IoT が拓く未来
2019 年度採択研究者

2021 年度
年次報告書

杉浦　慎哉

東京大学　生産技術研究所
准教授

IoT ワイヤレスネットワークセキュリティ

§1. 研究成果の概要

2021年度は、前年度から継続項目である(1)キーレス物理レイヤセキュリティを利用したワイヤレス通信の高度化と、(2)伝搬路キー生成による物理レイヤセキュリティの基礎検討の二項目から構成される。

(1) キーレス物理レイヤセキュリティ: 実用的セキュア通信を達成するために、知的反射面(Intelligent Reflecting Surface; IRS)を利用した伝搬路制御法を開発した。IRS は建物の壁面などに安価なパッシブメタサーフェスで構成され、入射した電磁波を制御できる性質を持ち、低コストを維持しながら仮想的な中継ノードして動作する。ここでは、情報の盗聴者が存在する環境を想定し、本研究で対象とするセキュア IoT ダウンリンク伝送に適した、低消演算量の IRS 制御手法を提案した。特に、ターゲットとなるセキュア送信レートを達成する QoS シナリオについて最適化アルゴリズムを開発した。さらに、本提案方式をマルチユーザ(IoT 端末)シナリオに拡張して一般化を行った。

(2) 伝搬路キー生成による物理レイヤセキュリティ:ワイヤレス伝搬路から正規の送受信者間でセキュアに秘密鍵を生成・共有を検討した。伝搬路に基づいて生成した秘密鍵はワンタイムパッドとして利用することで完全秘匿性を達成することができる。その他、軽量・低遅延の秘密鍵共有手法としても利用可能である。一般に物理レイヤキー生成は盗聴者へのキー漏洩を防ぐためにスモールスケールフェージングを仮定するが、同時に存在するラージスケールフェージングの状況によってはキー生成が非効率となる。これを克服するために、分散ノードシナリオにおける適応的キー生成リンク選択手法を考案した。

上記に関連する研究成果は、IEEE ジャーナル論文および国際会議論文に掲載または投稿され、一部は掲載されている。

【代表的な原著論文情報】

1) S. Sugiura, “Secrecy performance of eigendecomposition-based FTN signaling and NOFDM in quasi-static fading channel,” IEEE Transactions on Wireless Communications, vol. 20, no. 9, pp. 5872-5882, Sep. 2021.
2) T. Ishihara, S. Sugiura, and L. Hanzo “The evolution of faster-than-Nyquist signaling,” IEEE Access, vol. 9, pp. 86535-86564, June 2021.
3) Y. Kawai and S. Sugiura, “QoS-constrained energy-efficient beamforming and jamming with intelligent reflecting surface for secure multi-user downlink,” IEEE Transactions on Green Communications and Networking, vol. 6, no. 1, pp. 187-197, Mar. 2022
4) Y. Kawai and S. Sugiura, “QoS-constrained optimization of intelligent reflecting surface aided secure energy-efficient transmission,” IEEE Transactions on Vehicular Technology, vol. 70, no. 5, pp. 5137-5142, May 2021.