短距離無線通信向け脆弱性検査ツールの初期的検討

An Initial Study on a Vulnerability Testing Tool for Short-range Wireless Communication

瀬川 周平・マネジメント分科会・情報セキュリティ大学院大学

In the new application field using IoT, it is feared that many vulnerable devices that do not have encrypted communication implemented in the transition period. As a step toward addressing concerns, we created a tool that can analyze communication contents of the EnOcean protocol, which can not be dealt with by other similar researches and tools.

研究の背景

様々な分野で拡大する小型IoT機器は，リソース不足によりセキュリティ対策が十分に施されず市場に出回る懸念があるため，市場に出回る前に検査することが求められるが，既存のツールでは，未対応プロトコルや，解析精度の点で不十分であり，新たなツールが求められる．

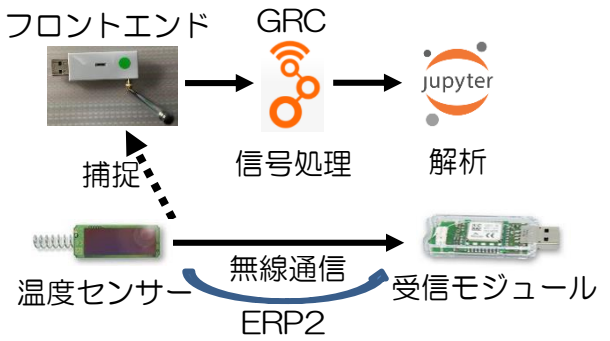
研究目的

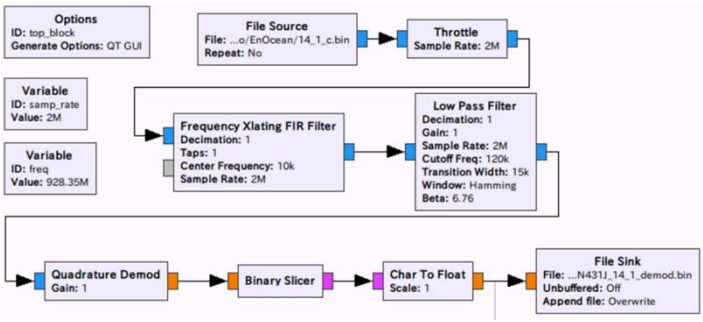
導入が容易で，正確な結果が出せる複数の短距離無線通信プロトコルのテストツールを開発すること

実証方法

- 無料オープンソースツールであるGRC，安価な汎用品フロントエンドを使用
- 結果は，既存ツールのURHと比較する

実験内容





- ノイズ処理のためのパラメータ最適化
- 周波数変調の復調にQuadrature Demodモジュールを応用

$$x[n] = A \cdot e^{i2\pi(\frac{f}{f_s}n+\varphi_0)}$$

$$y[n] = \arg(x[n] \cdot \dot{x}[n-1]) = \frac{f}{f_s}$$

結果・比較

解析対象	GRC	URH
（キーレス）	○	○
EnOcean	○	×

- 既存ツールでは解析できないEnOceanプロトコル(周波数変調)の解析が可能に
- 解析精度は 100%
- 無料のオープンソースツールであるGRCと安価な汎用品フロントエンドを使用しているので，導入が容易