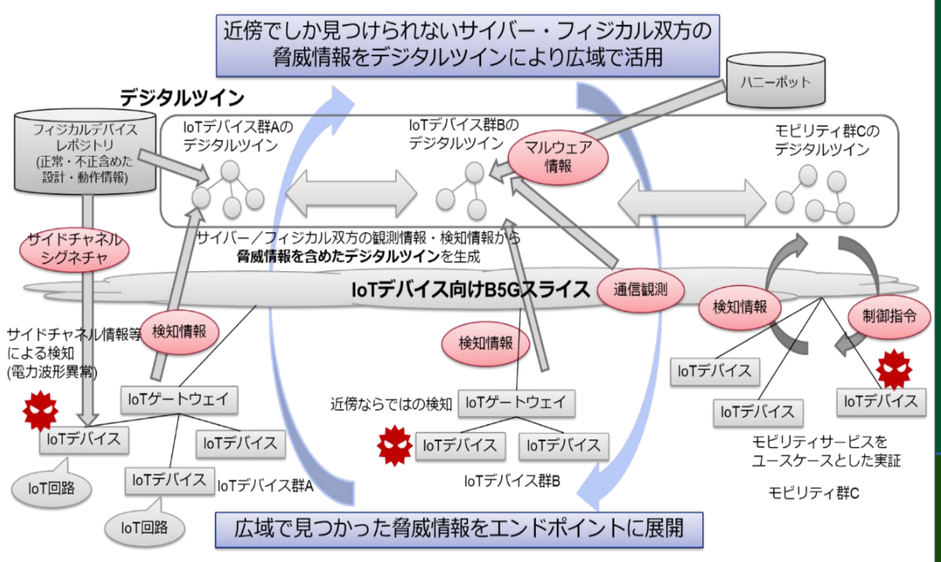
マイクロモビリティシステムのセキュリティ負荷耐性実験

芝浦工業大学工学部情報工学科
佐藤駿介（新熊研究室）

背景

1．次世代社会
- Beyond 5Gを利用したフィジカル空間とサイバー空間が一体化した社会
- 利用者が意識しなくてもセキュリティやプライバシーが常に確保され、災害や障害の発生時でもサービスが途絶えない瞬時の復旧を実現する「超安全・信頼性」の確保

2．次世代に求められるセキュリティ対策
- Beyond 5Gの10倍の同時接続数が見込まれる IoT デバイスやコネクテッドカーなどのエマージング技術に対応した、新たなセキュリティ対策が必要
- 局所的にサイバー・フィジカル空間で検知された脅威情報を広域に展開し、直接的には脅威を検知できない他の類似デバイスによる潜在脅威の発見や対策に活用するサイバー・フィジカル連携型のセキュリティ基盤の実現が必要

