるトランシーバであっても周波数オフセット量が認証される値として受け入れられる可能性は存在する。その場合にはデジタル情報での認証と組み合わせることや複数回の PLA における認証を行うことで誤認証を避けることが出来る。またこれ以外にも、周波数オフセット量は温度変化、経年劣化により変動することが知られており、今後、さらなる検証が必要である。ソフトウェア無線の攻撃手法もリプレイではなくさらに精度の良い方法を取ることが考えられ、その場合の検証も必要である。

提案手法の特長として既存のトランシーバと既に実装されている AFC 機能を用いており、送受信機自体を変更することなく、低コストで既存の機能を用いて無線通信のセキュリティ強度を向上させることができた。また実験等であがった課題についても、AD 変換後のデジタルの信号波形を用いることなどで、さらに認証の精度を高めることができる可能性があり、今後、新たな手法の提案、検証が必要である。

## 参考文献

- [1] Joshua Wright, Johnny Cache, " Hacking Exposed Wireless, Third Edition: Wireless Security Secrets & Solutions "
- [2] Craig Smith, " The Car Hacker's Handbook: A Guide for the Penetration Tester "
- [3] USRP N210, [https://www.ettus.com/content/files/07495\\_Ettus\\_N200-210\\_DS\\_Flyer\\_HR\\_1.pdf](https://www.ettus.com/content/files/07495_Ettus_N200-210_DS_Flyer_HR_1.pdf)
- [4] GNURadio, <https://www.gnuradio.org/>
- [5] "IEEE Std 802.15.4g-2012 Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs) Amendment 3: Physical Layer (PHY) Specifications for Low-

- Data-Rate, Wireless, Smart Metering Utility Networks " "IEEE Std 802.11-2012 Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications"
- [6] P. Hao, X. Wang, and A. Behnad, " Relay Authentication by Exploiting I/Q Imbalance in Amplify-and-Forward System " Proc. IEEE GLOBECOM, Dec. 2014, pp. 61318.
- [7] W. Hou et al., " Physical Layer Authentication for Mobile Systems with Time-Varying Carrier Frequency Offsets " IEEE Trans. Commun., vol. 62, no. 5, 2014, pp. 165867.
- [8] Y. Chen et al., " Detecting and Localizing Identity-Based Attacks in Wireless and Sensor Networks " IEEE Trans. Vehic. Tech., vol. 59, no. 5, 2010, pp. 241834.
- [9] L. Xiao et al., " Using the Physical Layer for Wireless Authentication in Time-Variant Channels " IEEE Trans. Wireless Commun., vol. 7, no. 7, 2008, pp. 257179.
- [10]