Vol.2016-DPS-166 No.15
Vol.2016-CSEC-72 No.15
2016/3/3

電波解析による車載通信機器の動作推定のための ソフトウェア無線環境のモデル化

西尾泰彦[†1]　城間政司[†1]　井上博之[†2†1]

概要：本研究では，リモコンキー等の車載通信機器の動作推定のための，ソフトウェア無線適用環境の構築とモデル化を行った．本研究の成果は，ワイヤレス攻撃とソフトウェア無線技術をつなぐインタフェース的役割を果たす．これからIoT機器のワイヤレスアクセス検証を行うエンジニア目線では，ワイヤレス攻撃とソフトウェア無線とのつながりが十分研究されていない現状を鑑みると，本研究の成果は，IoTセキュリティの無線通信検証に役立つ内容となっている．本研究のセールスポイントは，ソフトウェア無線通信で多く用いられる公開リポジトリ情報，電波解析ソフトウェア情報という2つの情報が，ソフトウェア無線とどのような関係にあるかを視覚的に明らかにしている点である．その成果物として，モデリングツールを用いた受信電波の動作推定プロセスを確立した．本研究の成果は，設計図（GSN図，概念クラス図）という形でソフトウェア無線の利用ノウハウを共有できることで，今後のIoTセキュリティにおけるワイヤレス攻撃テストスイートの開発に役立てることが可能である．

キーワード：IoTセキュリティ，ソフトウェア無線，電波解析，SDR Console, MATLAB/Simulink，モデルベース検証

Modeling of the Remote Attack Surface of a Software-Defined Radio Environment

YASUHIKO NISHIO[†1]　TADASHI SHIROMA[†1]　HIROYUKI INOUE[†2]

Abstract: In this study, we develop a software-defined radio (SDR) attack environment and construct models for identifying the remote attack surface. This SDR attack environment can act as an interface between the remote attack surface of a short-range wireless access environment and the SDR communication technique; hence, it can be used to verify wireless access security in IoT systems. Specifically, we present the relationship between an open repository (GitHub) and radio analysis software (SDR Console and MATLAB/Simulink) and develop a method to monitor the shape of radio data. Finally, we develop some designs that can be used for a model-base verification scheme. In future, we will discuss a remote attack method as a security test-suite for IoT system evaluation.

Keywords: IoT security, SDR (Software Defined Radio), radio analysis, SDR console, MATLAB/Simulink, model base verification

1. はじめに

IoT（Internet of Things）ビジネスが注目されるに伴い，あらゆるものがつながる世界が作られようとしている．そしてそれらの多くは無線による接続である．しかしながら，無線技術の導入が進むにつれ，ワイヤレスアクセスが第三者に監視される等の問題が，コンシューマにも認知されはじめている．ソフトウェア開発技術者やIoTを一つのシステム品として捉える技術者にとって，無線通信がアナログ/ディジタル信号の送受信でなされていることを把握し，セキュア通信へ利活用することは重要な課題となっている．

無線通信を知る術として認知されているものとして，ソフトウェア無線（Software Defined Radio：SDR）という技術がある[1][2]．ソフトウェア無線とは，ハードウェアによるディジタル信号処理をソフトウェアで置き換えて誕生した技術である．従来の無線機が，アナログ電子回路技術により実現されていたが，近年の通信方式の高度化・ディジタル化により，ディジタル信号処理によって無線の波形，通信の状況をリアルタイムに見ることができる．こうしたハードウェア/ソフトウェアの境界がなくなりつつある状況から，ソフトウェア無線の果たす役割が大きくなっている．これに伴い，一部のアナログ回路を除き，全ての処理を汎用のディジタル信号処理ハードウェアに置き換える動きが加速している．例えば，LTEを代表とする高度なディジタル無線通信装置（基地局，端末）や，地デジの送信装置・受信機（テレビ）の開発にも使われている[3].

自動車セキュリティの分野におけるワイヤレス通信を対象とするものとしては，FM/AM電波を経由して車載ECUと通信するものや，LTE等の広域無線通信を使用するものや，V2V/V2I通信や自動運転の支援等，さまざまな通信がある[4][5]．しかしながら，車載器を含むIoT機器を用いたシステムの通信分野においては，多くの技術者にとって無線通信の中身はブラックボックスなのが現状であり，これ

†1 重要生活機器連携セキュリティ協議会(CCDS) 研究開発センター
〒900-0031 沖縄県那覇市若狭 1-14-6
Connected Consumer Device Security Council,
1-14-6 Wakasa, Naha, Okinawa 900-0031, Japan.
†2 広島市立大学大学院情報科学研究科
〒731-3194 広島市安佐南区大塚東 3-4-1
Graduate School of Information Sciences, Hiroshima City University,
3-4-1 Ozuka-higashi, Asa-minami, Hiroshima 731-3194, Japan.

