公開

研 究 終 了 報 告 書

「IoT ワイヤレスネットワークセキュリティ」

研究期間: 2019 年 10 月～2023 年 3 月
研 究 者: 杉浦 慎哉

1. 研究のねらい

本研究では情報理論的安全性の保証がない暗号技術だけに頼るのではなく、物理レイヤの信号処理技術によって、「膨大なIoTデバイスによって構成される分散ノード通信ネットワークのための、新しいネットワークセキュリティ基盤を提案する」ことを目的とする。特に、高い電力利用効率といった IoT に求められる通信要件を満たしながら、情報理論に裏付けられた高いセキュリティを実現する物理レイヤセキュリティ技術の開発を行う。このとき、情報理論的セキュリティ状態を維持するためのコストを現実的なものとするため、キーレス物理レイヤセキュリティに加えて、伝搬路に基づく物理レイヤキー生成方式の高度化を提案する。非直交リソース配分技術や知的反射面技術を併用することにより、さらなるセキュリティ向上を目指す。以上の研究開発より、IoTを利用した将来のアプリケーションを実現するための社会システム基盤確立に貢献する。なお、本研究は現在の暗号技術の延長線上にあるシステム開発ではなく、将来的に暗号のみに頼る情報システムが安全・安心ではなくなることを見据えることにより、科学技術上にインパクトをもたらすことを目指している。IoT ネットワークは無線・有線の両方をまたがることになるが、本研究では特にIoTセンサーデバイスから情報を取得する入口であり、セキュリティのボトルネックとなるワイヤレス通信部分を対象とする。

2. 研究成果

(1)概要

IoT ワイヤレス通信を対象として、物理レイヤセキュリティ高度化に関する基礎的な研究を実施した。物理レイヤセキュリティは、高電力効率や量子耐性の利点がある一方、実現性能が所与のワイヤレス伝搬路に依存するため安定した性能維持が困難であるという本質的な課題がある。そのような課題に対して、大きく分けて(A)暗号が不要なキーレス通信と、(B)伝搬路を情報源とした秘密鍵共有の二項目において新方式を提案した。

(A) 暗号が不要なキーレス通信では、物理層信号処理の観点から秘匿性能の向上を図った。特に、非直交信号処理を利用し、送受信間で固有値分解の基づく処理を実行することで、現実的な帯域制限フィルタを用いた場合に最大二倍までの秘匿レート性能向上が可能であることを示した。また、時々刻々変化するワイヤレス伝搬路を能動的に制御する手段として知的反射面 (intelligent reflecting surface: IRS) をダウンリンクシナリオに利用し、高電力効率かつ低演算量が可能な quality-of-service (QoS) プロトコルを提案した。本項目(A)で開発技術の利用シナリオとして、マルチユーザ間でのアクティブ盗聴者に対する秘匿性の実現、または、直進性の高いミリ波通信における受動的盗聴者への秘匿性実現に適している。

(B) 伝搬路を情報源とした秘密鍵共有では、変動するワイヤレス伝搬路により確率的に劣化する鍵共有性能の影響を克服するための手法を提案した。特に、ワイヤレス伝搬路の状況に応じて適応的に送信モードやリンクを選択する方式を提案した。さらに、仮想全二重通信と

いうコンセプトを利用することで、受動的盗聴者への雑音を増大させて鍵共有の秘匿性能を向上させた。本項目(B)の開発技術の利用シナリオとして、公開鍵暗号方式による鍵共有と比べて高い電力効率が期待できるため、長寿命 IoT 端末の通信に適している。

上記研究項目(A)、(B)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されている。また、関連する研究課題が複数採択されており、本課題実施内容の実用化に向けた継続検討が決まっている。

