リプレイ攻撃に対する防御手法の検討と評価

2.4GHz帯無線リモコンシステムを対象とした確率的チャネル環境下での防御手法の性能比較

氏名：[あなたの名前]
所属：[大学名・学部名]
指導教員：[教員名]

研究背景：無線リモコンとリプレイ攻撃

- 2.4GHz帯の低価格無線デバイス（玩具カー、スマートロック等）が普及
- 無線通信では攻撃者が通信を傍受・記録可能
- **リプレイ攻撃**：記録した正規の通信を後で再送信し、受信側を騙す
- 物理層の暗号化がない、または弱い場合に脆弱
- パケット損失や乱順が発生する実環境での防御手法の性能は十分に評価されていない

研究目的

- 2.4GHz帯無線リモコンに適用可能な**3種類のリプレイ攻撃防御手法**を実装
- **パケット損失・乱順が存在する現実的な通信環境**をモデル化
- シミュレーションと実機実験により、各防御手法の性能を定量評価
- セキュリティ（攻撃成功率）と可用性（正規受理率）のトレードオフ関係を明らかにする

本研究の位置づけ

- **既存のリプレイ攻撃研究**:
  - 実機を用いたPoC（車のキーレスエントリ等）が中心
  - プロトコルレベルの防御手法の定量評価は限定的
- **既存のカウンタベース防御**:
  - rolling / window は提案済みだが、損失・乱順チャネルでの比較は不十分
- **本研究の貢献**:
  - 2.4GHz無線リモコンを想定した共通シミュレーションフレームワークを実装
  - Monte Carloシミュレーションにより、3方式のセキュリティ–可用性トレードオフを系統的に評価

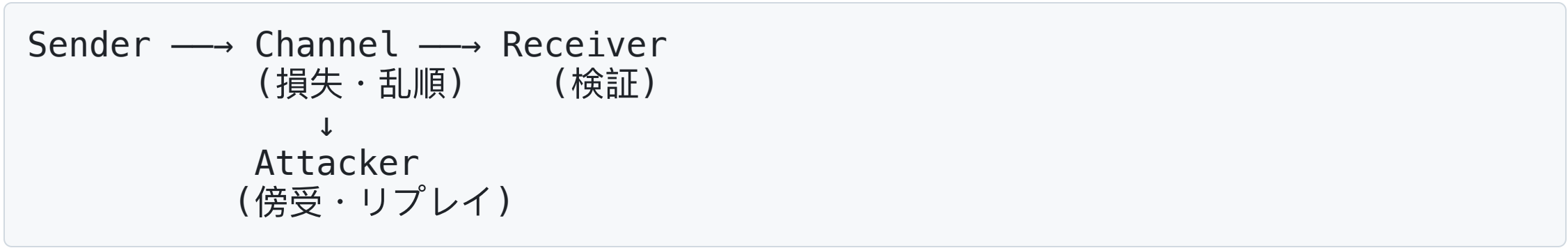
対象システムと抽象化レベル

- **対象**：2.4GHz帯の単方向無線リモコン（送信機→受信機）
- **物理層の抽象化**：
  - パケット損失確率 p_loss（0～30%）
  - パケット乱順確率 p_reorder（0～30%）（送信順とは異なる順序で到着する確率）
- **評価対象**：リンク層のフレーム検証ロジック
- この抽象化により、本質的な防御メカニズムの性能を評価可能

攻撃モデル

- 攻撃者は通信を完全に傍受・再送できるが、暗号学的なMAC（HMAC-SHA256）の偽造はできない
- **攻撃タイミング**:
  - 事後一括リプレイ：正規通信終了後に記録フレームを再送
  - インライン挿入：正規通信中にリプレイを混入
- 現実的な攻撃者モデル（いわゆるDolev-Yao型）に基づく

システム構成



- **Sender（送信機）**：指令フレームを生成、防御機構に応じてMAC/カウンタ付与
- **Channel（通信路）**：パケット損失・乱順をシミュレート
- **Receiver（受信機）**：フレームを検証、正規/リプレイを判定
- **Attacker（攻撃者）**：正規フレームを記録し、選択的に再送信

