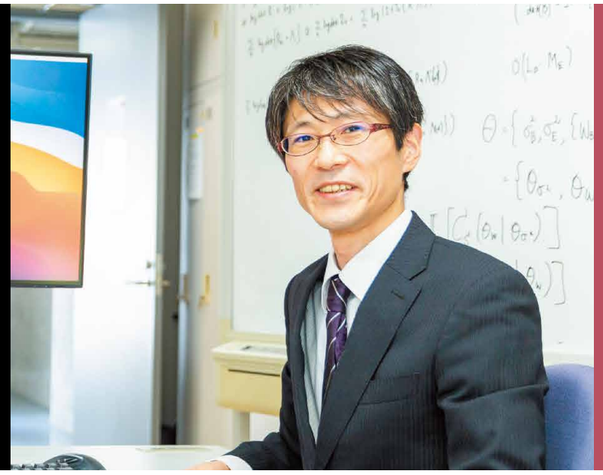
Society 5.0で求められる IoTインフラのセキュリティ向上へ。

029 Takano LABORATORY 高野研究室

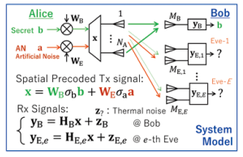
准教授・博士（情報科学） 高野　泰洋

■専門分野　情報通信工学
■立教大学理学部数学科卒業
■北陸先端科学技術大学院大学情報科学研究科
博士後期課程修了



APPEAL POINT アピールポイント

情報理論的安全性を活用することで、従来の暗号化技術の安全性向上を目指しています。現在の進捗状況は、理論構築と計算機シミュレーション検証です。今後、Software defined radio (SDR) による実証実験を計画しています。



情報理論に基づき、重み行列（$\mathbf{W}_B$,$\mathbf{W}_E$）の最適解を求める。

情報理論的安全性に着目し IoTインフラの安全性を向上

北海道の広大な土地を生かした農業、酪農業において、生産性および品質の向上を目指し、IoTシステムを活用したスマート農業、スマート酪農が始まりつつあります。システムを構成するセンサやドローンは、無線により情報通信を行います。例えばLoRaは、伝搬環境によっては、乾電池駆動で数十kmの通信を可能にします。しかし、手塩にかけて品種改良を重ねた種子が盗まれるという事件を見聞きします。無線システムの運用は通信エリアの拡大に応じて、第三者に傍受されたり、悪意のあるハッカーにシステムを乗っ取られる危険性も増加することを考慮すべきではないでしょうか。

このように、来るべきSociety 5.0において、重要な通信基盤として産業用IoTは強固なセキュリティが求められています。従来、通信の安全性は上位層における暗号化により保証されてきました。IoT機器向けの軽量暗号も研究が進められていますが、H/Wリソース制約のため、当該手法は従来に比べ安全性を損なう懸念があります。また、IoTシステムにおけるBlockchainの活用が期待されていますが、トラフィック容量の限られたIoTリンク間で逐次累積される分散台帳を共有することは困難です。

このような問題に対し、本研究室では情報理論に基づき、通信路の特徴と従来の暗号化を組み合わせ、要求された安全性を柔軟に達成するクロスレイヤ・セキュリティを検討し、IoTインフラの安全性向上を目指しています。

「無線マイニング」から 実用システムへの応用を

本研究室は通信の高速化、信頼性向上を目指したMIMO信号処理アルゴリズムを提案してきました。これら物理信号の解析技術を、自律的なIoTネットワークの構築へも応用していきたいと考えています。例えば、数百頭の家畜の放牧支援IoTシステムや、自動運転技術を支える自動車アドホックネットワークは、位置が変化しうる数百ノードからなるセンサネットワークです。信号解析結果を活用することで、数百ノードの自律的な通信制御や、通信障害の原因診断や障害予測を検討しています。

また、日常的に利用しているWi-FiやBluetoothの無線信号を解析することで、端末の位置情報だけでなく、部屋の在室人数や活動状況が推定できることが知られています。この技術は、プライバシーを損なう懸念のあるカメラ等を設置することなく、既存のWi-Fiルーターだけで高齢者や在宅患者の見守りサービスを実現します。

このように、本研究室は、統計的信号処理やAI技術を活用し、非線形性を持ちうる実サンプルデータから有意な情報採掘を行い、実用システムへの応用を目指します。

SEEDS

研究テーマ

情報理論的安全性を活用した セキュアな伝送法

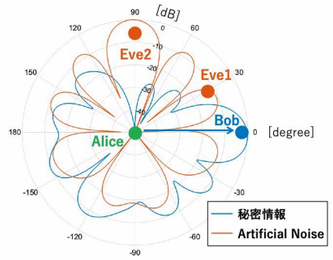
本研究室は、「情報理論的安全性に着目したIoT通信システム」をはじめ、「無線マイニングと応用システム」「大規模MIMO信号処理アルゴリズムの検討」を主なテーマとして研究に取り組んでいます。

ここでは、「情報理論的安全性に着目したIoT通信システム」の研究におけるセキュアな伝送法ついて、技術的な概要をご紹介します。

なおこの技術は、近距離の無線通信で使えるものと考えています。例えば、現在の交通系ICカードは改札の機器にかざし、その瞬間に無線通信をして決済しています。かざす範囲をもう少し伸ばした場合には、周りに電波が漏洩してしまいますが、この技術を使うと電波を制御でき、正しいユーザーのカードのみ通信を行って決済できるため、カードをポケットに入れたままでもうまく使うことができるかもしれません。また、車のスマートキーにも無線通信が使われていますが、この特性を悪用した車の盗難が起きています。この技術は、そうした犯罪の防止にもつながると考えられます。

セキュア伝送の概要

- 16本アンテナから重み付けした信号を送信することで正規の通信者Bobのみに Aliceから秘密情報を伝送する。
- しかし、送信重みを計算する空間信号処理は完全ではない。漏洩情報をマスクするため Artificial Noiseを同時に送信し、悪意のある第三者 (Eve1、Eve2) の受信を妨げる。
- 信号が届かないため、(Eve1、Eve2) はいかなる暗号解読手段でも秘密を解読できない。
- つまり、伝搬路の状況に応じて統計的に「情報理論的安全性」が保証される。

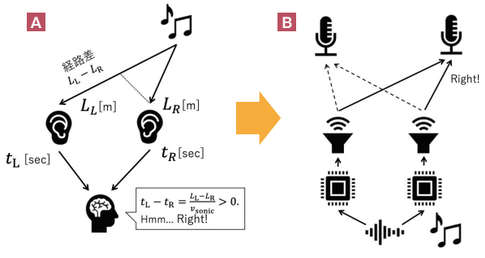


無線アンテナ電波放射パターンのシミュレーション図

空間信号処理の原理

[A図]
- 左右の耳へ到来する音波の経路差により生じる音のずれから到来方向を知覚する。

[B図]
- 逆処理を施した音を2つのスピーカーから鳴動させることで特定方向へ音を集中させることができる。
- 同様の原理で、複数アンテナと空間信号処理を活用し、電波の放射方向制御が可能になる。



電波を音に置き換えたイメージ図

企業等への提案

従来の暗号技術は、量子コンピュータが実用化される将来、安全性が揺らぎかねないといわれています。計算量的安全性と情報理論的安全性を兼ね備えたセキュアな伝送法を研究しています。

地域に向けてできること

組み込みシステムエンジニアの実務経験、および、これまでの教育経験を生かし、中高生や初心者向けのEdge AIやマイコンシステム講座等を提供していきたいと考えています。