から IoT 機器を検証しようとする技術者にとって不明な部分が多いのが現状である．その一方，ソフトウェア無線を使った攻撃事例が海外を中心に関心を集めている[6][7]. このことは，先の論文および，米国のハッカーの祭典である DEFCON 等でも話題になっていることからも明らかである[8]．このため，これから IoT 機器の開発や自動車セキュリティの評価検証に一から取り組む技術者にとって，無線通信部位の評価検証の仕組みを確立することは急務である. 現状，無線通信の評価検証の仕組みづくりに一から取り組んだ事例は見当たらない．これから仕組みを構築していく筆者らの組織やソフトウェアベンチャー企業等，一から始めなければならない組織にとっては無線通信の評価検証の仕組みを確立する必要がある．

そこで本研究では，ソフトウェア無線通信結果取得までのプロセスをモデル化するために，FPGA ベースのソフトウェア無線機のみが与えられた状態から，ソフトウェア無線環境の構築を行った．本研究の成果を使うことで，リモコンキーや FM 電波等による動作推定に役立てることが可能となる．本研究ではまた，SysML[9]や安全性の説明責任が生じる場面での論証で使われる GSN[10][11]と呼ばれるツールを用い，通信結果の取得というゴール達成の根拠を説明できるものとした．そして，公開リポジトリの情報や電波解析ソフトウェアに関する情報をどのようにして集め，それを体系化したプロセスモデルを作成した．最終的に，実際のソフトウェア無線機に適用することで，通信結果のエビデンスを取得するとともに，MATLAB/Simulink による正規信号データのサンプリングまでを行った．

本研究のセールスポイントは，技術者にとっての開発評価対象が，プロダクト品からシステム品へと移行し，エンジニアも変革しなければならないという状況において，誰でも無線通信の評価検証に役立てられるものとなっている点である．これにより，IoT セキュリティ検証基盤作りに苦慮している現場の実務家が，業務改善の参考にすることが可能となる．

2. ソフトウェア無線のモデル化に関する既存研究

ソフトウェア無線は，従来アナログ回路を中心にハードウェアで作っていた無線通信の仕組みをソフトウェアで実装した技術である．これにより，ソフトウェアを入れ替えることで機能拡張できる等，生産性，汎用性の高い無線通信の仕組みとして，LTE や Wi-Fi 通信等の分野で応用されている．そしてその一方で，以下のようなソフトウェア無線を使った IoT 攻撃の事例も増え始めている[12][13][14].

2.1 GNU radio を用いたシグナルフローモデル

例えば，Florian らはソフトウェア無線を使うことで，ホーム・オートメーションシステムやスマートホームシステムをアタックしたという研究成果を発表している[12]．高価な装置を使うことなく，通信プロトコルである ZigBee を安価なデバイスで実装し，解析および攻撃を行った．そして，Wireshark を使ったワイヤレスアクセスのスニフィングやトラフィックの注入を行っている．また，最近の製品における既存のアタックツールに基づいたソフトウェアフレームワークおよび財産を提案し，アイディア実現のためのコードも紹介している．同時に ability の提供も行っている．GNU radio を用いたシグナルフロー作成のグラフィカルインタフェースも紹介している．そして，GRC ファイルとよばれる GNU radio（ZigBee パケットの send/receive が行えるもの）を Python コードに翻訳も行っている．

2.2 ソフトウェア無線脆弱モデル

また，David らは，ソフトウェア無線のための，更新システムの脅威と要求の分析について考察している[13]. David らの論文では，ソフトウェア無線に，Wi-Fi 等の脆弱な波形をダウンロードするケーススタディを紹介している．そして Wi-Fi や GSM 等の脆弱なワイヤレスコネクトによりつながったインフラがはやり，ハッカーによるソフトウェア無線ネットワークへの攻撃の潜在リスクのケーススタディも紹介されている．そしてアメリカ空軍スモールビジネスイノベーションリサーチ契約のサポートのもと，脅威と要求の分析方法を示している．そしてソフトウェア無線を，SAFECOM や他の safety radio のための技術を可能なものにするという位置づけにしている．そして Wi-Fi や IEEE802.11 等のワイヤレスアクセスがハックされていることから，そしてソフトウェア無線脆弱モデルについても言及している．

2.3 サイドチャネルデータ収集モデル

Montminy らは，ソフトウェア無線を用いて，32 ビットマイクロプロセッサに対して異なる電磁攻撃を行う研究を発表している[14]．サイドチャネル攻撃が暗号化されたシステムを効果的に攻撃できるとしているが，追跡品質と，サイドチャネル攻撃データを容易に集めるために，攻撃者は対象デバイスを修正しなければならないとしている．そしてサイドチャネルデータを集める方法を提案している．また，異なる周波数で key byte なるものが漏れることも指摘している．

2.4 従来研究の問題点

上記背景よりソフトウェア無線を使った攻撃事例が増えている状況を鑑み，IoT 機器に対する不正なワイヤレスアクセスやリモート攻撃に備えることが必要となる.（以下，これらの不正アクセスや攻撃をワイヤレス攻撃と呼ぶ）. しかしながら，上記の既存研究においては，ワイヤレス攻撃とソフトウェア無線とのつながりを，これから IoT 機器のワイヤレスアクセスを評価検証しようとしているエンジニア目線で描いているとは言いがたい．

