機械学習を活用した非信頼中継ネットワークの適応型物理層セキュリティ設計

研究代表者　鵞　申　東京都市大学　メディア情報学部　情報システム学科 准教授

1 はじめに

近年、Beyond 5G および第 6 世代移動通信システム（Sixth-Generation: 6G）に向けて、無線通信ネットワークは高密度化、低遅延化、多接続化、分散化の方向に急速に発展している。スマートフォン、IoT（Internet of Things）機器、車載端末、センサ、ロボット、無人航空機など、多様な端末が無線ネットワークに接続されることで、通信容量や接続数だけでなく、通信の安全性、プライバシー保護、リアルタイム制御の重要性も高まっている。従来、通信の安全性は主として上位層の暗号技術により確保されてきた。しかし、IoT 端末や移動端末のように計算資源や電力に制約がある環境、または短時間で頻繁に通信状態が変化する環境では、暗号処理や鍵管理だけに依存する安全対策には限界がある。そのため、無線チャネルの雑音、フェージング、干渉、空間的な相関の違いを利用して秘匿性を高める物理層セキュリティ（Physical-Layer Security: PLS）が、暗号技術を補完する有力な安全対策として注目されている。

特に本研究で対象とする非信頼中継ネットワークでは、中継ノードが通信を支援する一方で、内部盗聴者として機能する可能性がある。通常の外部盗聴者モデルでは、盗聴者は正規通信経路の外側に存在し、正規受信者よりも劣悪なチャネル条件を持つことが仮定される場合が多い。これに対して、非信頼中継ネットワークでは、中継ノードが送信元からの信号を受信し、それを宛先に転送するため、通信プロトコル上は正規の協力ノードでありながら、同時に機密情報を復号し得る立場にある。このような内部盗聴リスクは、単純な外部盗聴者対策よりも深刻であり、通信品質と秘匿性を同時に満たす送信機会の選択、中継ノードの選択、送信電力の制御、チャネル状態の予測が重要となる。

一方、機械学習（Machine Learning: ML）は、複雑な無線環境の特徴をデータから抽出し、従来の閉形式解析や逐次最適化では扱いにくい動的環境に適応するための手段として期待されている。とくに、時系列的に変化するチャネル状態情報（Channel State Information: CSI）の予測、端末間のトポロジーを考慮した状態表現、分散ノード間での協調学習、強化学習に基づく制御方策の獲得は、非信頼中継ネットワークにおけるリアルタイムな PLS 設計に適している。そこで本研究では、非信頼中継ネットワークにおける物理層セキュリティの強化を目的として、機械学習を用いたインテリジェントで適応性のあるセキュリティアルゴリズムを設計した。具体的には、1）無線チャネルの時間変動を予測し、信頼性と秘匿性を同時に満たす通信機会を選択するためのチャネル予測手法を比較評価した。2）再構成可能知的反射面（Reconfigurable Intelligent Surface: RIS）を備えた非信頼中継ネットワークに対して、グラフニューラルネットワーク（Graph Neural Network: GNN）、深層強化学習（Deep Reinforcement Learning: DRL）、連合学習（Federated Learning: FL）を組み合わせた安全制御手法を検討した。

本報告書では、まず本研究の目的と技術的背景を整理し、次に非信頼中継ネットワークにおけるチャネル予測型 PLS 設計、さらに RIS 支援非信頼中継ネットワークにおける GNN 支援連合深層強化学習の方法を説明する。その後、シミュレーション評価に基づく結果を示し、最後に研究成果、受賞、今後の課題について述べる。

2 研究の目的

本研究の目的は、非信頼中継ネットワークにおいて、チャネル変動やネットワーク状態の変化に応じて動作する適応型物理層セキュリティ手法を構築することである。従来の PLS 研究では、瞬時 CSI が完全に既知であること、盗聴者の位置やチャネルが正確に把握できること、またはネットワーク構造が静的であることを仮定する場合が多かった。しかし、実際の無線ネットワークでは、端末移動、フェージング、トラフィック変動、RIS 制御遅延、CSI 取得誤差などにより、通信環境は時間的に変化する。また、非信頼中継ノードは通信を支援するために信号を受信する必要があるため、単に中継リンクの品質を高めるだけでは秘匿性を保証できない。正規宛先が復号可能であり、非信頼中継が復号困難となるようなチャネル状態や制御方策を選

公益財団法人電気通信普及財団
研究調査助成報告書　第41号　2026年度

ぶ必要がある。

この目的を達成するため、本研究では、主に三つの観点から検討を行った。まず、チャネル状態の予測に基づく送信判断である。無線チャネルはランダムに変動するが、その変動には時間的相関や状態遷移構造が含まれる場合がある。過去の CSI や信号対雑音比（Signal-to-Noise Ratio: SNR）の時系列から将来のチャネル状態を予測できれば、正規宛先にとって有利で、非信頼中継にとって不利な通信機会を選択できる可能性がある。次に、単なる予測精度だけでなく、通信の信頼性と秘匿性を同時に評価する指標を用いることである。予測誤差が小さくても、その予測が安全な送信判断に寄与しなければ PLS の観点では十分ではない。そこで本研究では、Reliable-and-Secure Probability（RSP）を用い、正規宛先が信頼性条件を満たし、非信頼中継が秘匿性条件を破らない確率を評価した。さらに、RIS、GNN、DRL、FL を組み合わせることで、複数中継ノードを含む複雑なネットワークにおいて、トポロジー、CSI、制御変数を統合的に扱うことである。

