様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　６ 年　 ６ 月　 ７ 日現在

機関番号：３２７０２
研究種目：若手研究
研究期間：2021～2023
課題番号：２１Ｋ１７７３８

研究課題名（和文）有歪み復号転送を用いた非信頼中継ネットワーク物理層セキュリティに関する研究

研究課題名（英文）Physical Layer Security of Untrusted Relay Networks with Lossy Decode-and-forward

研究代表者

謇　申（Qian, Shen）

神奈川大学・情報学部・助教

研究者番号：８０８６８３３１

交付決定額（研究期間全体）：（直接経費）　　2,300,000円

研究成果の概要（和文）：本研究課題は、(1) 有歪み復号転送プロトコルを用いた非信頼中継ネットワークにおいて、秘匿性と信頼性のトレードオフを解析し、Slepian-Wolf符号化領域とマルチアクセス通信路符号化領域の交差で上界条件を決定した。(2) 非信頼中継ネットワークにおけるショートパケット伝送の信頼性と安全性パフォーマンスを解析し、最大のreliable-and-secure確率を得る条件を明らかにした。(3) Alamouti時空間ブロック符号を用いた物理層セキュリティ性能を検証し、送信電力と中継電力の最適な配分を明らかにした。

研究成果の学術的意義や社会的意義
本研究課題は、情報理論に基づく非信頼中継ネットワークの安全性と信頼性に関する新たな解析手法を提供し、特に有歪み復号転送プロトコルの適用による秘匿性-信頼性トレードオフの最適化に貢献した。次世代通信ネットワークにおけるデータ伝送の安全性と信頼性が向上および、IoTや6Gなどの分野において重要な役割を果たす。より安全で信頼性の高い通信ネットワークの構築に寄与し、情報漏洩や通信障害のリスクを軽減することで、安心・安全な社会の実現に貢献する。

研究成果の概要（英文）：(1) The trade-off between secrecy and reliability was analyzed in untrusted relay networks based on lossy decode-and-forward protocol. Using formal methods from information theory, upper bound conditions for lossless coding rates were determined by intersecting Slepian-Wolf coding regions with multi-access channel coding regions. This analysis led to the calculation of secrecy outage probabilities. (2) Short packet transmissions' reliability and security performance in unreliable relay networks were analyzed. The study confirmed that the highest reliable-and-secure probability (RSP) is achieved when the contributions of source-to-relay and relay-to-destination links are balanced. (3) The physical layer security performance in untrusted relay networks using Alamouti space-time block codes (STBC) was examined. The transmission signal's resistance to potential attacks was evaluated. The optimal power allocation for achieving peak RSP was revealed under real-world constraints.

研究分野：情報ネットワーク

キーワード：物理層セキュリティ　非信頼中継　reliable-and-secure確率　情報相関　有歪み復号転送　情報源・通信路結合符号化

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

(1) 無線通信における盗聴対策としては、正規局間での電波伝搬特性などを利用して生成した情報を共有する秘密鍵共有方式と、正規局-盗聴局間の受信特性の差をつける電波伝送方式が検討されてきた。これら二つの方式はともに正規局と盗聴局を明確に区別しうることを前提においている。今後増加していくと見込まれる大規模協調無線通信ネットワークにおいて、介在する中継局は情報伝送のヘルパーとして、ネットワーク通信の信頼性を高める一方で、ネットワークセキュリティに脅威する潜在的な盗聴者となりうる。それ故、無線協調通信システムの設計において、強固なセキュリティを確保するためには、ネットワーク外部からの盗聴を防ぐことに加えて、ネットワーク内にある非信頼中継が情報転送に対してセキュリティ上の脅威になりうることを抑制する必要がある。

(2) 物理層セキュリティの理論的基礎はシャノンの完全秘匿性理論に基づく。協調通信ネットワークの物理層セキュリティーに関する研究は基本的に中継局で情報を完全に復元できる（無歪み）と想定しているが、中継局は情報伝送のヘルパーとして必ずしも情報を完全に復元する必要はない。発信局と中継局間の情報を考慮する場合、中継局で復号する情報に一部の歪みを許容した場合、達成可能な情報レート領域（source coding with side information レート領域）が、中継局で情報を完全復元する無歪みレート領域（Slepian-Wolf レート領域）より大きいことが知られている。

２．研究の目的

本研究課題の研究代表者は、有歪み中継経路を介して受信される信号列の間の相関を取り込んだ効率的な復号アルゴリズムの開発について研究を進めてきた。その過程で中継局において情報を完全に復元する必要がないことを利用し、非信頼中継からの盗聴を防ぐことの可能性に気づき、本計画を発案した。本研究では、無線通信ネットワーク内部の非信頼中継局（untrusted relay）を介した電波の傍受・盗聴や不正アクセスを防ぐため、有歪み復号転送の概念に立脚した物理層セキュリティの特性指標である秘密保持容量を検討し、送信情報の秘匿性を保証しながら信頼できる無線協調伝送技術の開発を目指す。