(2)詳細

研究テーマ A「キーレス物理レイヤセキュリティ」

キーレス物理レイヤセキュリティ方式では、従来の暗号方式で必要な鍵共有および暗号化(復号)が不要なため、原理的に高い電力効率を実現可能であり情報理論的安全性(量子耐性)が保証される。一方、秘匿レートや秘匿不稼働率などの基本的性能が盗聴者の伝搬路状況に依存するため、時間的空間的に変化する伝搬路の状況によらず高い品質を維持することが本質的に重要となる。ここでは、(1)非直交信号処理および (2) 知的反射面(intelligent reflecting surface: IRS)を利用したキーレス物理レイヤセキュリティ方式を提案した。

(1) 非直交信号処理による秘匿性向上**業績 1**

正規の送信元(Alice)、正規の受信者(Bob)、盗聴者(Eve)の三端末を考えたとき、秘密容量は Alice-Bob 間の正規チャネルのキャパシティ C_1 と Alice-Eve 間の盗聴者チャネルのキャパシティ C_2 の差である、$C_1 - C_2$ で与えられる。したがって、両キャパシティ C_1、C_2 が k 倍になれば、秘密容量をも k 倍に増やすことができる。そこで、時間領域の非直交リソース配分技術である faster-than-Nyquist (FTN) 信号伝送を利用した物理レイヤセキュリティの高性能化を提案した。提案方式では、送受信端末間で固有値分解に基づく事前信号処理を実行した上で、ナイキスト第一基準よりも小さいシンボル間隔で情報シンボルを送信する。レイズドコサインフィルタ等の実用的な帯域制限フィルタを利用する場合に、秘密容量の向上は

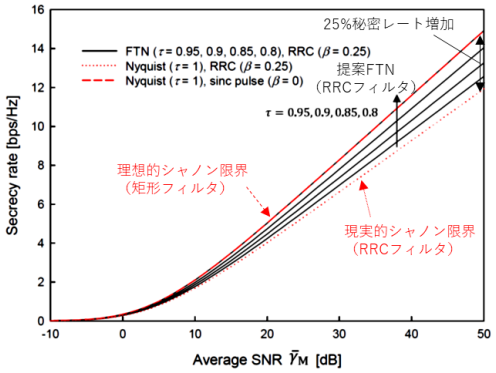

図 1. FTN による秘密レート向上

(1+β)倍であることを理論的に証明した(図1)。ここで、β (0≦β≦1)は帯域制限フィルタのロールオフファクタである。したがって、提案の FTN 信号伝送を用いることで秘密容量の増加は最大二倍となることがわかる。さらに本非直交伝送は時間領域だけではなく、周波数領域(サブキャリア次元)への拡張にも成功している。

(2) IRS 伝搬路制御による秘匿性向上**業績 2**

変動するワイヤレス伝搬路において実用的セキュア通信を達成するために、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、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、低消演算量の IRS 制御手法を提案した。特に、ターゲットとなる秘匿レートが与えられる QoS シナリオにおいて、基地局アンテナウェイトと IRS パラメータの繰り返し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。数値解析結果より、IRS を用いない場合と比べて、情報理論的安全性を達成しながら、大幅に消費電力を削減できることを確認した。なお、IRS は伝搬損の大きいミリ波通信の高性能化のために次世代規格に向けて広く研究開発が進められている。本項目での提案技術をミリ波帯通信へ適用する際、盗聴者が正規の受信者の近傍にいないことがわかっており、盗聴者の受信電力レベルが一定の閾値以下であることを前提とすれば、盗聴者チャネルが未知であってもキーレス物理レイヤセキュリティが実現できる。このため、受動的盗聴者が存在するシナリオへの適用が可能である。

研究テーマ B「伝搬路を情報源とした秘密鍵共有による物理レイヤセキュリティ」

ワイヤレス伝搬路を情報源として二端末間で鍵生成および鍵共有する手法の高度化について研究を実施した。現状広く利用されている共通鍵暗号方式による鍵共有と比べて、低消費電力・低遅延・量子耐性のメリットがあることが知られている。一方、伝搬路の状態に鍵共有性能（秘匿レート、鍵一致率等）が大きく影響を受けるため、時々刻々変動する伝搬路の状況によらず高い品質を維持する手法が重要となる。ここでは、以下に示す(3)適応モード選択による鍵共有の高性能化を実施した。