防御手法①：ローリングカウンタ方式

- **原理**：送信側が単調増加するカウンタをフレームに付与
- **受信側の検証**：
  - カウンタが前回より大きい → 受理
  - カウンタが前回以下 → リプレイと判定して拒否
- **MAC（HMAC-SHA256）**で改ざんを防止
- **利点**：実装が単純、計算コスト低
- **欠点**：パケット乱順に対して脆弱（後述）

防御手法②：受信ウィンドウ方式（Sliding Window）

- **原理**：RFC 6479（IPsec）に基づくスライディングウィンドウ
- **ビットマップ**で最近Wフレーム分の受信履歴を記録
- **動作**：
  - 新しい最大カウンタ → ウィンドウを前進
  - ウィンドウ内の古いカウンタ → ビットマップでリプレイ判定
  - ウィンドウ外の古すぎるカウンタ → 拒否
- **調整パラメータ**：ウィンドウサイズW（本研究ではW=3〜7を評価）

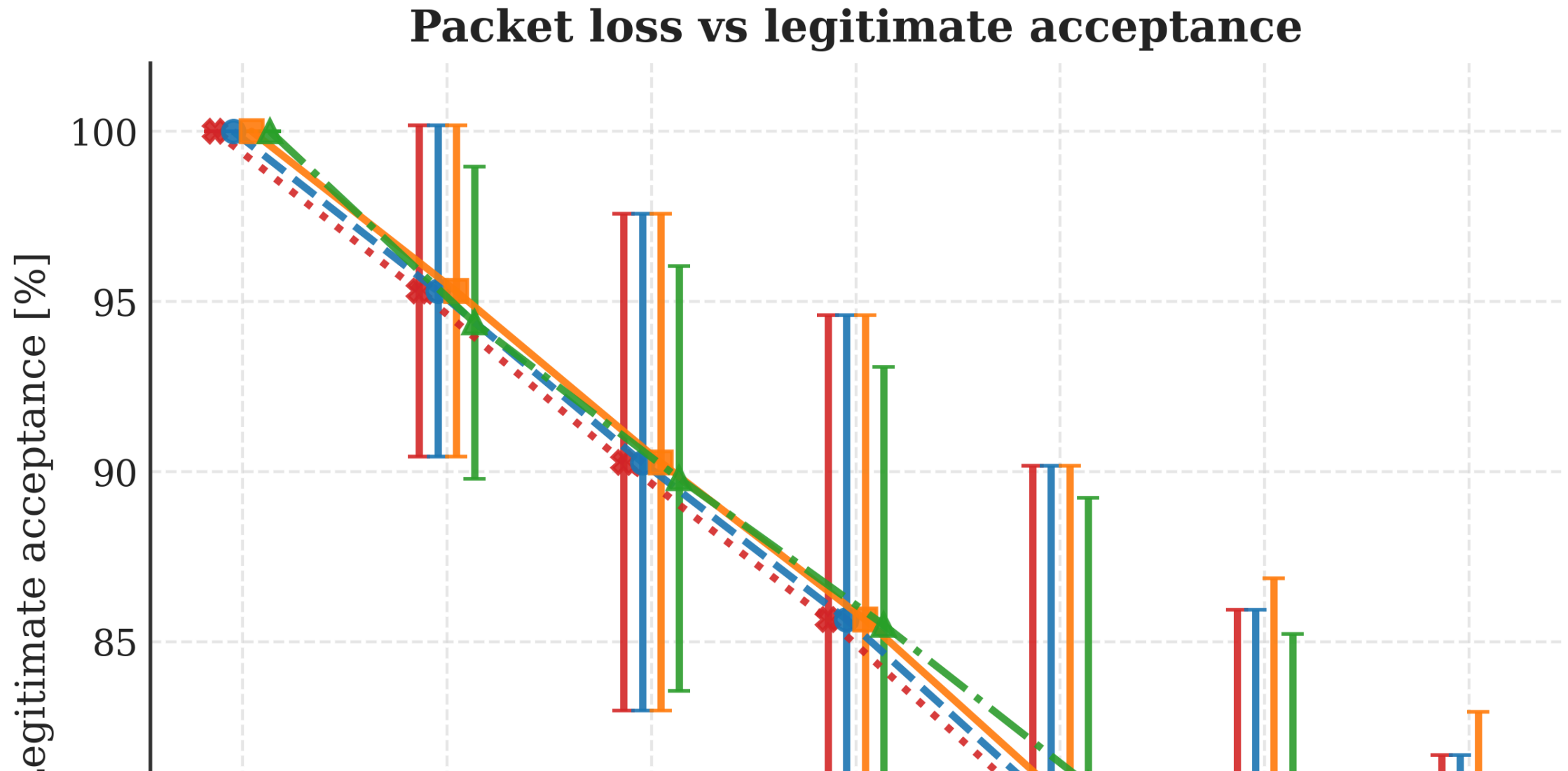
防御手法③：チャレンジレスポンス方式

- **原理**：受信側が乱数（nonce）を発行、送信側がそれに応答
- **手順**：
    i. 受信機 → 送信機：challenge（nonce）
    ii. 送信機 → 受信機：response（command + nonce + MAC）
    iii. 受信機：nonceが一致し、MACが正しければ受理
- **利点**：本研究で比較した中ではセキュリティレベルが最も高い
- **欠点**：双方向通信が必要、レイテンシ増大
- **位置づけ**：理論的な上限性能を示すベースライン

