SecHack365

スマホを用いた偽基地局の位置推定システム

学習駆動コース　今岡ゼミ　田原史之典

1. 背景・目的

背景：インバウンドを狙う「見えない攻撃」

2024年春頃より訪日外国人観光客を標的とした、
GSM偽基地局によるサイバー攻撃が発生しています。

目的：安全な通信環境の提供

偽基地局を特定・位置推定するシステムを開発し、
検挙や抑止に繋げることによって、訪日外国人が安心して利用できる通信インフラを守ります。

GSM(2G)
日本以外での2Gの規格
脆弱性アリ
まだ世界中に**10億台**

偽基地局
不法基地局
車やバイクに搭載
発見・特定が困難

2. 偽基地局の攻撃手法

Ⅰ. 4G/5Gを妨害
妨害電波を出して、
スマホを「圏外」にする

Ⅱ. 2Gへ強制接続
安全性の低い2G(GSM)へ
接続させ、**通信を乗っ取る**

主な攻撃被害

サービス妨害
決済端末や配車アプリが通信不能になり業務停止

偽SMS送信
偽サイトへ誘導しIDやパスワードを窃取する

偽電話
折り返し電話をかけさせ、高額な通話料を請求する

3. 本システムの概要

A. 2G電波を検知
捜索用のスマホを2Gに接続して電波の強さの情報を取得

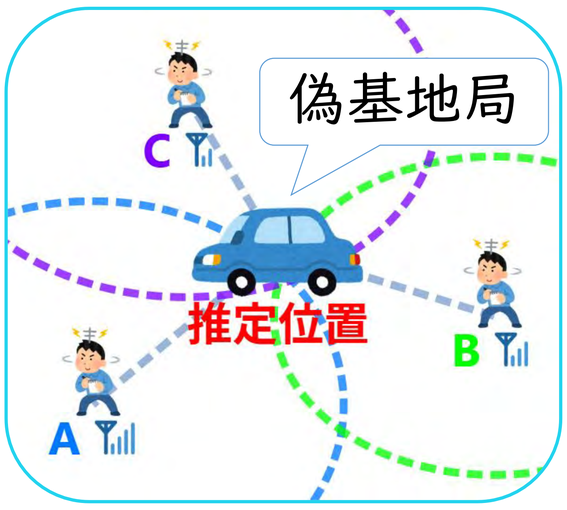
B. 三辺測量
電波の強さの情報を集めて偽基地局の位置を推定

C. マップに表示
偽基地局の推定位置を表示

4. 偽基地局の位置推定方法

電波の強さ(RSSI)を用いて、複数の基地局からの電波の強さを測定し、三辺測量の原理で位置を特定します。

https://x.com/denpa893/status/1911755963516014940
電波やくざ氏のXより引用



5. 実証実験でのアプリ画面

※偽基地局の稼働は散発的であるため、常時観測可能なLTE商用網を用いて位置推定アルゴリズムの原理検証を実施しました

開発中のアプリ画面の様子

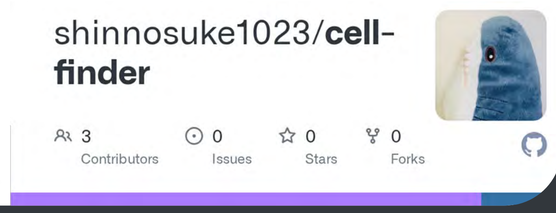
実際の基地局設置位置と推定位置の比較

6. まとめ・今後の展望

- 偽SMSや情報の窃取などを行う偽基地局が社会問題
- ハニーポットにしたAndroidスマホで位置を推定
- 端末を持って歩き回って偽基地局の位置を絞り込む
  LTE基地局でビル一棟分程度の誤差
  - 十分な精度であるかの検証
  - より高精度にできるか
- **みんなのスマホをセンサネットワークにして偽基地局を見つけて、安心安全な通信環境をつくりましょう！**

本システムのリポジトリは →こちらから！

https://github.com/shinnosuke1023/cell-finder



NICT National Institute of Information and Communications Technology
SecHack365での活動に際して事務局、トレーナー、トレーニー、関係者の方々のご支援に心から感謝申し上げます。