以下，第 3 章では，こうしたエンジニアにとっても理解しやすい平易なモデルを構築し，ワイヤレス攻撃という目

的を見失うことなく，たどりつけるソフトウェア無線環境モデルを構築する．そして第 4 章では，DEFCON[8]等のハッカーの祭典や国内のソフトウェア無線事例で紹介されている Nuand 社の bladeRF[15][16]という実際のソフトウェア無線製品を用いたモデルの適用結果を示す．

3. 動作推定のためのソフトウェア無線環境のモデル化

ソフトウェア製品が時代とともに多様化し，既存製品における評価検証コストが割けなくなる一方，新作業である IoT ソフトウェアや車載通信機器の開発現場ではその人員もノウハウも足りない．このため，今までシステム品や組み込みを担当していた技術者が車載通信機器をはじめとする IoT 製品の評価をしなければならなくなることも大いに考えうる．本研究では，これから IoT 機器のワイヤレスアクセスを評価検証しようとしているエンジニア目線で，要求図によるスコープモデルとその詳細化モデルについて考察する．

3.1 要求図によるスコープモデル

先の背景を想定した場合に必要となるのが，ワイヤレス攻撃とソフトウェア無線がどのような関係にあるのかを明らかにすることである．具体的には，ソフトウェア無線機のみ所有している状態で，どうすればワイヤレスアクセスの評価検証につなげられるかの道筋を示すことである．これを実現するためには，分析ツール等の形式手法が有効であるが，本研究では UML/SysML の要求図を用いる．理由としては，ワイヤレス攻撃とソフトウェア無線をつなぐものという概念をイメージしやすくするためである．ワイヤレスアクセスに必要な手順，プログラムを要求インタフェースで表し，それを成し遂げるものを提供インタフェースで表現することで，プロセスを部品のように扱い，汎用性を高めることができるためである．こうしたモデリングは，自動車や組み込み設計等でも用いられている．よって，本研究では要求図を用い，ソフトウェア無線からワイヤレス攻撃や評価検証の道筋となる汎用モデルを構築する．

このモデルは，スタートモデルの役割も示し，ワイヤレス攻撃技術を求めるステークホルダが要求するものを要求インタフェースで表し，ソフトウェア無線を使いそれを成し遂げる成果を提供インタフェースで表し，常にここに立ち返るものにすることを意図している．次節より，このインタフェース部分の詳細化について議論する．

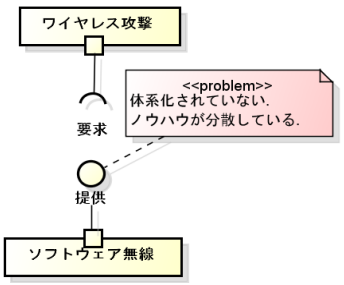

図 1: 本研究のスコープモデル
（要求図による表現）

3.2 スコープモデルとその詳細化

既存研究より，ワイヤレス攻撃を検証するためには，ソフトウェア無線機を動かすことで，どのような入力/出力が生じるかを明らかにしなくてはならない．

ソフトウェア無線通信は，通信基盤をソフトウェアですべて実装しているため，出力をディジタル信号として処理を行う．このためモデル構築するためには，信号データの取得が必要となる．信号データの取得のためにはソフトウェア無線を操作するコマンドラインや GUI 等の操作が必要であることから，これらが中継点となる．また，信号の波形出力および変調方式を特定するためには，MATLAB/Simulink 等のシミュレーションソフト等を用いる必要がある．そこで本研究では，図 1 のスコープモデルにおいて，ソフトウェア無線側からのコマンドライン操作ハンズオン手順や Simulink 手順を提供インタフェースとして表現することで，波形出力処理が求める要求インタフェースにつなげるというモデルに詳細化した．

ワイヤレス攻撃側からのモデル詳細については，ソフトウェア無線の正規の信号データ（変調信号）を拾い，そのデータの解析を想定した．理由としては，駒野[17]，他の研究により，電磁波をサンプリングし，その統計から鍵データの解析等につなげているためである．このため本研究

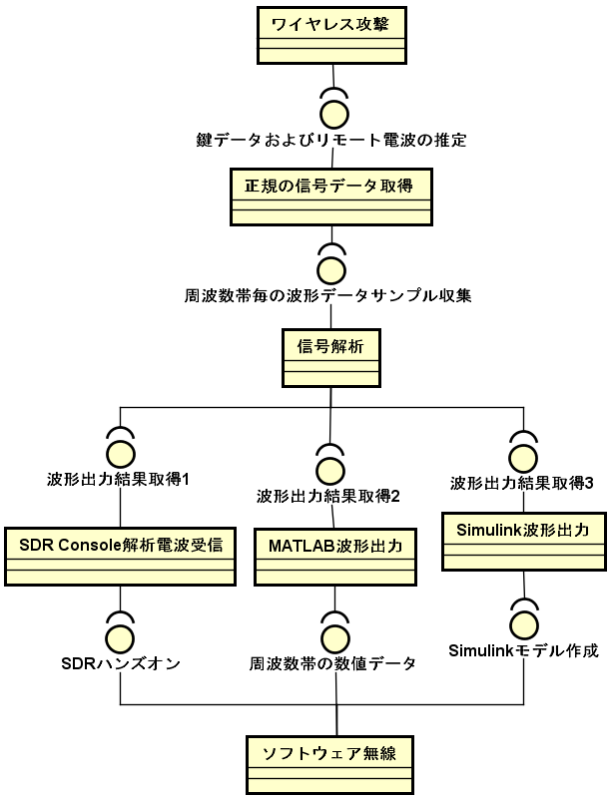

図 2: スコープモデル詳細化

では，ワイヤレス攻撃が要求するインタフェースを，鍵データおよびリモート電波の推定とした．これにより，ワイヤレス攻撃の側面を検証するために,正規の信号データ(変調信号）の収集というアウトプットを作るモデル部位を図 2 のように詳細化した．