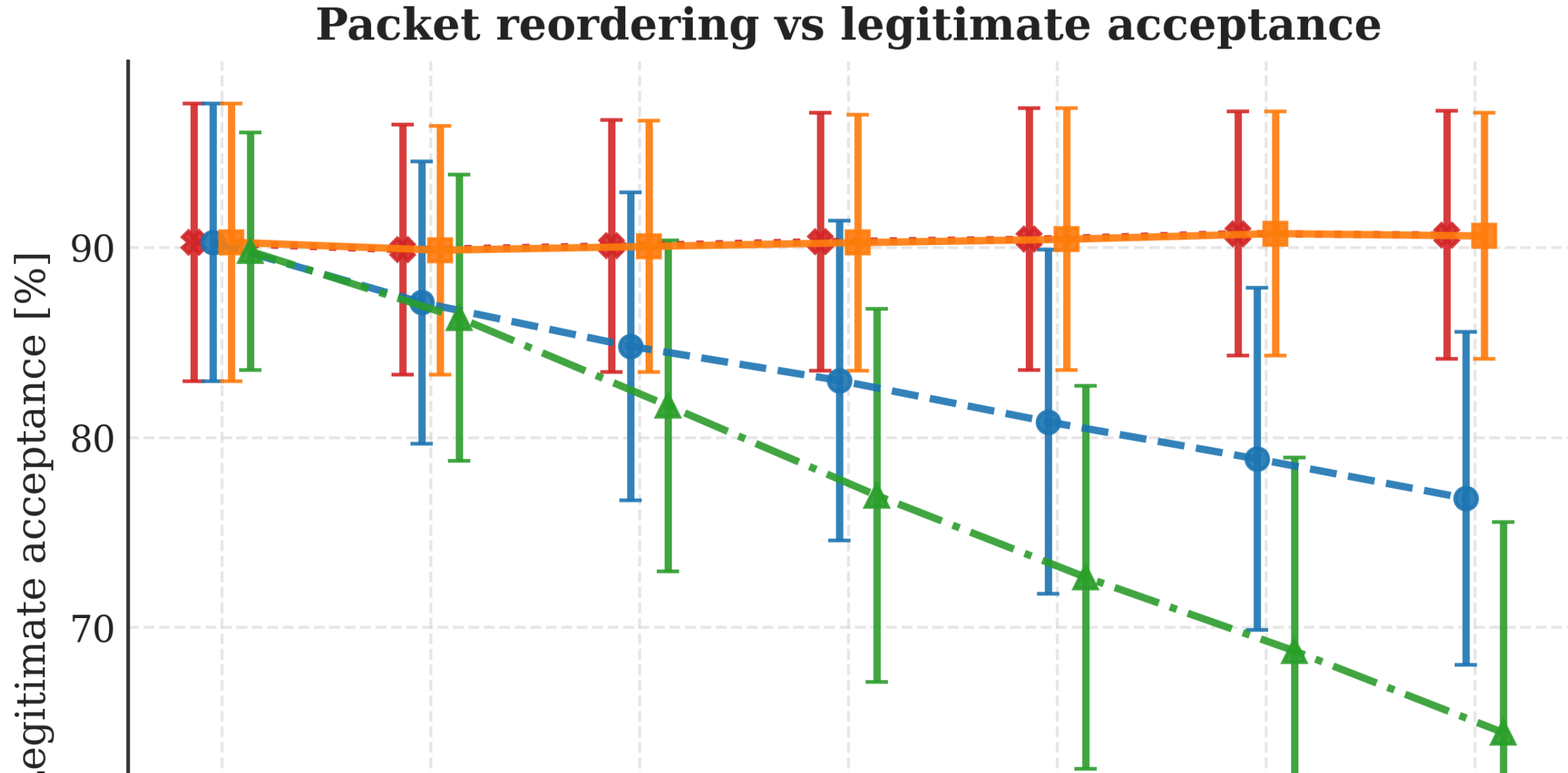
シミュレーション手法

- **Monte Carlo法**：各設定ごとに200回の独立試行を実行
- **評価指標**：正規受理率（可用性）、攻撃成功率（セキュリティ）
- **主なパラメータ**：p_loss（0〜30%）、p_reorder（0〜30%）、window_size（1〜20）
- 固定ランダムシード（42）により実験結果の再現性を確保