以上を踏まえ、本研究では、(1) 機械学習を用いたチャネル予測と RSP 評価、(2) RIS 支援非信頼中継ネットワークのモデル化、(3) GNN によるトポロジー認識型状態表現、(4) DRL による中継選択、送信電力配分、RIS 位相制御の統合最適化、(5) FL によるローカル CSI を直接共有しない分散学習の可能性を検討した。

3 研究方法

3-1 非信頼中継ネットワークにおけるチャネル予測

本研究の第一段階では、非信頼中継ネットワークにおけるチャネル予測手法を比較し、予測結果が PLS 性能に与える影響を評価した。対象とするネットワークは、単一の送信元、単一の宛先、複数の非信頼中継ノードから構成される。中継ノードはプロトコルに従って信号を転送するが、同時に機密情報を復号しようとする可能性がある。このような環境では、正規宛先のチャネル品質が十分に高く、中継ノードのチャネル品質が十分に低いタイミングで送信を行うことが望ましい。

チャネル予測手法として、自己回帰モデル（Autoregressive model: AR）、再帰型ニューラルネットワーク（Recurrent Neural Network: RNN）、長短期記憶ネットワーク（Long Short-Term Memory: LSTM）、隠れマルコフモデル（Hidden Markov Model: HMM）を比較した。AR モデルは線形時系列モデルであり、実装が容易で計算量が小さいという利点を持つが、複雑な非線形変動や状態遷移を表現する能力には限界がある。RNN は過去の入力系列を内部状態に保持し、時系列データの予測に利用できる。LSTM は RNN の一種であり、入力ゲート、忘却ゲート、出力ゲートを用いて長期依存性を扱うことができるため、フェージングチャネルのように過去の状態が将来に影響するデータに適している。HMM は、観測されるチャネル状態の背後に隠れ状態が存在すると仮定し、良好状態と不良状態などの離散的な状態遷移を表現する確率モデルである。

予測精度の評価には平均二乗誤差（Mean Squared Error: MSE）を用いた。MSE は予測値と真値の差の二乗平均であり、値が小さいほど予測精度が高いことを意味する。ただし、PLS において重要なのは予測誤差の低さだけではない。正規宛先が復号可能であっても、非信頼中継も復号できてしまえば秘匿性は失われる。そこで本研究では、通信の信頼性と秘匿性を同時に反映する指標として RSP を導入した。RSP は、正規宛先の SNR が所定の信頼性閾値を上回り、同時に非信頼中継の SNR が秘匿性上の閾値を下回る確率として評価される。これにより、予測モデルが単にチャネルを正確に予測するだけでなく、安全な送信判断にどの程度貢献するかを定量的に評価できる。

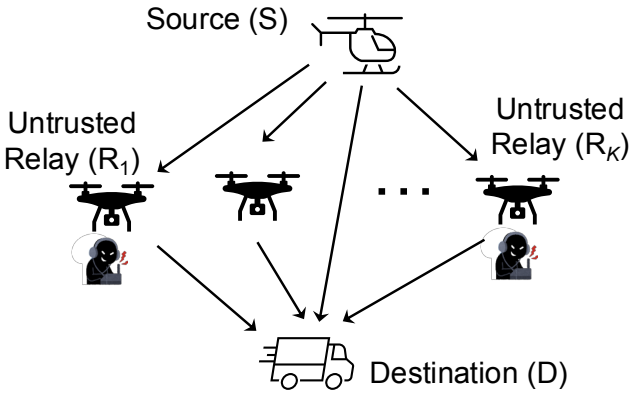

図 1　非信頼中継ネットワークの基本モデル

3-2 チャネル予測に基づく安全送信判断

チャネル予測の評価では、Rayleigh フェージングチャネルを想定し、複数の SNR 条件の下で、各予測手法の MSE と RSP を比較した。送信元から宛先、送信元から非信頼中継へのチャネルは時間とともに変動するものとし、過去のチャネルサンプルを用いて次時刻のチャネル状態を予測する。RNN および LSTM では、連続する複数サンプルを入力系列として与え、将来のチャネル値を予測した。HMM では、チャネル状態を良好状態と不良状態などの離散状態に分類し、状態遷移確率に基づいて将来状態を推定した。

送信判断の考え方は次の通りである。予測された宛先側チャネルが所定の品質を満たし、同時に非信頼中継側チャネルが復号に不十分である場合、その時刻を安全かつ信頼可能な送信機会とみなす。逆に、宛先側チャネルが低品質である場合には信頼性が不足し、非信頼中継側チャネルが高品質である場合には秘匿性が不足するため、送信を避けるべきである。これにより、本研究では、チャネル予測を単なる通信品質向上の手段ではなく、リアルタイム適応を想定した制御に利用する枠組みとして位置づけた。