以上のモデルに沿うことで，ソフトウェア無線における作業を，目的を見失うことなく，評価検証に役立てることが可能となる．しかしながら，図 2 はスコープとしては有用であるものの，目的を達成するためのソリューションという意味では不十分であることから，本研究ではさらに，GSN とよばれるゴール達成プロセスのための論証ツールを適用し，通信結果の取得という名のソリューションの導出を行った．次節にてその詳細について示す．

3.3 GSN プロセスに基づいたソフトウェア無線通信結果取得モデル

ものづくりの現場において，特定の問題を解決する際，様々な形式手法が存在する．たとえば，FTA 分析や WBS 分解等がそれにあたるが，ここに銀の弾丸は存在しない．このため，組み込みソフトウェアや自動車システムの安全分析等，ディペンダブルなモノづくりのための形式手法である，GSN を用いた．

GSN は，DEOS プロセス[11]やディペンダブルなモノづくりのため，組み込み業界や自動車業界にて多く使われるツールである．メリットとしては，後で検証する際，なぜそのアプローチが妥当かを説明する際の道具になることがあげられる．自動車業界では，セーフティケースの説明ツールとしても，多くの実績があることから，本研究でも，通信結果を得る上で，なぜその作業をおこなったかの説明責任も果たすことができる．また本手法は，車載器セキュリティの研究[18]においても実績がある．この手法を使うことで，図 4 のような，通信結果を得る上で，ソフトウェア無線通信エビデンスを得るソリューションを図 3，図 4 で導出した．

図 3 は，ソフトウェア無線の信号解析をゴールにした場合の GSN 図を示す．このモデルでは，いざ使いたくても使えない状況を打破するというストラテジ（戦略）のもと，サブゴールを導出し,デバイス提供元の情報体系化および，ユーザ・コミュニティ情報の体系化という 2 つのサブゴールに分割を行った．そしてどのような電子データを得ることが必要かというストラテジのもと，受信データの取得およびデータ送受信メカニズムを明らかにする．そのサブゴールから，特定周波数の数値データ取得というソリューションを導き出すことで，図 3 のようなモデルを構築し，通信エビデンス取得 GSN モデル 1 とした．

さらに，図 3 のソリューションを特定周波数の数値データ取得というゴールに再設定し，以下の 3 つのストラテジから，どのような出力ファイルを得るべきかのモデルを構築したところ図 4 のようになった．このモデルを通信エビデンス取得 GSN モデル 2 とする．

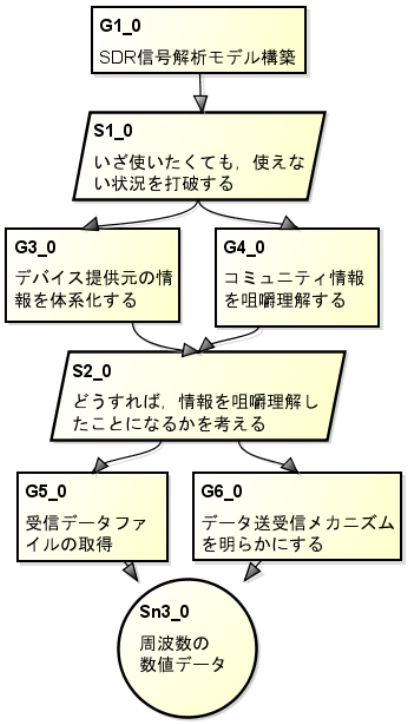

図 3: 通信エビデンス取得 GSN モデル1

ストラテジその 1： IQ サンプルファイル
ストラテジその 2： 信号送信コマンド
ストラテジその 3： 信号受信コマンド

IQ サンプルファイルとは，I/Q データは、信号波形の正弦波の振幅および位相の変化を示すものである。振幅と位相が規定の方法で規則的に変化すると，それにより変調と呼ばれるプロセスの正弦波に関する情報の符号化を行うことが可能となる。そしてこの IQ サンプルファイルを信号送信コマンド,および信号受信コマンドで制御することで，信号処理データとしてのソフトウェア無線における，特定周波数の数値データを得ることができることから，図 4 のような GSN モデルに基づいたソリューション導出モデルを構築した.そしてこのモデルに沿って作業を行うことで，MATLAB と連携した波形出力を得ることが可能となる．事次章では，図 2，図 3，図 4 のモデルを，実際の FPGA ベースのソフトウェア無線機へ適用し，波形出力データのサンプル出力例について述べる．

