

IoT が拓く未来  
2019 年度採択研究者

2020 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

2020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、新規の項目である(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2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:時間領域の非直交時間領域多重化技術である faster-than-Nyquist (FTN) 信号伝送を利用した物理レイヤセキュリティにおいて、同じルートレイズドコサインフィルタの利用を仮定した場合、古典的なナイキスト基準限界よりも高い秘密容量の向上が可能であることを示した。さらに、このアイデアを周波数領域での非直交リソース配分技術である非直交マルチキャリア伝送に応用するためのアイデアについて基礎的な結果を得た。

(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・共有する方式を検討した。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。軽量・低遅延の秘密鍵共有手法としても利用可能である。課題であるキー生成レート向上のための研究を次年度に継続する。

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された。

### 【代表的な原著論文情報】

- 1) S. Osaki, T. Ishihara, and S. Sugiura, "Eigenvalue-decomposition-precoded ultra-dense non-orthogonal frequency-division multiplexing," *IEEE Transactions on Wireless Communications*, vol. 19, no. 12, pp. 8165-8178, Dec. 2020.
- 2) K. Masaki, T. Ishihara, and S. Sugiura, "Tradeoff between calculation precision and information rate in eigendecomposition-based faster-than-Nyquist signaling," *IEEE Access*, vol. 8, pp. 223461-223471, Dec. 2020.
- 3) J. Kochi, R. Nakai, and S. Sugiura, "Hybrid NOMA/OMA broadcasting-and-buffer-state-based relay selection," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 2, pp. 1618-1631, Feb. 2021.
- 4) S. Sugiura, Y. Kawai, T. Matsui, T. Lee, and H. Iizuka, "Joint beam and polarization forming of intelligent reflecting surfaces for wireless communications," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 2, pp. 1648-1657, Feb. 2021.
- 5) Y. Akiba, T. Ishihara, and S. Sugiura, "Variable-block-length joint channel estimation and data detection for spatial modulation over time-varying channels," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 11, pp. 13964-13969, Nov. 2020.