表 1　チャネル予測シミュレーション条件

項目	設定値・内容
チャネルモデル	Rayleigh フェージングチャネル
サンプル数	1000 サンプル
学習データ比率	0.8（残り 20%をテストデータとして使用）
時間窓	5 サンプル（RNN および LSTM の入力系列長）
信頼性・秘匿性判定閾値	5 dB
平均 SNR 範囲	0, 1, 2, …, 20 dB
オフセット	宛先局と非信頼中継局の平均 SNR 差を 5 dB と設定
AR モデル	1 次自己回帰モデル
HMM モデル	2 状態モデル（良好状態・不良状態を K-means により近似）
RNN モデル	隠れユニット数 10、50 エポック、バッチサイズ 16
LSTM モデル	隠れユニット数 10、50 エポック、バッチサイズ 16
評価指標	平均二乗誤差（Mean Squared Error: MSE）および RSP

3-3 RIS 支援非信頼中継ネットワークのモデル化

本研究の第二段階では、RIS を備えた非信頼中継ネットワークにおいて、GNN 支援連合深層強化学習による適応型 PLS 制御を検討した。RIS は多数の受動反射素子から構成され、各素子の位相を制御することで、電波伝搬環境をプログラム可能にする技術である。RIS を適切に制御すれば、宛先に対しては建設的合成を生じさせ、非信頼中継や外部盗聴者に対しては信号を弱めるような伝搬環境を構成できる。したがって、RIS は 6G 時代の低消費電力かつ柔軟な PLS 技術として有望である。

対象とするネットワークは、単一の送信元 S、単一の宛先 D、K 個の非信頼中継ノード、L 素子からなる RIS、および外部盗聴者 E から構成される。各中継ノードは半二重で動作し、送信元から受信した信号を宛先へ転送する。一方で、非信頼中継ノードは内部盗聴者として機密情報を復号しようとする可能性がある。RIS は送信元、中継、宛先、外部盗聴者の間の有効チャネルを変化させるため、中継選択、送信電力配分、RIS 位相制御は相互に強く結合する。したがって、この問題は離散変数と連続変数を含む混合最適化問題となり、従来の全探索や反復最適化では、ノード数や RIS 素子数が増加するにつれて計算量が急増する。

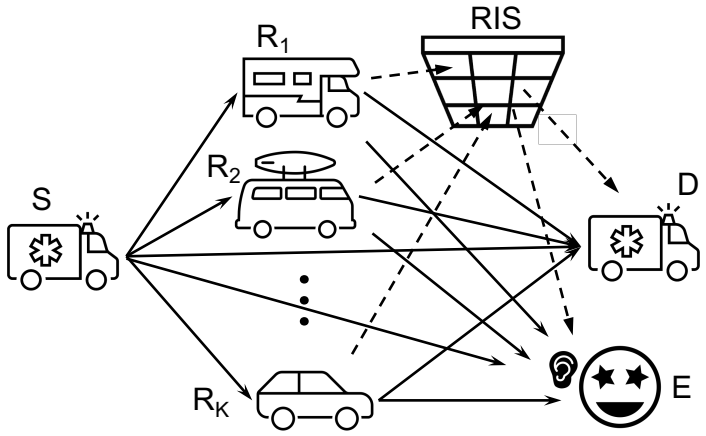

図 2　RIS 支援非信頼中継ネットワーク

3-4 GNN によるトポロジー認識型状態表現

複数中継ノードを含む無線ネットワークでは、各ノードのチャネル状態だけでなく、ノード間の関係、距離、伝搬経路、RIS を介した反射リンクなどの構造的情報が性能に影響する。このような構造を単純なベクトルとして扱うと、ノード数の変化やリンク間の相互作用を十分に表現できない。そこで本研究では、ネットワークをグラフとして表現し、GNN を用いてトポロジーと CSI を反映した状態表現を獲得した。

グラフのノード集合には、送信元、中継ノード、宛先、RIS を含める。エッジには、送信元から中継、中継から宛先、RIS を介したリンクなど、通信に関わる有効チャネル情報を対応させる。各ノード特徴量には、チャネル利得、SNR、位置情報に関する特徴、または RIS との関係を表す特徴を含めることができる。GNN は、近傍ノードからの情報集約を繰り返すことで、各ノードの局所的な情報とネットワーク全体の構造を反映した埋め込み表現を生成する。この埋め込みを DRL エージェントの状態入力として用いることで、単純な固定次元ベクトル入力よりも、トポロジー変化に対して柔軟な制御が可能となる。

3-5 DRL による中継選択、電力配分、RIS 位相制御

GNN により得られた状態表現は、DRL エージェントに入力される。本研究では、actor-critic 型の DRL 構造を想定し、actor が制御行動を生成し、critic がその行動の価値を評価する。行動には、選択する中継ノード、送信元と中継ノードへの電力配分、RIS の位相設定が含まれる。報酬は秘匿通信性能に基づいて設計され、たとえば宛先での受信性能が高く、非信頼中継および外部盗聴者での受信性能が低い場合に高い値を与える。これにより、エージェントは反復的な学習を通じて、秘匿容量を改善する制御方策を獲得する。