4. ソフトウェア無線環境モデルの実機器への適用

4.1 FPGA ベースのソフトウェア無線機への適用

上記モデルにおいて，ソフトウェア無線をつかったワイヤレス攻撃への利用モデルと，波形出力結果の利用までのアクティビティをモデル化した．本章ではこれらのモデルを実際のソフトウェア無線環境に適用した結果について述

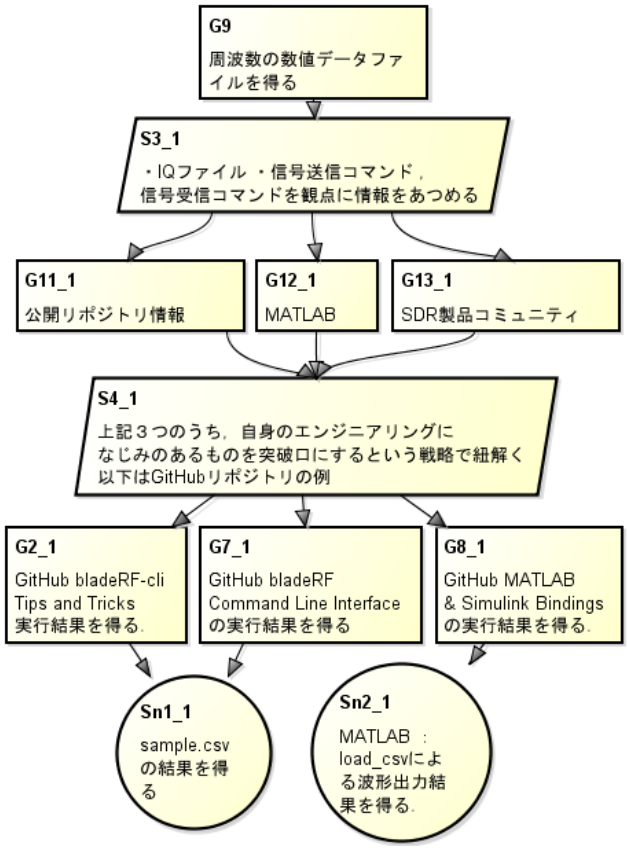

図4: 通信エビデンス取得 GSN モデル 2

べる．使用機器としては，FPGA ベースのソフトウェア無線機を選定した．FPGA は通信電波の生成に多く用いられており，幅広い帯域の受信が可能であるだけでなく，以下のようなことが可能である[19].

- 逐次処理であるソフトウェア処理と比較して，FPGA ではディジタル回路で並列処理を行うことができるため高速な処理が可能である．
- 回路の仕様変更が容易なので，設計を試行錯誤できる．
- 設計したらコンパイル後すぐに実機動作させられるため，ソフトウェア・ハードウェアの設計を同時に行うことが可能である．

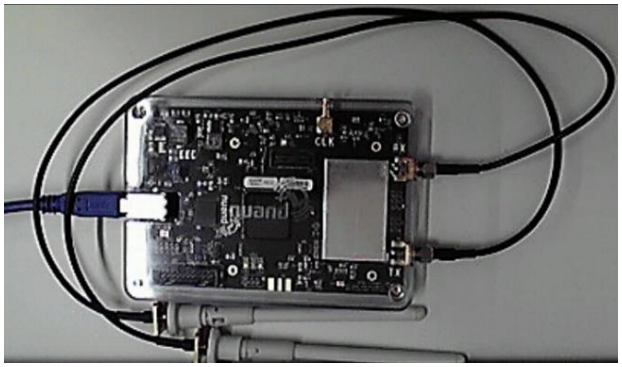

図 5: ソフトウェア無線機（Nuand 社 bladeRF）

- マスクが不要なためイニシャルコストが安い．

また，ファームウェアの入れ替えを行うことで，あらゆるタイプの通信が可能となる．本研究では，Nuand 社製，bladeRF と呼ばれるソフトウェア無線トランシーバ[15][16]を用いた．詳細は後述する．

4.2 通信エビデンス取得

図 6 では，bladeRF を用いた通信結果取得の様子を示している．3.3 節で述べたモデルを適用することで，特定周波数帯における電波出力結果を得られた．図 4 の通信エビデンス取得 GSN モデル 2 において，IQ ファイル，tx コマンドとよばれる信号送信コマンド，rx コマンドと呼ばれる信号受信コマンドを軸，20MHz 帯の通信結果を取得していることがわかる．また，MATLAB/Simulink もサポートしていることから，CSV で得られたデータから波形出力結果を得ることも可能であり，その結果も得ることができた．

bladeRF-cli は，bladeRF を制御するコマンドラインであることから，通信に必要なコマンドを実行しなければならない．以上より，相互通信コマンドである rx コマンド，tx コマンドの実行として手順化することで，図 7 のように波形出力結果が得られることを示すことができた．

4.3 MATLAB/Simulink によるリモートキーデータ取得

車載器通信におけるディジタル信号解析のため，

```
bladeRF> set frequency rx 1575.42M
 Set RX frequency: 15754200000Hz
bladeRF> set samplerate rx 8M
Setting RX sample rate - req: 8000000
0/1Hz,
actual: 8000000 0/1Hz
bladeRF> set bandwidth rx 5M
bladeRF> rx config file=”my_samples2.csv”
       format=csv n=20M
bladeRF> rx start
bladeRF> rx
State: Running
Last error: None
File: my_samples2.csv
File Format: SC16 Q11, CSV
# Samples: 2097150
# Buffers: 32
# Samples per buffer: 32768
# Transfers: 16
Timeout (ms): 1000
bladeRF>
```