(3) 適応モードによる鍵共有の高性能化**業績 3**

正規の送受信者間で共有するワイヤレス伝搬路を情報源として、盗聴されることなく簡易に秘密鍵を生成・共有の高度化を実施した。一般にワイヤレス通信では伝搬路推定が情報伝送に必須であるため、鍵共有によって生じるオーバヘッドを最小限に抑えることができる。公開鍵暗号方式を利用した鍵共有と比べて、80 倍以上の電力効率を達成できる報告がある。一方、盗聴者への鍵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、同時に正規の伝搬路も時間的空間的に変化する伝搬路の影響を受けるため、安定的に鍵共有をすることが本質的な課題となる。そこで本研究項目ではこの課題を克服するために、複数ノードシナリオにおいて適応的にモード/リンク選択を行う手法を考案した。提案方式が従来方式と比べて安定的に鍵共有が可能であることを数値解析により確認した。なお、提案方式で共有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。一方、共有コストが低く漏洩しない秘密鍵として現状の暗号方式に利用することが可能であるため、適応シナリオの範囲は広いと考える。

3. 今後の展開

提案する物理レイヤセキュリティ技術固有の公開鍵暗号方式に対するメリットである量子耐性・低消費電力・低遅延が活かせるシナリオが重要であると考える。現状のシステムでは、

量子耐性は必須ではないため、即時導入のモチベーションは高くない。さらに、低消費電力・低遅延のメリットについては、ターゲットシナリオが特殊なものであることが想定されるため、標準化時の優先度も高くない。そのため、アプリケーションに応じて柔軟に性能限界・トレードオフをカスタマイズできる開発環境が不可欠である。また、物理レイヤセキュリティの技術的な課題も残るため引き続き研究開発が必要である。

これらを踏まえて、次世代 6G 以降の通信規格への導入を考えたとき、大手ベンダから与えられる標準フレームワークだけではなく、開発段階で物理レイヤセキュリティ技術導入のテスト実装・検証を繰り返すことができることが望ましい。そこで、柔軟にカスタマイズ可能なフレームワークの応用例として本研究課題で提案した方式（伝搬路に基づく鍵共有）の高度化と検証を進める予定である。

4. 自己評価

- 研究目的の達成状況

  本研究課題は、現在スタンダードとなっている暗号による情報秘匿技術の欠点を補完可能な物理レイヤセキュリティの実用化に重要な高度化を目的とした。特に、本質的な課題である伝搬路変動の影響、および、低レート上限に取り組んでいる。大きく分けて暗号を不要とする方式と暗号を生成する方式の二つを実施したが、両項目において秘匿性の向上を見込める新規技術の開発をすることができた。また、本研究課題開始後にいただいたアドバイスに基づいて、提案方式の簡易認証への応用についても提案し結果を得ることができた。上記成果は IEEE ジャーナルに掲載（一部は投稿中）となっている。以上により、全体として本研究の目的はおおむね達成できていると考える。

- 研究の進め方（研究実施体制及び研究費執行状況）

  研究実施体制：本課題について研究代表者が主体となって進める中で、主宰する研究室のメンバーである特任助教1名、特任研究員1名、博士課程学生2名、修士課程学生3名を含む若手研究者の協力のもと実施し、共著論文を多く出版できている。その意味で、若手研究者の育成に大きな貢献ができたと考える。また、計画時の予定通り、英サウサンプトン大学の共同研究者と議論をすることにより、理論的な研究をスピードアップすることができた。さらに、さきがけ研究者間の交流による研究体制を追加できた。特に、電子デバイスに強みを持つ名工大若土准教授、情報ネットワーク・アプリケーションに強みを持つ阪大猿渡准教授の二名と定期的にミーティングを行ってきている。これまでに共同で研究費獲得2件、学術論文掲載1件、学会発表1件の成果を得ている。また、研究費については全体としておおむね計画通りの執行ができた。