この問題では、中継選択は離散制御、電力配分は連続制御、RIS 位相設定は多数の離散または連続パラメータを含む制御である。そのため、従来の単純な最適化問題よりも複雑であり、全探索では候補数が急速に増加する。本研究で採用した GNN 支援 DRL は、ネットワーク構造を反映したコンパクトな状態表現を用いることで、このような高次元かつ混合的な制御問題に対応することを目的とする。

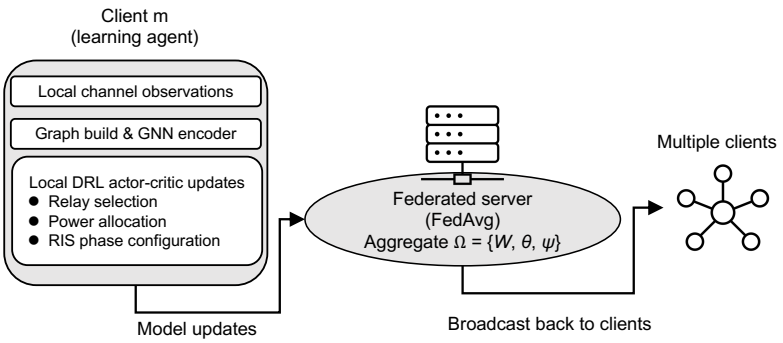

図 3　GNN 支援 FedDRL による制御処理の概念図

3-6 FL によるプライバシー保護型分散学習

非信頼中継ネットワークや RIS 支援ネットワークでは、各端末や各基地局が保持する CSI、通信履歴、トラフィック特徴量は、場所やユーザ行動に関する情報を含む可能性がある。これらの生データを中央サーバに集約すると、プライバシー保護や通信オーバーヘッドの観点で問題が生じる。そこで本研究では、FL を用いて、各端末や分散ノードがローカル CSI を直接共有せずにモデルを協調学習する枠組みを検討した。

FL では、各クライアントが自身のローカルデータを用いて GNN エンコーダおよび DRL エージェントのパラメータを更新し、そのモデル更新量のみをサーバに送信する。サーバは複数クライアントから受け取ったモデル更新を集約し、更新されたグローバルモデルを各クライアントに配布する。この方式により、ローカル CSI や通信データを直接外部に出すことなく、複数環境で得られた学習経験を共有できる。非信頼中継ネットワークにおいては、CSI そのものが機密性を持つ可能性があるため、FL は PLS 制御の学習基盤として重要である。

4 研究結果

4-1 チャネル予測精度の評価

第一の成果として、AR、RNN、LSTM、HMM の各手法を用いてチャネル状態を予測し、MSE により予測精度を比較した。その結果、単純な線形モデルである AR はチャネル変動の複雑な時間構造を十分に捉えられず、他の手法に比べて大きな予測誤差を示した。一方、RNN と LSTM は時系列データの依存関係を利用することで、AR よりも高い予測精度を示した。特に、HMM はチャネル状態の遷移構造を捉えることで最も低い MSE を示し、RNN および LSTM も AR に比べて高い予測精度を示した。また、HMM はチャネル状態を良好状態と不良状態などの離散状態として表現することで、状態遷移構造を効果的に捉え、低い MSE を示した。

この結果は、非信頼中継ネットワークにおける適応型 PLS 設計において、機械学習に基づくチャネル予測が有効であることを示している。とくに、チャネル状態に潜在的な状態遷移構造が存在する場合には HMM が有効であり、連続的な時系列パターンを学習する場合には RNN や LSTM が有効である。AR は計算量が小さいため低複雑度の基準手法として有用であるが、セキュリティ判断の精度を高めるためには、より高度な時系列モデルが望ましい。

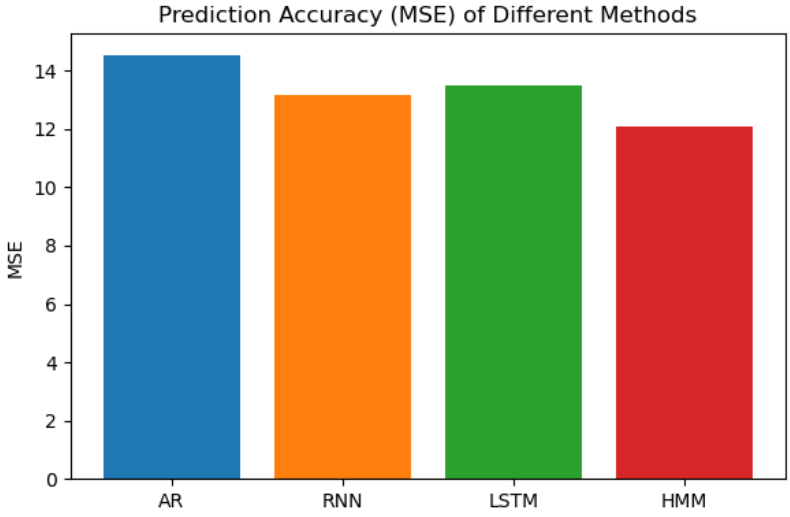

図 4　MSE によるチャネル予測精度比較

4-2 RSP による信頼性・秘匿性の同時評価

次に、各チャネル予測手法が PLS 性能に与える影響を RSP により評価した。RSP は、正規宛先が信頼性条件を満たし、非信頼中継が秘匿性を破らない条件を同時に満たす確率である。シミュレーションでは、平均 SNR を変化させながら RSP を評価した。その結果、RSP は極端に低い SNR および極端に高い SNR では低く、中程度の SNR 領域で最大となる傾向が確認された。