図 6: 受信サンプルデータの出力結果

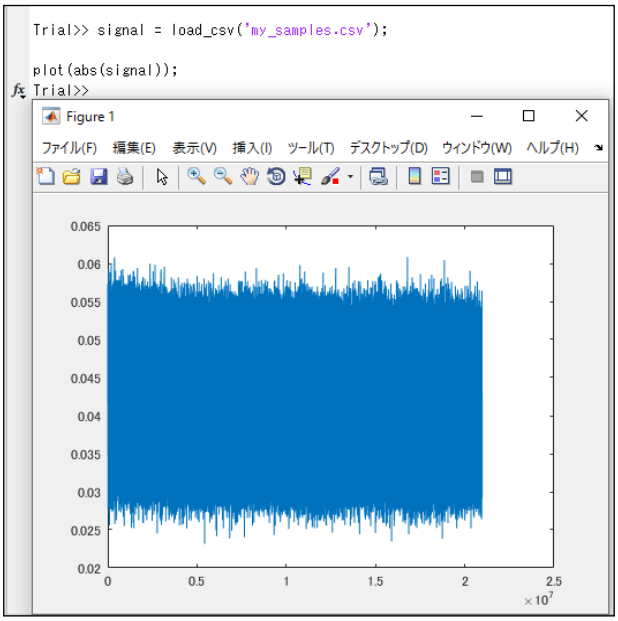

図7: MATLAB による波形出力例

MATLAB/Simulink を用いることで，以下を用いたシミュレーションを行うことができる．

① DSP System Toolbox
リアルタイム信号処理用のテストシステムの作成や，IoT アプリケーション用のシステムの作成が可能となる[20].

② ソフトウェア無線機による OTA での信号の送受信
外部ハードウェアデバイスからの信号を読み取ることが可能となる[21].

本研究ではその準備段階として，bladeRF のモデルを Simulink でモデル化し，そこから得られるタイムスコープ，ベースバンド，オーディオ信号表示を試み，正規の信号電波の収集に使用可能なアクティビティを作成した．図 8 は，bladeRF を用いた FM 受信機を Simulink でモデル化したものである．こうしたモデルを使用してシミュレーションを行うことで，タイムスコープ，ベースバンド，オーディオ信号表示のデータを取得することが可能となる．

これらのシミュレーションで得た出力を応用し，ソフトウェア無線モデルに沿った図 10，図 11 のような自動車のキーレスエントリーのスペクトラムデータの収集を行った．リモコンキーから車への信号が 315MHz であることから，実験を行ったところ，図中で水色の波形で示される各周波数のピーク値を出力することができた．図 10 はリモコンキー操作なしの場合，図 11 はリモコンキー操作ありの場合で，-100kHz～+100kHz の間で変化が生じることをつきとめた．-30kHz と+30kHz の部分に 2 つのピーク周波数があることから，このリモコンキー電波の変調方式は FSK（Frequency Shift Keying）であると推測される．

本研究ではさらに図 12 のような SDR Console とよばれるツールでも波形出力結果の収集を試みた．ソフトウェア無

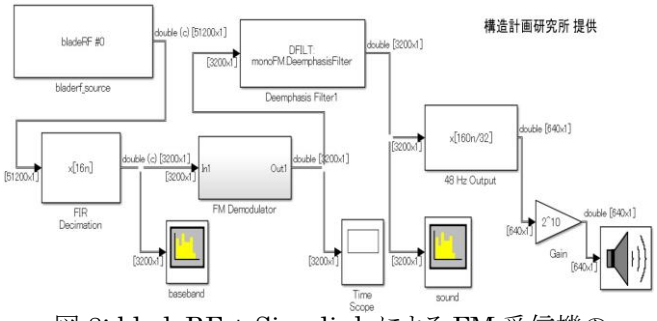

図 8: bladeRF + Simulink による FM 受信機のモデルサンプル

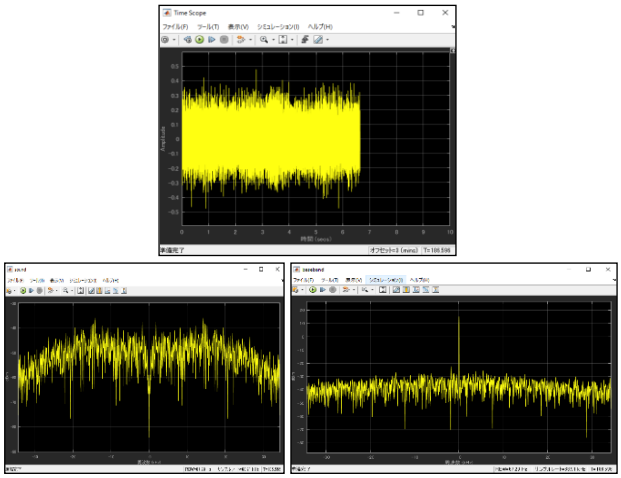

図 9: FM 受信機のタイムスコープ，ベースバンド，オーディオ信号表示サンプル

線はより多目的であり，異なるソフトウェア定義を使うことで，ソフトウェア無線機が Bluetooth, FM ラジオ, Wi-Fi, GPS，LTE 等，異なる帯域で通信可能であることから，FM ラジオ受信する方法を模索した．