３．研究の方法

(1)　本研究課題は、有歪み復号転送プロトコルにより非信頼中継ネットワークでの盗聴を防ぐため、物理層セキュリティ対策を検討する。従来の無歪み復号転送プロトコルでは伝送ネットワーク信頼性の向上限界があるという課題に対して、非信頼中継において有歪み復号転送プロトコルを提案し、ネットワーク情報理論に基づいて、秘密保持容量、秘匿アウテージ確率などのパフォーマンス評価関数を明らかにする。また、パフォーマンス評価関数を用いて、各伝送局間に最適な伝送電力の割り当ておよび、最適な中継局選択フレームワークを構築することで、非信頼中継の情報伝送セキュリティにおいて有歪み復号転送の役割を明らかにする。

(2)　非信頼中継システムにおいて、達成可能な符号レートを source coding with side information の定理で計算し、モンテカルロシミュレーションで理論結果を検証する。秘密保持容量、秘匿アウテージ確率を明確することにより、機密性と信頼性のそれぞれを目的関数とするトレードオフ関数である Reliable-and-secure 確率を確立する。秘密保持容量の計算は、従来の無歪み復号転送に基づく中継ネットワークの計算手法を直接流用できないため、直交多元接続と前提した形式化分析に基づいて、秘匿性と信頼性のトレードオフ評価関数を導き出す。

４．研究成果

(1)　有歪み復号転送プロトコルに基づく非信頼中継ネットワークにおいて、盗聴を防止するために情報理論的に安全性を解析するため、非直交多元接続アップリンクにおける相関がある情報源コーディング問題を検討した。3 ノード非信頼中継ネットワークにおいて秘匿アウテージ確率を解析するため、ネットワーク要素を情報理論の形式手法を用いて形式的モデルで記述した。ロスレス符号化レートを達成可能な上界条件を Slepian-Wolf 符号化領域とマルチアクセス通信路符号化領域の交差で決定し、アウテージ確率を計算した。研究成果を国際会議 IEEE WCNC 2022 に発表された。また、発信局の情報源のみを復元するに着目した符号化レートを達成可能な上界条件を source coding with side information 符号化領域とマルチアクセス通信路符号化領域の交差決定し、モンテカルロシミュレーションで理論結果を検証した。研究成果を学術誌 IET Communications に出版された。また、有歪み復号転送プロトコルを用いた 2 つの非信頼中継があるダイヤモンドネットワークにおいて、直交多元接続と前提した形式化分析に基づいて秘匿性-信頼性トレードオフ関係を表す Reliable-and-secure 確率を計算した。機密性(security)と信頼性(reliability)のそれぞれを目的関数とするトレードオフ関数を確立されることによって、

秘匿性と信頼性のトレードオフ評価関数を導き出した。研究成果を国際会議 IEEE ISNCC 2022 に発表された。

(2) 非信頼中継ネットワークにおけるショートパッケージ伝送の信頼性と安全性パフォーマンスを解析した。物理層のセキュリティ性を強化するために、有歪み復号転送プロトコルを考慮した。ショートパケット通信の特徴に基づき、信頼性と安全性を示す reliable-and-secure 確率(RSP)を性能指標としてパフォーマンス評価した。ブロック長が有限の場合、発信局-中継局リンクと中継局-宛先局リンクの寄与が釣り合う限り、最大の RSP 確率が得られることが確認できた。この研究成果は国際会議 IEEE CCNC 2023 に発表された。また、ダイヤモンド型非信頼中継ネットワークにおけるショートパッケージ伝送の信頼性と安全性を解析した。2 つの非信頼中継には、有歪み復号転送プロトコルを利用する。信頼性と安全性を考慮している RSP を計算した。発信局から 2 つの非信頼中継への伝送と 2 つの非信頼中継から宛先局先への伝送の寄与がバランスしたときに最大の RSP が得られることが示された。研究成果は 1 編の学術雑誌論文として IEEE Access に発表された。さらに、2 つの非信頼中継を持つダイヤモンド型ネットワークにおいて信頼性と安全性を解析した。ただし、宛先局から送信される協調妨害信号は、送信元からのオリジナルメッセージを解読するためのサイド情報として利用される。協調妨害信号のパワーが強くなると、優れた RSP 性能が達成できることがわかった。研究成果を学術雑誌論文 IEICE ComEX および 2023IEICE 総合大会に報告された。