低 SNR 領域では、正規宛先のチャネル品質が十分でないため、宛先が復号に失敗する可能性が高く、信頼性条件を満たす送信機会が少ない。そのため、秘匿性が保たれていても通信として成立せず、RSP は低くなる。一方、高 SNR 領域では、正規宛先だけでなく非信頼中継の受信品質も向上するため、中継ノードが機密情報を復号できる可能性が高まり、秘匿性条件が破られやすくなる。そのため、RSP は再び低下する。これに対して、中程度の SNR 領域では、宛先が復号可能であり、非信頼中継は復号困難となる条件が成立しやすく、RSP が最大化される。

この結果は、非信頼中継ネットワークにおける安全通信では、単純に送信電力や SNR を高めることが常に有利とは限らないことを示している。むしろ、宛先と非信頼中継のチャネル差を利用し、適切な送信タイミングや制御方策を選択することが重要である。機械学習によるチャネル予測は、このような送信機会の選択を支援し、リアルタイム制御に向けた基礎的基盤となる。

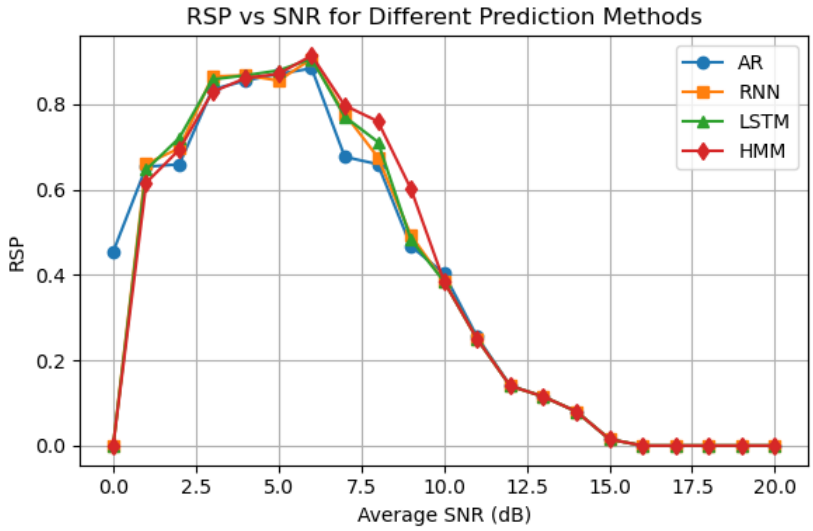

図 5　RSP 性能比較

4-3 RIS 支援非信頼中継ネットワークにおける秘匿性能

第二の成果として、RIS を備えた非信頼中継ネットワークに対して、GNN 支援 FedDRL による制御手法を検討し、秘匿通信性能を評価した。提案手法では、ネットワークをグラフとして表現し、GNN によりトポロジーと CSI を反映した状態埋め込みを生成した。その後、DRL エージェントが中継選択、電力配分、RIS 位相制御を統合的に決定した。さらに、FL の考え方を取り入れることで、各分散ノードがローカル CSI を保持したままモデルを協調的に学習する枠組みを示した。

シミュレーションでは、提案手法をランダム中継選択、ランダム RIS 制御、Max-SNR 型中継選択などの基準法と比較した。その結果、提案手法は従来の基準法に比べて高い秘匿通信性能を示した。ランダム手法はネットワーク状態を考慮しないため、宛先に有利で非信頼中継に不利なチャネル条件を安定して選択できない。Max-SNR 型手法は宛先または中継リンクの信号品質を高めることを重視するが、非信頼中継や外部盗聴者への漏洩を十分に考慮しない場合がある。これに対して、提案手法は秘匿容量を報酬として学習するため、宛先の受信性能と盗聴側の受信性能の差を考慮した制御を行うことができる。

4-4 全探索との比較と計算量

RIS 支援非信頼中継ネットワークでは、中継数 K と RIS 素子数 L が増加するにつれて、全探索で評価すべき組合せが急速に増加する。たとえば、中継選択だけでも K 通りの候補があり、RIS 位相を量子化して各素子に複数の候補位相を与える場合、RIS 位相構成の候補数は指数的に増える。さらに、送信電力配分を考慮すると、探索空間は離散変数と連続変数の混合空間となり、全探索は小規模なネットワークでのみ実行可能である。