FM 電波はワイヤレス攻撃における侵入ポイントとして挙げられている．このことからソフトウェア無線から FM 受信を行うことを考えた．これらの技術は，FM/AM/XM を侵入ポイントとする不正アクセスに応用することが可能となる．

4.4 まとめと考察

本研究では，bladeRF のみ与えられている状態から，ワ

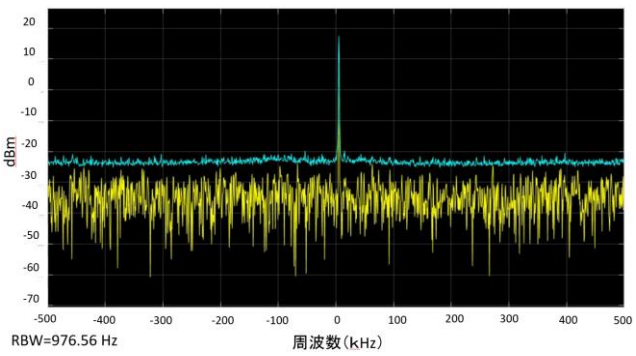

図 10: 車のリモコンキーの電波スペクトラムデータ（リモコンキー操作なし）

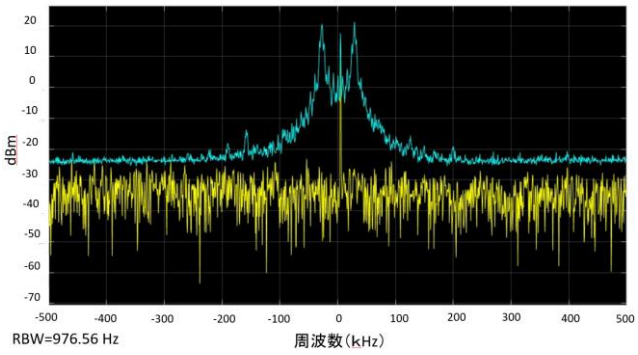

図 11: 車のリモコンキーの電波スペクトラムデータ
(リモコンキー操作あり)

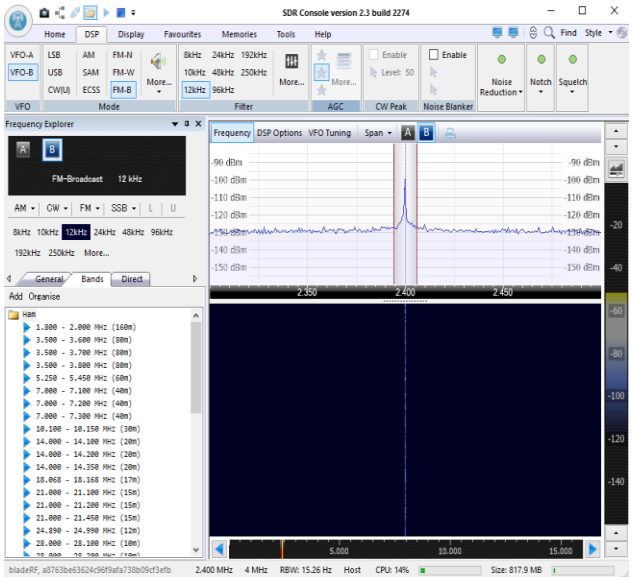

図 12: SDR Console による FM 電波受信

イヤレス攻撃と bladeRF をつなぐもの（インタフェース部分）の開発を行った．具体的には，FPGA ベースのソフトウェア無線受信機を使った正規の信号電波取得モデルを作り，それにそった作業を行うことで，bladeRF セットアップから，ソフトウェア無線の受信データである変調信号取得までを行った．現在の成果は以上にとどまっているが，ソフトウェア無線のノウハウが体系化されていない昨今の現状を鑑みると，情報精査，体系化，コマンドラインによる通信結果取得，波形出力までをモデル化し，関係するファクター同士の関連を視覚的に明らかにする意義は大きいと考える．また，これから IoT 機器のワイヤレスアクセス検証を行う技術者にとっては，ソフトウェア無線はノウハウが無い状態からのスタートがほとんどである．無料のセミナーやサービス等も行われているが，本研究の成果を生かすことで，セミナー等の体系化情報の早期吸収が可能となるという副次的意義も得られた．また，MATLAB/Simulink との連携により，ゼロからの状態で波形出力までを実行した本成果を，これから IoT 機器のワイヤレスアクセス検証を行うエンジニア目線でのものとすることができた．