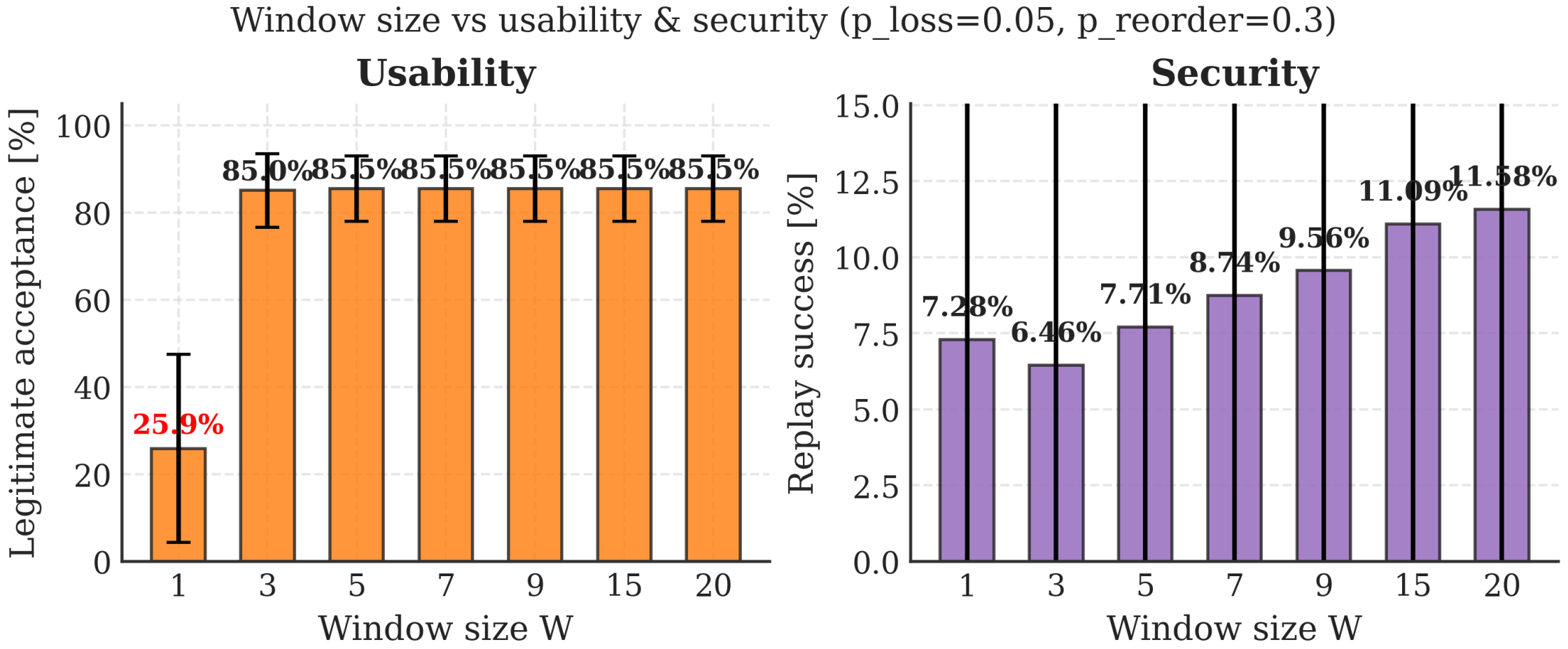
実験結果①：パケット損失の影響



実験結果②：パケット乱順の影響（重要）



実験結果③：ウィンドウサイズのトレードオフ



- **W=1**：正規受理率約25%（使用不可）

実機実験の概要


実験環境

- **実験環境**：2.4GHz玩具カーのリモコンシステムを改造
- **測定項目**：実際のパケット損失率、乱順発生率
- **シミュレーションとの比較**：
  - 実測の損失率：約8～12%
  - 実測の乱順率：約3～5%
  - window方式（W=5）の実機性能：正規受理率約85%、攻撃検出率約99%
- シミュレーション結果と実機実験は概ね一致
- 物理層抽象モデルの妥当性を確認

考察：各防御方式の特性

方式	可用性	セキュリティ	乱順耐性	実装コスト	適用先
rolling	高	高	**低**	低	有線・低遅延環境
window	高	高	**高**	中	**一般的な無線IoT**
challenge	高	**最も高い**	中	高	高セキュリティ要求

- **rolling**：乱順環境では性能が大きく劣化、実用には不向き
- **window**：乱順に強く、無線IoTの第一選択
- **challenge**：本研究で比較した中ではセキュリティレベルが最も高いが、双方向通信が必須

本研究で明らかになったこと

- **乱順がリプレイ攻撃防御に与える影響を定量評価**
- rolling方式は理論的には単純だが、乱順環境では性能が大きく劣化
- window方式（RFC 6479準拠）が、本研究で想定した無線環境において**最もバランスの良い選択肢であることを示した**