(3) Alamouti 時空間ブロック符号(STBC)を用いた非信頼中継ネットワークにおける物理層のセキュリティ性能を検証した。Alamouti STBC が提供する時空間ダイバーシティを活用することにより、有歪み復号転送非信頼中継ネットワークにおいて、潜在的な攻撃に対する送信信号の耐性を検証した。Reliable-and-secure 確率(RSP)を用いて、送信情報が非信頼中継によって解読されないまま、宛先での復号が可能であることを情報理論的に確認した。Alamouti STBC を適用する非信頼中継ネットワークにおいて、送信元の送信電力と中継局の送信電力の寄与が均衡することで、RSP のピークが達成されていることがわかった。研究成果を国際会議 IEICE ICETC 2023 に報告された。また、Alamouti 時空間ブロック符号(STBC)を利用した非信頼中継ネットワークにおける電力配分についても検討した。非信頼中継からの潜在的な侵害に対する送信信号の安全性を強化するため、Alamouti STBC が提供する時空間ダイバーシティを利用している。RSP の解析式を利用した実世界の制約を反映した総送信電力制約の下で、中継位置を固定した最適な電力割り当てを探索した。スペクトル効率が高いシナリオでは、送信電力の大部分を非信頼中継に割り当てるべきであることを明らかにしている。この研究成果は国際会議論文 IEEE ICCCN 2024 に発表する。さらに、空中の送信元から水中の宛先の送信に利用される 2 つの非信頼中継があるトランスミッション方式を検討した。中継局の復号誤りを許容する特性を活用することにより、非信頼中継ベースのネットワークにおける信頼性の高いかつ安全なデータ伝送が保証されている。非信頼中継による情報の漏れがないと同時に、水中の宛先が空中の送信元からメッセージを正常に取得できる確率を測定した。空中の送信元と水面の非信頼中継の間で電力配分の調整を行うことにより、 最適な RSP を達成できることを示唆している。研究成果を国際会議 ACM WUWNet 2024 に報告された。

５．主な発表論文等

〔雑誌論文〕　計3件（うち査読付論文　3件／うち国際共著　1件／うちオープンアクセス　3件）

１．著者名 Qian Shen	４．巻 12
２．論文標題 Diamond untrusted relay networks with cooperative jamming: physical layer security perspective	５．発行年 2023年
３．雑誌名 IEICE Communications Express	６．最初と最後の頁 169～174
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/comex.2022XBL0151	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

１．著者名 Qian Shen	４．巻 11
２．論文標題 Reliable and Secure Short-Packet Communications in Untrusted Diamond Relay Networks	５．発行年 2023年
３．雑誌名 IEEE Access	６．最初と最後の頁 24686～24695
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/ACCESS.2023.3255881	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

１．著者名 Shen Qian, Jiguang He, Xiaobo Zhou, Takamasa Imai, Tad Matrumoto	４．巻 －
２．論文標題 Performance Analysis of One-Source-with-One-Helper Transmission over Shadowed κ-μ Fading Multiple Access Channels	５．発行年 2022年
３．雑誌名 IET Communications	６．最初と最後の頁 －
掲載論文のDOI（デジタルオブジェクト識別子） 10.1049/cmu2.12402	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 該当する

〔学会発表〕　計7件（うち招待講演　0件／うち国際学会　6件）

１．発表者名 Shen Qian and Meng Cheng
２．発表標題 Optimal Power Allocation for Secure Transmission in Untrusted Relay Networks with Alamouti Space-Time Block Coding
３．学会等名 The International Conference on Computer Communications and Networks (ICCCN)（国際学会）
４．発表年 2024年

１．発表者名
Shen Qian and Xiaobo Zhou

２．発表標題
Physical Layer Security in Untrusted Relay Networks with Alamouti Space-Time Block Coding

３．学会等名
International Conference on Emerging Technologies for Communications (ICETC)（国際学会）

４．発表年
2023年

１．発表者名
Shen Qian and Xiaobo Zhou

２．発表標題
Physical Layer Security in Air-to-Underwater Untrusted Relay Networks

３．学会等名
The International Conference on Underwater Networks & Systems (WUWNet)（国際学会）

４．発表年
2023年

１．発表者名
Shen Qian

２．発表標題
Diamond Untrusted Relay Networks with Friendly Jamming: Physical Layer Security Perspective

３．学会等名
IEICE総合大会

４．発表年
2023年

１．発表者名
Qian Shen

２．発表標題
Physical Layer Security in Untrusted Lossy Decode-and-Forward Relay Networks with Finite Blocklength

３．学会等名
IEEE Consumer Communications & Networking Conference（国際学会）

４．発表年
2023年

１．発表者名
Shen Qian

２．発表標題
Outage Analysis for Correlated Sources Coding over NOMA in Shadowed κ-μ Fading

３．学会等名
IEEE Wireless Communications and Networking Conference (WCNC)（国際学会）

４．発表年
2022年

１．発表者名
Shen Qian

２．発表標題
Physical Layer Security in Untrusted Diamond Relay Networks With Imperfect Source-Relay Links

３．学会等名
International Symposium on Networks, Computers and Communications (ISNCC)（国際学会）

４．発表年
2022年

〔図書〕　計0件

〔産業財産権〕

〔その他〕

神奈川大学 研究者情報
https://kenkyu.kanagawa-u.ac.jp/kuhp/KgApp?kyoinId=ymbgyygdggy

６．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考

７．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

８．本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関