5. 今後の課題

今後の課題としては，得られた変調信号の復調を行うモデルの確立が挙げられる．自動車のリモートキーは FSK の変調信号形式が多いため，FSK 変調方式の特定の自動化と中心周波数の特定をおこなっていく必要がある．筆者らの組織では，ハンズオン作業を行いながら攻撃手法の開発と検証の仕組み作りを並行して行っている．無線による攻撃手法もモデル化する予定であるが，こちらは防御の仕組みにしてから公開の予定である．本研究で構築したモデルは，設計図という形をとっているが，攻撃の複雑度を示すヒントにもなりうるため，攻撃複雑度というメトリクスを作り[18]，総合的なセキュリティ評価に寄与することも検討中である．

謝辞

本研究における MATLAB/Simulink シミュレーションにおいて多大なるご協力およびサンプルモデルの提供をいただきました，株式会社マスワークスおよび株式会社構造計画研究所の皆様に感謝の意を表します．

参考文献

[1] 河野隆二，春山真一郎，”ソフトウェア無線の現状と将来”，電子情報通信学会論文誌 B，通信 J84-B(7), pp.1112-1119, 2001.
[2] 東京大学 森川研究室，” Gnu Radio/USRP を用いた研究事例と今後の展開”，http://sarulab.inf.shizuoka.ac.jp/pdf/mlab/MBL49_saru.pdf，参照 Dec. 13, 2015.
[3] 寺前裕司，“らくらく！SDR 無線機入門”, RF ワールド No. 22, CQ 出版社，2013.
[4] S. Checkoway, et al., “Comprehensive experimental analyses of automotive attack surfaces”, USENIX Security Symposium, Aug. 2011.
[5] Chris Valasek, and Charlie Miller, “Remote Exploitation of an Unaltered Passenger Vehicle,” Technical White Paper, pp.1-93, IOActive Security Service, Aug. 2015.
[6] D. Genkin, L. Pachmanov, I. Pipman, and E. Tromer, “Stealing Keys from PCs using a Radio: Cheap Electromagnetic Attacks on Windowed Exponentiation”, Workshop on Cryptographic Hardware and Embedded Systems (CHES) 2015 in September 2015.
[7] Wired.com Website, “Watch This Wireless Hack Pop a Car’s Locks in Minutes”, http://www.wired.com/2014/08/wireless-car-hack/, accessed, Dec. 13, 2015.
[8] RTL-SDR.COM Website, “SOFTWARE DEFINED RADIO TALKS FROM DEFCON 23”, accessed, Jan. 19, 2016.
[9] 株式会社チェンジビジョン，“astah* SysML システムモデリングツール，” astah* ホームページ，http://astah.change-vision.com/ja/product/astah-sysml.html，参照 Dec. 8, 2015.
[10] 株式会社チェンジビジョン，“astah* GSN - GSN 支援ツール，” astah* ホームページ，http://astah.change-vision.com/ja/product/astah-gsn.html，参照 Dec. 8, 2015.
[11] Mario Tokoro (Ed.), “Open System Dependability: Dependability Engineering for Ever-Changing Systems Second Edition,” CRC Press, A SCIENCE PUBLISHERS BOOK, 2015.
[12] Florian Eichelberger, “Using Software Defined Radio to Attack

"Smart Home" Systems", SANS Institute InfoSec Reading Room, pp. 1-30, 2015.
[13] David Murotake, and Antonio Martin, "Updated System Threat and Requirement Analysis for High Assurance Software Defined Radios", Wireless Innovation Forum, SDR'05 Papers, Jan. 06, 2014.
[14] Montminy, D.P, Baldwin, R.O, Temple, M.A, and Oxley, M.E, "Differential Electromagnetic Attacks on a 32-bit Microprocessor Using Software Defined Radios", Information Forensics and Security, IEEE Transactions on (Volume: 8, Issue: 12), pp. 2101-2114, 2013.
[15] 構造計画研究所, "bladeRF 情報", http://network.kke.co.jp/products/rrp/whats_sdr.shtml, 参照, Dec. 13, 2015.
[16] Nuand co. ltd., "bladeRF Windows installation", https://www.nuand.com/windows-pre-2014.11.php, accessed, Dec. 13, 2015.
[17] 駒野雄一, "CARDIS 2015 の Re-keying 方式の再考察 Reconsideration on Re-keying scheme from CARDIS 2015, "暗号と情報セキュリティシンポジウム SCIS2016, pp.1-8, Jan. 2016.
[18] 西尾泰彦, 井上博之, "ISO/IEC 25010 品質特性に基づいた IoT セキュリティ評価メトリクスの策定～車載 LAN セキュリティのハンズオン作業からの策定～," 暗号と情報セキュリティシンポジウム SCIS2016, pp.1-8, Jan. 2016.
[19] マスワークス, "プログラム可能な集積回路 FPGA の設計", マスワークスホームページ, http://jp.mathworks.com/discovery/fpga-design.html, 参照 Feb. 4, 2016.
[20] マスワークス, "DSP System Toolbox", マスワークスホームページ, http://jp.mathworks.com/help/dsp/, 参照 Feb. 4, 2016.
[21] MathWorks, "Documentation: Signal Transmitting and receiving by OTA via SDR device", MathWorks Website, http://jp.mathworks.com/help/comm/ug/transmit-and-receive-signals-over-the-air-with-software-defined-radios.html, accessed Feb. 4, 2016.