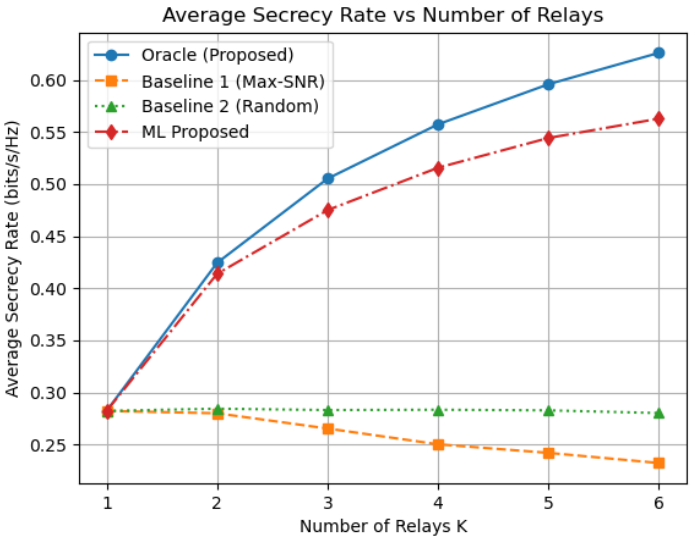

図 6　中継数に対する秘匿率性能

提案手法では、学習済みモデルを用いた推論により、中継選択、電力配分、RIS 位相制御を直接生成するため、全探索のように全候補を逐一評価する必要がない。GNN はネットワーク構造を圧縮した状態表現を生成し、DRL エージェントはその表現に基づいて行動を決定する。このため、推論時の計算量は全探索に比べて大幅に削減される。一方で、シミュレーション結果から、提案手法は全探索に近い秘匿性能を達成できることが示された。これは、GNN 支援 DRL が、非凸かつ複雑な PLS 制御問題に対して、性能と計算量のバランスに優れた解を提供できることを意味する。

表 2　計算量比較

手法	主な処理内容	計算量・オーバーヘッドの傾向	特徴
Random relay + random RIS	中継ノードと RIS 位相をランダムに選択	$O(K + L)$	計算量は小さいが，チャネル状態や秘匿性を考慮しないため性能は低い
Max-SNR relay	宛先側 SNR が最大となる中継を選択	$O(KL)$ 程度	宛先の受信品質を重視するが，非信頼中継や外部盗聴者への漏洩を十分に考慮しない
Exhaustive search	中継選択と RIS 位相候補を全探索	$O(K2^{BL})$ 程度	小規模では上限性能の参考になるが，RIS 素子数 L の増加に対して指数的に複雑化する
Proposed GNN/DRL actor	GNN による状態埋め込みと DRL による制御方策生成	$O(L_G\|E\|d + L_G N d^2 + Kd + dL)$ 程度	学習済みモデルにより，中継選択，電力配分，RIS 位相制御を低遅延で決定できる
FedAvg aggregation	複数クライアントのモデル更新を集約	$O(M\|\Omega\|)$ / round	ローカル CSI を共有せず，モデルパラメータのみを集約するため，プライバシー保護に有効

4-5 FL 導入によるプライバシー保護と分散性

本研究では、GNN および DRL の学習を分散環境で行うために FL の導入を検討した。FL の利点は、ローカル CSI や通信履歴を中央に集約せず、モデル更新のみを共有する点にある。無線通信における CSI は、端末位

置、移動状態、周辺環境、通信相手との関係などを反映するため、プライバシーやセキュリティ上の観点から慎重に扱う必要がある。特に非信頼中継ネットワークでは、ネットワーク内の一部ノードが完全には信頼できないため、ローカルデータの集中管理は望ましくない。

FedDRL の枠組みにより、複数の分散ノードは各自の観測データを用いてローカルに GNN エンコーダと DRL エージェントを更新し、モデルパラメータだけを共有する。サーバはこれらの更新を集約し、グローバルモデルを再配布する。この方法により、各ノードの生 CSI を共有することなく、複数のチャネル環境やネットワーク状態から得られた学習結果を活用できる。これは、将来の 6G ネットワークにおいて、エッジノードや基地局が分散的に PLS 制御を実行するための基盤となる。

5 考察

5-1 申請時の研究目的に対する達成状況

本研究は、申請時に掲げた「非信頼中継ネットワークにおける物理層セキュリティの強化」「機械学習を用いたインテリジェントで適応性のあるセキュリティアルゴリズムの設計」「チャネル状態を予測することによるリアルタイムなセキュリティ対策」という目的に沿って実施された。チャネル予測に関しては、AR、RNN、LSTM、HMM を比較し、MSE と RSP の二つの観点から評価した。これにより、単なる通信品質予測ではなく、信頼性と秘匿性を同時に考慮した送信判断への応用可能性を示した。

また、RIS 支援非信頼中継ネットワークに関しては、GNN、DRL、FL を統合した枠組みを提案し、複雑なネットワーク構造を持つ安全通信環境に対して、学習に基づく制御手法が有効であることを示した。これは、申請時に想定した「機械学習を活用した CSI 推定・チャネル状態予測」および「リアルタイムに適応する物理層セキュリティ手法」の方向性を具体化する成果である。