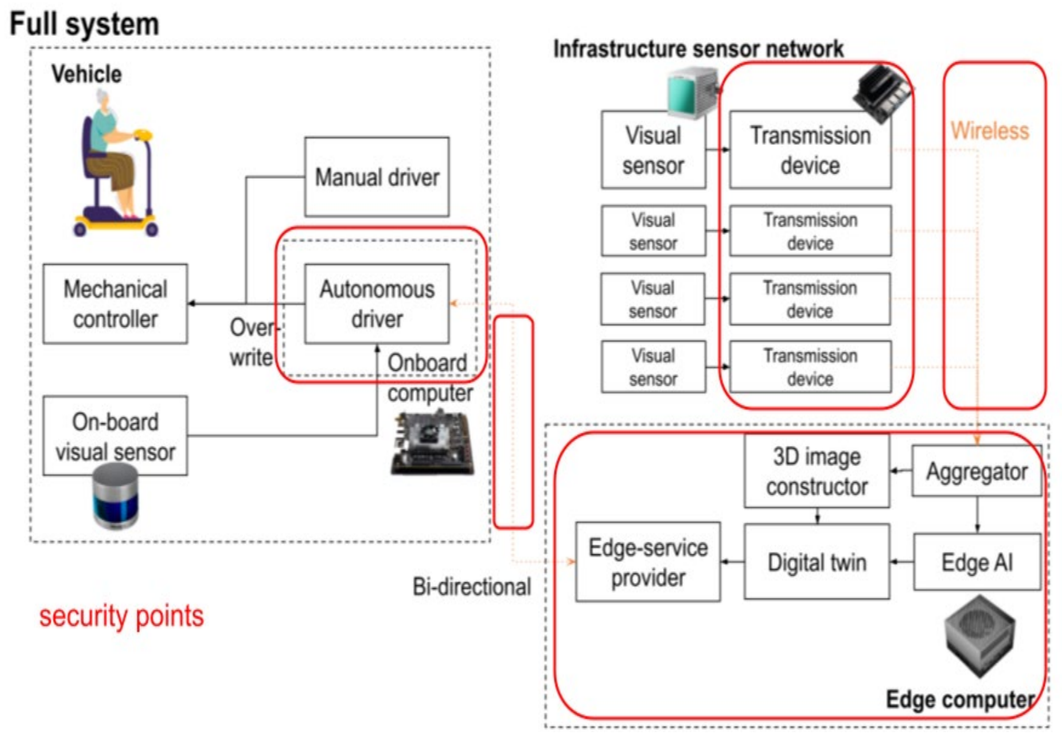


提案方式

1．提案システム
- デジタルツインを実現した自動運転モビリティシステム（右図）
- 環境センサネットワークとエッジコンピュータ、モビリティから構成
- マイクロモビリティはJetson nano mouse、WHILLなど点群データを使用して走行可能

2．攻撃モデル
- システムには多くのセキュリティ攻撃ポイントが存在。セキュリティ攻撃には、フィジカル型やサイバー型、もしくはそれらを併用した攻撃が予想

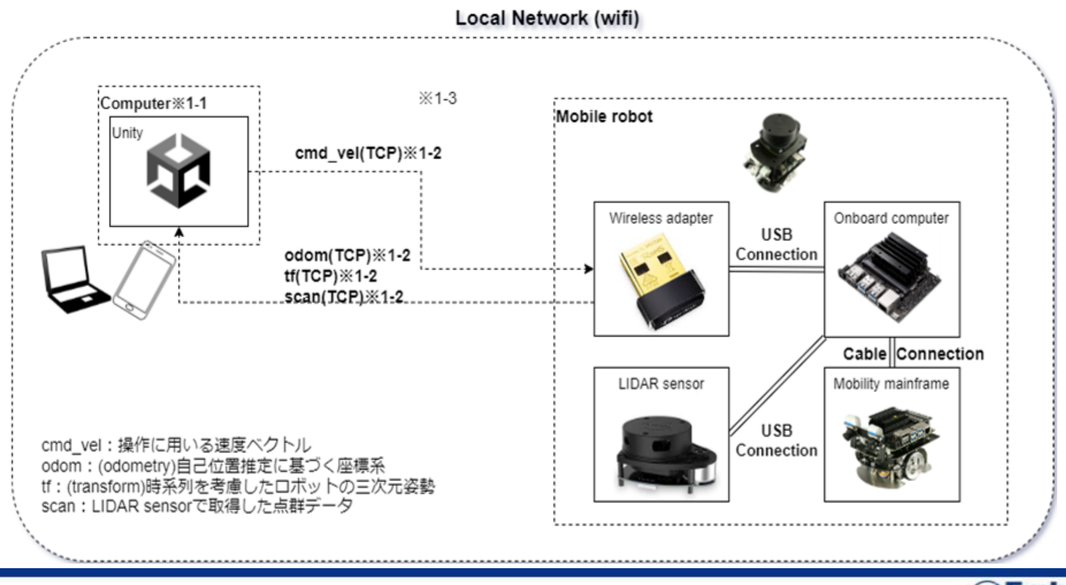
3．セキュリティ攻撃タイプ
- フィジカル型: センサに対し対象物を誤認識させる攻撃
- サイバー型: 機械学習システムに対するランサムウェア攻撃
- 複合型: 上2つを併用

