

高杢慎介, 鈴木信雄

(近畿大学産業理工学部)

1. はじめに

近年実用化された5Gでは、オープンソースによる評価実装が進んでおり、基地局(BS)などの機能を試すことが比較的容易となっている。そのため、様々なセキュリティ課題が現実的になってきている。中でも、不正BSによる中間者攻撃の脅威が多く指摘されており対策が望まれている。3GPPでも課題は認識しており、不正BS検出法が多く提案されている[1]。しかし、そのほとんどが通信プロトコルの改変を伴うものであり、標準化や設備更改などの多大な作業が必要である。そのため、通信プロトコルの改変を前提としない第三者による不正BSを検出する手法が必要である。本研究では、MIMOで用いられているチャンネル状態情報(CSI)の固有値を用いる。CSIを用いたBS識別の研究は現状では見当たらないが、無線LANのCSIを使った位相誤差による通信接続を識別する類似研究がある[2]。この手法では、APと端末間の接続を識別しているため、あらかじめAPと端末を接続する必要がある。そのため、本研究の目的である第三者からの識別には適さない。本稿では、CSIの固有値を用いた基地局識別法を提案する。さらに、不正BS攻撃に多く利用されるハンドオーバー処理時に、不正BSを検出する手法について考察する。

2. CSI固有値を用いた基地局識別法

本研究では、MIMOのチャンネル行列推定に利用されている固有値を使ってBSを識別することを提案する。MIMOでは、送信指向性制御や適応変調などに固有値が用いられている。この時の固有値算出処理をそのまま利用することでBS識別処理コストを低減することが考えられる。固有値は、主成分分析でも用いられており、どのサブキャリアがBSの特徴にどのくらい影響しているかを示している。

固有値は、式(1)で表現されるBS每位相の固有ベクトルを式(2)の固有方程式で解くことにより算出する。ここで、 A はCSIから求めた位相行列、 λ は固有値、 I は単位行列、 x は固有ベクトルを示す。BS毎に固有値の個数は異なっており、一般的には値が1以上で有意であると解釈される。

$$(A - \lambda I)x = 0 \quad \dots(1)$$

$$\det(A - \lambda I) = 0 \quad \dots(2)$$

評価用に収集したCSIデータを用いて固有値を実際に求めたところ、第5主成分までの値がBS毎の変化が最も大きいことがわかった。そのため、第5主成分までの固有値の分散を代表値としてBSを識別することとした。本提案方式のシステム構成を図1に示す。

3. 評価

評価では、CSIから算出する生の位相、既存研究にて提案されている位相誤差、そして本研究で提案するCSI固有値を比較した。本評価では、低コストで実現できる無線LAN APを用いた。比較結果を図2に示す。この結果から提案したCSI固有値の場合が最も分散が大きいことがわかった。これは、最も多くのBSを識別することができることを示している。

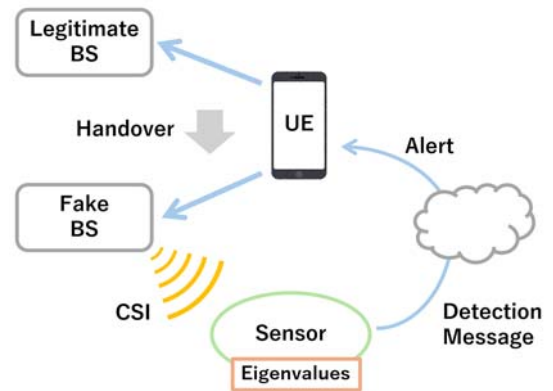


図1 システム構成

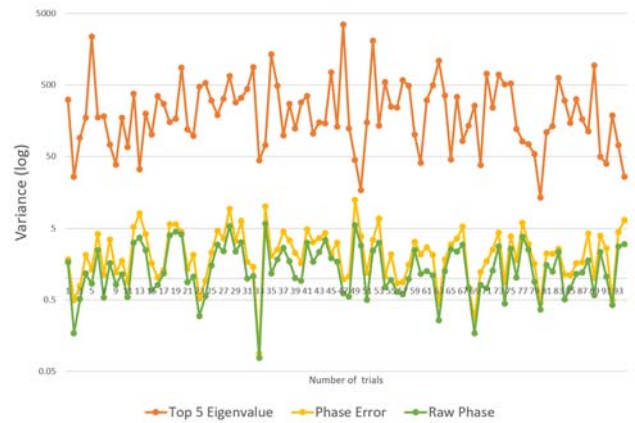


図2 識別性能の比較

4. 不正基地局検出の考察

不正BSがUEを接続する時にはハンドオーバーを利用することが多い。5Gでは、ハンドオーバーにより別な正当BSへ接続する時には相互認証により不正BSへの接続を防ぐことができる[3]。しかし、初回の接続時にはBSの正当性を確認することができない。そのため、初回接続時に不正BSを検出する必要がある。さらに、ハンドオーバー時には不正BSへ接続されないが、UEは接続の試みを長時間継続してしまう。その結果、UEが正当なBSへ接続できないDoS攻撃が成立してしまう。これまでの研究では、正当BSのフィンガープリントを事前にDBへ登録し、不正BSを抽出する方式が多い[3]。しかし、DB登録や検索処理のコストが大きく、IoTなどのUEでは負荷が高い。そのため、UE周辺BSのCSI固有値をクラスタリングすることにより不正BSを検出する方式が有効である。

参考文献

- [1] 3GPP, TS 33.501: Security architecture and procedures for 5G system, 2022.
- [2] Pengfei Liu, et al., Real-time Identification of Rogue WiFi Connections Using Environment-Independent Physical Features, IEEE INFOCOM 2019.
- [3] Amiraslan Haghray, et al., A survey on the handover management in 5G-NR cellular networks: aspects, approaches and challenges, EURASIP Journal on Wireless Communications and Networking, No.2023.52, 2023.