一方で、申請時には Software Defined Radio（SDR）を用いた検証も視野に入れていたが、本研究期間内では主として理論モデル化と計算機シミュレーションに注力した。これは、非信頼中継、RIS、GNN、DRL、FL を含む統合的な制御問題の定式化と評価を優先したためである。今後は、シミュレーションで得られた知見をもとに、SDR または小規模テストベッドを用いた実験的検証へ発展させることが課題である。

5-2 チャネル予測型 PLS の意義

チャネル予測型 PLS の意義は、通信機会の選択を能動的に行える点にある。従来の PLS では、与えられたチャネル状態に対して符号化、電力制御、人工雑音、ビームフォーミングなどを最適化することが多かった。これに対して、本研究では、将来のチャネル状態を予測し、信頼性と秘匿性の両条件を満たすタイミングを選ぶことで、安全通信を実現するアプローチを採用した。これは、リアルタイムに変動する無線環境に対して、予測に基づく先回り型のセキュリティ制御を行う試みである。

RSP 評価により、セキュリティ性能が SNR に対して単調に向上するわけではないことも明らかになった。一般に通信品質の向上を目的とする場合、SNR を高めることは有利である。しかし、非信頼中継環境では、中継側の受信品質も同時に向上する可能性があるため、単純な高 SNR 化は秘匿性の低下につながる場合がある。この点は、非信頼中継ネットワークに特有の重要な設計上の知見である。

5-3 GNN/FedDRL 型 PLS 制御の意義

GNN 支援 FedDRL 型 PLS 制御の意義は、複雑なネットワーク構造と多数の制御変数を統合的に扱える点にある。RIS 支援ネットワークでは、RIS 位相、送信電力、中継選択が相互に影響するため、個別に最適化しても全体として最適な秘匿性能が得られるとは限らない。また、非信頼中継ノードが複数存在する場合、どの中継を選択するかによって、宛先への信号強度だけでなく、内部盗聴リスクも変化する。

GNN は、このようなネットワーク構造を明示的に扱うための有効な手段である。ノードとエッジからなるグラフ表現を用いることで、複数中継、RIS、宛先、送信元の関係を自然に表現できる。DRL は、グラフ表現から得られた状態に基づいて、長期的な報酬を最大化する制御方策を学習できる。さらに、FL を組み合わせることで、ローカル CSI を共有せずに複数ノードが協調学習できる。このような構成は、将来の 6G ネットワークにおける分散的かつプライバシー保護型の PLS 制御に適している。

6 研究成果

本研究の主要成果は、以下の二つの国際会議論文として採択された。

一つ目の成果である “Machine Learning-Based Adaptive Physical-Layer Security in Untrusted Relay Networks” では、非信頼中継ネットワークにおけるチャネル予測型 PLS を検討した。AR、RNN、LSTM、HMM を比較し、MSE による予測精度評価と RSP による信頼性・秘匿性の同時評価を行った。その結果、HMM、RNN、LSTM などの時系列・状態遷移を扱える手法が、単純な AR モデルよりも有効であり、チャネル予測精度の改善が安全送信判断に結びつくことを示した。本成果は、The 8th International Conference on Information Communication and Signal Processing (ICICSP 2025) において採択され、Best Paper Award を受賞した。二つ目の成果である “GNN-Assisted Federated Deep Reinforcement Learning for Physical-Layer Security in RIS-Enabled Untrusted Relay Networks” では、RIS 支援非信頼中継ネットワークにおける GNN、DRL、FL を統合した FedDRL 型 PLS 制御手法を提案した。提案手法は、ネットワークをグラフとしてモデル化し、GNN によりトポロジーと CSI を反映した状態表現を生成し、actor- critic 型 DRL により中継選択、送信電力配分、RIS 位相制御を統合的に最適化する。さらに、FL によりローカル CSI を直接共有せずに分散学習を行う枠組みを示した。本成果は、The International Symposium on Computer Applications and Information Technology (ISCAIT 2026) において採択され、Best Poster Award を受賞した。これらの成果により、本研究は、非信頼中継ネットワークにおける予測型 PLS と、RIS 支援ネットワークにおける学習型 PLS 制御の二つの方向から、機械学習を活用した適応型セキュリティ設計の有効性を示した。

さらに，本研究で得られた知見を発展させ，RIS 支援物理層セキュリティおよび GNN 支援学習制御に関する論文を投稿中であり，今後，より一般的な 6G/ITS 環境への展開を進める予定である。

