自動車ネットワークにおける通信遅延を考慮した密度ベース動的仮名変更手法の検討

山崎 玲[1] 團 皆人[1] 吉田 匡志[1] 重野 寛[1]

概要：ITS（Intelligent Transport Systems）の多くのアプリケーションでは，自動車ネットワークにて各車両の位置情報の交換が必要である．一方で，各車両の位置情報を追跡することで，位置プライバシは容易に侵害されてしまう．位置プライバシを保護する手段として，自動車ネットワークにおける仮名の使用が注目されている．先行研究では，車両からの要求と周辺車両数に応じて仮名を動的に変更することによって，位置プライバシを保護している．しかし，無線路側機の数が少ない場合や通信遅延が大きい場合，仮名変更に必要な通信に失敗し，適切な仮名変更を行うことができない．そこで，本稿では VDMC（Vehicle-based Dynamic Mix-zone Considering Communication Delay for Location Privacy in Vehicular Networks）を提案する．VDMC は，Mod-IBS 手法を適用した認証付き仮名 ID 鍵通信を活用することで，仮名を変更するために路側機を使用することが不要になる．さらに，仮名変更のための基準として複数の領域を用いることで，仮名変更の失敗を防ぐ．シミュレーション評価より，提案手法が先行研究と比較して，通信完了率と仮名変更回数を改善できることを示す．

A Study of Vehicle-based Dynamic Mix-zone Considering Communication Delay for Location Privacy in Vehicular Networks

REI YAMAZAKI[1] MINATO DAN[1] MASASHI YOSHIDA[1] HIROSHI SHIGENO[1]

1. はじめに

自動車社会における交通事故や渋滞等の課題を解決するために ITS（Intelligent Transport Systems）のさらなる実用化が推進されている．ITS を実現するためには，各車両と周辺車両や路側機，歩行者との間での情報通信が必要である．特に，交通事故や渋滞を未然に防ぐためには，各車両の位置情報を自動車ネットワーク内で共有する必要がある．しかし，悪意のある攻撃者は車両の位置情報を監視することでユーザの位置プライバシ [1] を侵害することが可能である．ITS を実現するためには，車両の位置プライバシを保護することが重要である．

位置プライバシの保護手法は大きく仮名を用いる手法とダミー位置を用いる手法に分類できる．ダミー位置を用いる手法では，攻撃者だけでなくサービス提供者も車両の正しい位置情報を把握することができず，ITS アプリケーションでの使用に支障をきたす可能性がある．そのため，本稿では仮名を用いる手法に着目する．仮名を自動車ネットワークに導入するためには，車両の識別化と非識別化が達成される必要がある．識別化とは，ITS アプリケーションを提供するために，認証機関等の ITS を管理する機関が仮名を通して車両情報を完全に把握できるようにすることである．一方で非識別化とは，位置プライバシを保護するために，攻撃者による完全な車両情報の把握を防ぐことで連続的な追跡を不可能にすることである．

車両の非識別化を実現する手法として，DMLP（Dynamic Mix-zone for Location Privacy）[2] が存在する．DMLP では，路側機が仮名変更のための領域を適切に定義した後，車両が周辺車両の予測位置を考慮した仮名変更を行うことで，車両の非識別化を実現する．プライバシを十分に保護するために，仮名変更時の領域内車両数が一定以上である場合のみ仮名を変更する．しかし，無線路側機の数が少ない場合や通信遅延が大きい場合，仮名変更に必要な通信に

[1] 慶應義塾大学大学院理工学研究科
Graduate School of Science and Technology, Keio University, Yokohama, Kanagawa, 223-8522, Japan

失敗し，適切な仮名変更を行うことができない．

本稿では，路側機の数や通信遅延によって仮名変更が失敗することを防ぐために，VDMC（Vehicle-based Dynamic Mix-zone Considering Communication Delay for Location Privacy in Vehicular Networks）を提案する．VDMC では，Mod-IBS 手法を適用した認証付き仮名 ID 鍵通信を活用し，収集した周辺車両情報に基づいて動的に仮名変更を行うことで，路側機を使用することが不要になる．また，仮名変更の基準として周辺の車両台数を用いることで同時仮名変更車両台数が増加するため，位置プライバシの保護の度合いが高まる．さらに，仮名変更のための基準として複数の領域を用いることで，通信遅延を原因とした仮名変更の失敗を防ぐ．

