位置プライバシ保護のための通信遅延を考慮した動的仮名変更手法

理工学部情報工学科　重野・森研究室

位置プライバシの保護

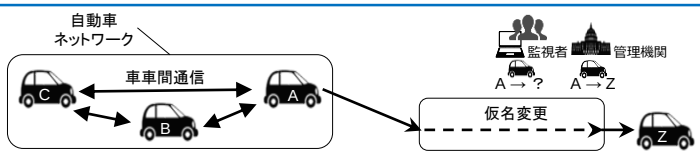
・自動車ネットワーク：道路交通の性能向上のために車両が形成するネットワーク
・監視者：各車両が交換する位置情報を連続的に監視

ユーザの位置プライバシが侵害される危険性

自動車ネットワークへの仮名の適用

・仮名：時間経過で変化可能な識別子
・仮名変更：頻繁かつ適切なタイミングでの変更で連続的な追跡を防止

仮名変更による位置プライバシ保護

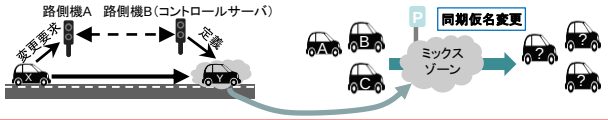


仮名変更手法

関連研究：DMLP

車両の要求に応じたミックスゾーンの動的形成

・ミックスゾーン：暗号化通信に基づいて仮名変更を行う領域
1.車両が仮名変更要求メッセージを近傍の路側機に送信
2.近傍の路側機はメッセージをコントロールサーバへ転送
3.路側機を通じてコントロールサーバがミックスゾーンの位置等を決定
　・車両の予測位置，交通状況，要求プライバシレベルにより決定



路側機の位置に依存

路側機に依存しない仮名変更

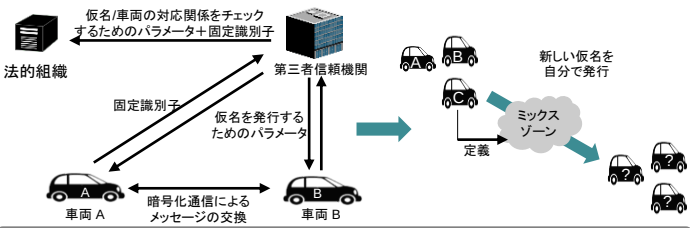
・IDベース署名暗号

路側機を用いない車両通信の認証

接続性の低下により通信遅延の影響が増大

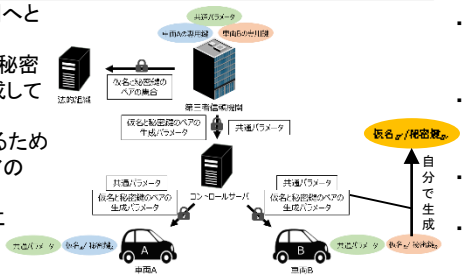
・2段階ミックスゾーン

仮名変更への通信遅延の影響を抑制



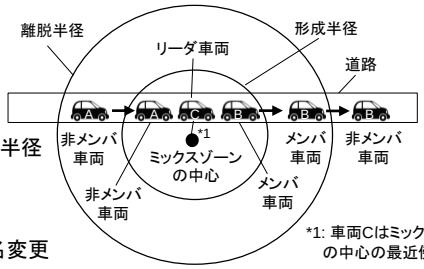
IDベース署名暗号

1.各車両は第三者信頼機関へと固定識別子を登録
2.第三者信頼機関が仮名と秘密鍵の生成パラメータを生成して各車両に送付
（仮名の正当性を確認するため同時に法的組織へとペアの集合を送付）
3.各車両が生成パラメータに基づき自身の仮名と秘密鍵のペアを生成



2段階ミックスゾーン

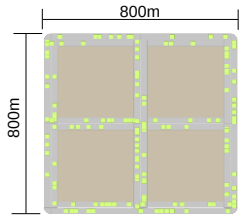
・形成半径
ミックスゾーン参加のために満たすべき半径
・離脱半径
ミックスゾーン外への離脱を判定するための半径
・リーダ車両
仮名変更を主導
・メンバ車両
リーダ車両とともに仮名変更

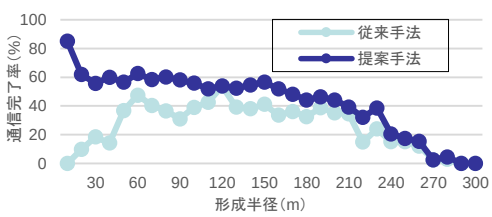


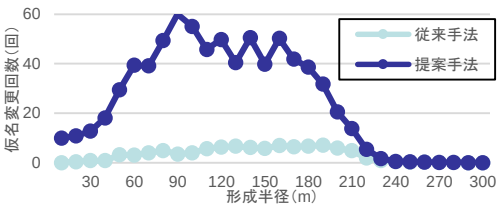
*1: 車両Cはミックスゾーンの中心の最近傍車両

認証と通信遅延を考慮したアルゴリズムに基づく協調同期仮名変更

ノードの移動に対応した通信シミュレーション







・最大で80%以上の通信完了率を達成し，従来との比較で約15%上昇　・1000秒の実験で最大60回以上の仮名変更を達成し，従来との比較で約8.3倍に

通信遅延の抑制に起因してミックスゾーンの性能が改善

本研究はJSPS科研費JP20H04180の助成を受けたものです

研究者名　重野寛

お問合せ先　shigeno@mos.ics.keio.ac.jp