- 研究成果の科学技術及び社会・経済への波及効果

  本研究課題は、実用化がされていない基礎的かつ先行的な基礎技術がメインであり挑戦性が高く、本さきがけ研究後すぐに実装されることを想定していない。そのうえで、将来的に量子耐性および軽量を実現する物レイヤセキュリティについて高度化に向けて重要な成果を得ることができた。また、関連する理論的な枠組みを示すことができた。このことは、将来の量子コンピュータの発展・実用化により現状利用されている公開鍵暗号方式の盗聴リスクが重要な課題となる中、有効なセキュリティオプションとなりうるため、潜在的な波及効果は高いと考える。また、本研究の成果は、低消費電力・長寿命が重

要な IoT アプリケーションにも貢献できるものと考える。

本研究の継続として、カスタマイズ可能な無線通信フレームワークへの適用を検討している。すなわち、今後カスタマイズ適用例の一つとして物理レイヤセキュリティを組み込むことができれば、低消費電力が求められる IoT アプリケーションを含め、実用化への道が開けることが見込まれる。

5. 主な研究成果リスト

(1)代表的な論文(原著論文)発表

研究期間累積件数:18件

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.
非直交信号処理により物理レイヤセキュリティの性能上限を向上することを理論的に示した。特に、ワイヤレス通信における実用的な帯域制限を仮定した場合に、faster-than-Nyquist (FTN) 信号伝送と呼ばれる時間領域での非直交信号処理を用いることで最大二倍の秘匿容量を実現できることを示した。また、基本的な送受信機構成を提案し、数値解析により理論解析結果の妥当性を裏付けした。さらに、周波数領域での非直交信号処理によっても上記と同様の利得が得られることを示した。
2. 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.
電波の伝搬環境を能動的に制御可能な知的反射面(intelligent reflecting surface: IRS)を利用することでダウンリンクの物理レイヤセキュリティの性能を向上させる方式を提案した。特に、所望の送信レートに対して送信電力を最小化可能な最適化アルゴリズムを提案した。基地局アンテナウェイトと IRS 制御パラメータの最適値を効率的に求めるために、非凸最適化問題を二次錐計画問題とみなして交互に繰り返し計算を行うことで、従来方式と比べて大幅に演算量を削減した。
3. G. Srirutchataboon and S. Sugiura, "Secrecy performance of buffer-aided hybrid virtual full-duplex and half-duplex relay activation," IEEE Open Journal of Vehicular Technology, vol. 3, pp. 344-355, July 2022.
仮想全二重(virtual full-duplex: VFD)モードと半二重モードを融合した物理レイヤセキュリティに基づく中継伝送を提案した。物理レイヤセキュリティは伝搬路の影響を大きく受ける。本方式は、複数の中継モードを伝搬路の状況に応じて選択することで高い秘匿レートを実現することができる。また、中継ノード間でシームレスに共通パケットを共有できるように設計されており、VFD モードで生じる中継ノード間干渉の影響を逐次干渉キャンセルによって排除することが可能である。

(2)特許出願

研究期間全出願件数:0 件(特許公開前のものも含む)

(3)その他の成果(主要な学会発表、受賞、著作物、プレスリリース等)

1. 第 18 回日本学術振興会賞(受賞者:杉浦慎哉)、2022 年 2 月.
2. インタビュー記事、“Looking beyond 6G,” UTokyo-IIS Bulletin, vol. 9, Feb. 2022.
3. 関連テーマ研究費獲得 4 件:①JST 創発的研究支援事業(研究代表者:杉浦)、②科研費基盤(B)(研究代表者:名工大 若土准教授)、③科研費基盤(A)(研究代表者:阪大 猿渡准教授)、④NICT B5G 研究開発促進事業 (研究代表機関:シャープ)、⑤NICT B5G 研究開発促進事業 (研究代表機関: 日本電気)
4. G. Srirutchataboon and S. Sugiura, "Physical layer security of buffer-aided hybrid virtual full-duplex and half-duplex relay selection," in IEEE 95th Vehicular Technology Conference, Helsinki, Finland, 19-22 June 2022.