2. 関連研究

本章では，仮名変更に関する導入を行った後，識別化を達成するための暗号化手法と非識別化を達成するための仮名変更手法について述べる．その後，既存の仮名変更手法の問題点を述べる．

2.1 仮名変更

位置プライバシを保護するための代表的な手法として仮名を用いた手法がある．仮名は時間経過とともに変化し得る識別子である．自動車ネットワークに仮名を導入する際には識別化と非識別化が同時に達成される必要がある．識別化とは，仮名を導入した各車両の情報を管理機関が完全に把握可能にすることである．一方で，非識別化とは自動車ネットワーク内における仮名以外の車両情報を秘匿し，攻撃者からの連続的な追跡を防ぐことである．同一の仮名を長期間使用した場合，固定識別子と同様に連続的な監視によって車両と識別子を紐づけられてしまう．加えて，仮名を変更するタイミングが攻撃者に知られていた場合，変更前後の仮名を紐づけられることで連続的な監視を防止できない．そこで，非識別化を達成するためには頻繁かつ適切なタイミングでの仮名変更が必要となる．また，非識別化を達成すると同時に識別化を達成するためには，攻撃者に盗聴されないような信頼機関でのみ車両データ全体を把握できるような暗号化手法が必要となる．

2.2 暗号化手法

識別化を達成するための基本的な暗号化手法として IBS（Identity-Based Signcryption）手法 [3][4] がある．IBS 手法では，第三者信頼機関が生成した公開鍵や仮名と秘密鍵のペアを車両に割り当て，仮名を宛先として公開鍵暗号方式で通信を行う．しかし，IBS 手法にはスケーラビリティや仮名の再利用の点で課題がある．そこで，Mod-IBS 手法 [5][6] が提案された．Mod-IBS 手法は，IBS 手法における仮名と秘密鍵のペアの軽量割り当て手法である．手法の全体像は図 1 に示す．IBS 手法では全車両の仮名と秘密鍵のペアを生成するために必要なマスタ秘密鍵を保持しておく必要があったが，Mod-IBS 手法ではマスタ秘密鍵から各車両の専用秘密鍵を生成しておくことでマスタ秘密鍵の役割を分割し，仮名の再利用を実現している．また，IBS 手法では第三者信頼機関から各車両に仮名と秘密鍵のペアが渡されていたが，Mod-IBS 手法ではペアの生成パラメータのみを渡し，各車両が自身の持つ疑似乱数生成器によって自律的にペアを生成することでスケーラビリティが向上する．なお Mod-IBS 手法では，公開鍵の配布元であるディレクトリサービスの信頼性が十分であれば，安全性が IBS 手法と等価となる．

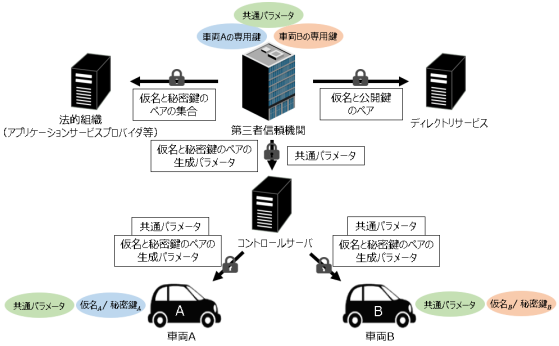

図 1 Mod-IBS 手法

2.3 仮名変更手法

これまで数多くの仮名変更手法が提案されてきたが，特に本研究と関連の深いものとして車両中心手法 [7]，協調同期変更手法 [8][9]，DMLP が挙げられる．車両中心手法は，移動する車両位置の予測に基づいて仮名を変更する場所とタイミングを車両が動的に決定する手法だが，周囲の車両の存在が担保されない問題がある．協調同期変更手法では，車両の要求メッセージに対して同時に複数車両が仮名変更を行う領域であるミックスゾーンを形成する．領域内では位置情報を含むメッセージの送信を行わないことで，攻撃者が変更前後の仮名を紐づけることは困難となる．しかし，仮名変更時に周囲に複数車両の存在を担保するためには交差点等の車両の集まりやすい地点をミックスゾーン候補とする必要があることから，候補地点数が少ないために仮名変更を十分に行うことができない事態が想定される．