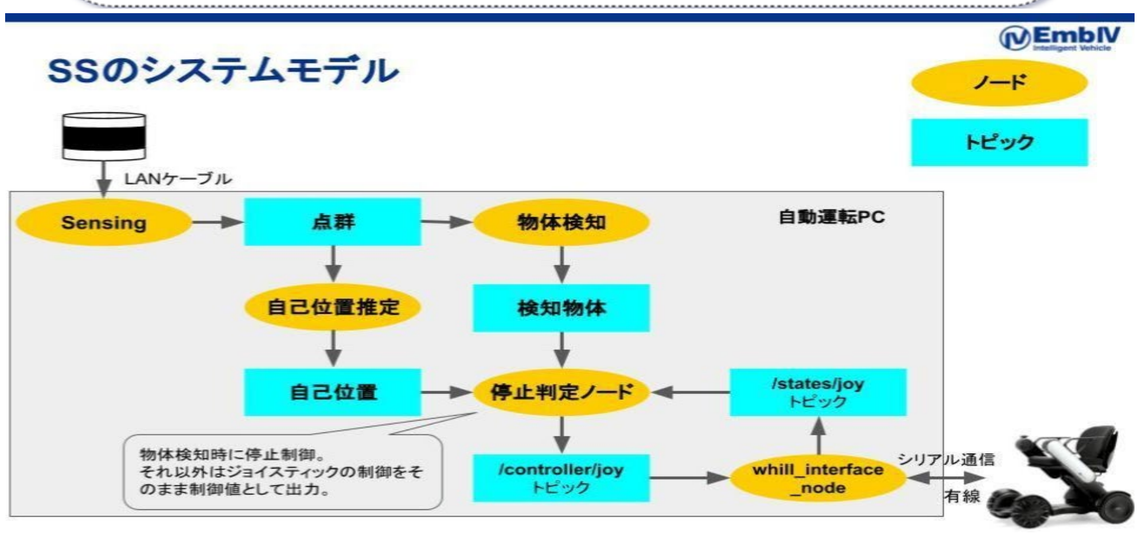


評価方式

1．実装システム
- マイクロモビリティ車両
  - 手動運転型スタンドアロン（右上図）：Jetson nano mouse
  - 運転補助型スタンドアロン（右下図）：電動ホイールチェアWHILL
- 後者は点群データを使用して、緊急停止などの運転補助を実施

2．評価方法
- 実装システムに対してセキュリティ負荷耐性実験を行い影響を評価
- モビリティが正常に操作するコースを予め設定し、走行中のモビリティシステムには常にセキュリティ攻撃を実施
- 評価指標として運転停止率と移動経路誤差を使用
- 攻撃手法
  （本実験においてサイバー型攻撃は機械学習に限定しない）
  - 鏡面による点群データへの干渉（フィジカル型）
  - パケットデータの損失（フィジカル型、サイバー型）
  - UDP送信による通信負荷（サイバー型）
  - 上記の組み合わせ





結論

1．要約
- デジタルツインを実現した自動運転モビリティシステムの先駆けとして、手動運転型スタンドアロンシステムと運転補助型スタンドアロンシステムを実装し、双方に対してのセキュリティ負荷耐性実験を示した

2．今後の展望
- モビリティシステムに対するセキュリティ負荷耐性実験の評価をもとに、セキュリティ基盤を構築
- セキュリティ基盤を適応前と後において、セキュリティ攻撃による誤作動のしきい値を比較評価
- 最終的には、提案システムにセキュリティ基盤を実装しセキュリティを確保