7 今後の課題

本研究により、機械学習を用いた非信頼中継ネットワークの適応型 PLS 設計について一定の成果が得られたが、今後検討すべき課題も残されている。1) チャネル予測モデルの汎化性能の検証である。本研究では Rayleigh フェージングを用いた計算機シミュレーションにより評価を行ったが、実環境では移動速度、遮蔽物、端末密度、周波数帯、アンテナ配置などによりチャネル統計が変化する。今後は、より多様なチャネルモデルや実測データを用いた評価が必要である。2) SDR や RIS 実機を用いた実験的検証である。シミュレーションでは制御手法の有効性を確認できたが、実機環境では CSI 取得遅延、RIS 制御遅延、推論処理時間、同期誤差、フィードバックオーバーヘッドなどが性能に影響する。これらを考慮したリアルタイム実装は、実用化に向けた重要な課題である。3) 外部盗聴者や複数攻撃者に対するロバスト性である。本研究では非信頼中継を中心に検討したが、実際のネットワークでは外部盗聴者、ジャミング、偽 CSI 報告、モデル更新攻撃などが同時に発生し得る。FL を用いる場合には、悪意あるクライアントによるモデル汚染攻撃やプライバシー漏洩にも注意が必要である。今後は、PLS、機械学習セキュリティ、ロバスト最適化を統合した設計が求められる。4) 計算量と性能のトレードオフである。GNN や DRL は高い表現力を持つ一方で、学習には計算資源とデータが必要である。エッジデバイスや基地局でリアルタイムに動作させるためには、モデル圧縮、軽量化、転移学習、オンライン学習などの導入が有効である。特に RIS 制御では、チャネル coherence time 内で位相制御を更新する必要があるため、推論遅延の削減が重要となる。

8 まとめ

本研究では、非信頼中継ネットワークにおける内部盗聴リスクに対し、機械学習を活用した適応型物理層セキュリティ設計を行った。まず、AR、RNN、LSTM、HMM を用いたチャネル予測手法を比較し、MSE と RSP により、予測精度と信頼性・秘匿性の同時評価を行った。その結果、時系列依存性や状態遷移を扱える学習モデルが、安全な送信機会の選択に有効であることを確認した。次に、RIS を備えた非信頼中継ネットワークに対して、GNN 支援 FedDRL による制御手法を検討した。提案手法は、ネットワークトポロジーと CSI をグラフとして表現し、DRL により中継選択、送信電力配分、RIS 位相制御を統合的に最適化するものである。さらに、FL によりローカル CSI を直接共有しない分散学習の可能性を示した。

以上の成果により、当初の研究目的であった、チャネル変動やネットワーク状態に応じてリアルタイムに

適応する PLS 手法の有効性を確認した。本研究で得られた知見は、6G 時代の高密度・分散型無線ネットワークにおいて、暗号技術を補完する軽量かつ適応的な安全通信基盤の構築に貢献するものである。今後は、実測チャネル、SDR、RIS 実機、複数攻撃者モデル、FL に対する攻撃耐性を含めた検証を進め、実環境に近い適応型物理層セキュリティシステムへ発展させる予定である。

【参考文献】

[1] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," IEEE Communications Surveys & Tutorials, vol. 16, no. 3, pp. 1550–1573, 2014.

[2] H.-M. Wang and X.-G. Xia, "Enhancing wireless secrecy via cooperation: Signal design and optimization," IEEE Communications Magazine, vol. 53, no. 12, pp. 47–53, 2015.

[3] S. Qian and M. Chen, "Physical layer security in lossy untrusted relay networks with finite blocklength," Comm&Optics Connect, vol. 1, no. 1, pp. 1–14, 2024.

[4] H. Ye, G. Y. Li, and B.-H. Juang, "Power of deep learning for channel estimation and signal detection in OFDM systems," IEEE Wireless Communications Letters, vol. 7, no. 1, pp. 114–117, 2018.

[5] C. Zhang, P. Patras, and H. Haddadi, "Deep learning in mobile and wireless networking: A survey," IEEE Communications Surveys & Tutorials, vol. 21, no. 3, pp. 2224–2287, 2019.

[6] J. Jagannath, N. Polosky, A. Jagannath, F. Restuccia, and T. Melodia, "Machine learning for wireless communications in the Internet of Things: A comprehensive survey," Ad Hoc Networks, vol. 93, 101913, 2019.

[7] Q. Wu and R. Zhang, "Towards smart and reconfigurable environment: Intelligent reflecting surface aided wireless network," IEEE Communications Magazine, vol. 58, no. 1, pp. 106–112, 2020.

[8] H. Yang, X. Xiong, J. Zhao, D. Niyato, C. Yuen, and Y. L. Guan, "Deep reinforcement learning based intelligent reflecting surface for secure wireless communications," IEEE Global Communications Conference, 2020.

[9] Y. Shen, J. Zhang, S. H. Song, and K. B. Letaief, "Graph Neural Networks for Wireless Communications: From Theory to Practice," IEEE Transactions on Wireless Communications, vol. 22, no. 5, pp. 3554–3569, 2023.

[10] B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. y Arcas, "Communication-efficient learning of deep networks from decentralized data," AISTATS, pp. 1273–1282, 2017.

[11] D. H. Tashman, S. Cherkaoui, and W. Hamouda, "Federated learning-based MARL for strengthening physical-layer security in B5G networks," IEEE International Conference on Communications, pp. 293–298, 2024.

〈発　表　資　料〉

題　　名	掲載誌・学会名等	発表年月
Machine Learning-Based Adaptive Physical-Layer Security in Untrusted Relay Networks	The International Conference on Information Communication and Signal Processing	2025 年 9 月 （Best Paper Award 受賞）
GNN-Assisted Federated Deep Reinforcement Learning for Physical-Layer Security in RIS-Enabled Untrusted Relay Networks	The International Symposium on Computer Applications and Information Technology	2026 年 1 月 （Best Poster Award 受賞）