- ウィンドウサイズW=5前後で良好なバランスを実現
- 物理層を抽象化したモデルでも、実機と整合する結果が得られた

本研究の限界

- **物理層の抽象化の限界**:
  - RF干渉、フェージング、マルチパスの影響は未考慮
  - バースト損失（連続的なパケット損失）のモデル化が不十分
- **攻撃モデルの制約**:
  - 選択的ジャミング攻撃は未検証
  - タイミング攻撃（早すぎるリプレイ）の評価が必要

今後の課題

- **実機実験の拡充**:
  - より多様なデバイス・環境での検証
  - 長期運用時の性能評価
- **物理層モデルの拡張**:
  - バースト損失やフェージングの影響評価
- **攻撃モデルの拡張**:
  - ジャミング攻撃との組み合わせ評価
  - より高度な攻撃者モデルの検討

結論

- 2.4GHz帯無線リモコンを対象に、3種類の防御方式を共通フレームワーク上で比較
- 本研究で想定した条件下では、**window方式がセキュリティ–可用性のバランスが最も良い結果を示した**
- 実機実験により、物理層抽象モデルの有効性を確認
- **実用的示唆**：一般的な低価格無線IoTデバイス向けに、window方式（W=5前後）が**有力な防御候補である**

ご清聴ありがとうございました

質疑応答

コード・データ公開:
https://github.com/tammakiiroha/Replay-simulation

- 全実験データ（results/*.json）
- 完全なソースコード（Python 3.11+）
- 再現手順（README.md）