ミックスゾーン形成位置に関しての発展手法として DMLP が提案された．図 2 に手法の全体の流れを示す．DMLP では，仮名の有効期限が近付いた車両が仮名変更要求メッセージを送信する．メッセージは受信した路側機からコントロールサーバへとフォワーディングされ，コントロールサーバはメッセージに基づいてミックスゾーンを定義する．DMLP は，路側機を用いることで車両の要求に応じてより多くの場所でミックスゾーンを形成することを

可能としている．しかし，DMLP ではミックスゾーン形成を路側機に依存しているために，路側機の数が不足している場合に仮名変更の位置やタイミングが限定され，位置プライバシの保護に重大な支障をきたす可能性がある．そして，路側機の十分な配備にはコストなどの問題が考えられる．加えて，DMLP では通信を導入した際の具体的な遅延時間について考慮されていないため，通信遅延によって仮名変更が失敗する可能性がある．

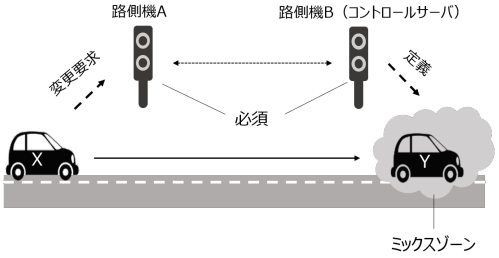

図 2　DMLP

3. 提案手法

路側機の数や通信遅延によって仮名変更が失敗することを防ぐために，本稿では VDMC を提案する．VDMC では，自動車ネットワークへの参加から車車間通信を行うまでの過程において Mod-IBS 手法を適用した認証付き仮名 ID 鍵通信を用いることで，識別化のために路側機を使用する必要が無くなる．加えて，通信遅延によって仮名変更が失敗することを防ぐために，2 段階ミックスゾーンを適応する．2 段階ミックスゾーンを採用することで，車両のミックスゾーン外への離脱を抑制することにより，仮名変更が失敗することを防ぐ．

3.1 提案手法のシステムモデル

図 3 に，提案のシステム構成と手順の流れを示す．提案手法の構成要素を以下に示す．

第三者信頼機関

各車両の参加先となる．仮名と秘密鍵のペアの生成パラメータの生成と生成結果の法的組織とコントロールサーバへの送付や，仮名と公開鍵のペアの生成とディレクトリサービスへの送付を行う．

コントロールサーバ

第三者信頼機関から仮名と秘密鍵のペアの生成パラメータを受け取って各車両に割り当てる．ミックスゾーンの候補地点を定義して車両に提供する．

ディレクトリサービス

第三者信頼機関から仮名と公開鍵のペアを受け取って格納しておく．ペアを車両に提供することで認証付き仮名 ID 鍵通信が可能となる．

法的組織

第三者信頼機関から仮名と秘密鍵のペアの集合を受け取って格納しておく．

車両

通信を行うための車載器と生成パラメータから仮名と秘密鍵のペアを生成するための疑似乱数生成器，位置情報を取得するための GPS デバイスの搭載を想定する．

以下では，提案手法の流れについて説明する．

(i) 各車両は信頼できる方法を用いて第三者信頼機関に登録を行う．

(ii) 第三者信頼機関は，コントロールサーバを通して各車両に仮名と秘密鍵のペアの生成パラメータやその他パラメータを割り当てる．

(iii) 各車両は生成パラメータを基にペアを生成し，認証付き仮名 ID 鍵通信を実施する．

(iv) 通信によって収集した情報を判断することによって各車両はミックスゾーンが形成可能かどうか判定する．

(v) 形成が可能であると判断した場合には車車間通信を用いて形成動作を行い，形成後は仮名変更のタイミングまでミックスゾーン維持動作を行う．

(vi) ミックスゾーンが維持されたまま仮名変更のタイミングを迎えた場合，ミックスゾーン範囲内の車両が協調同期して仮名を変更する．

ミックスゾーンの詳細について説明する．ミックスゾーンの候補地点はコントロールサーバによって定義され，十分かつ一様に配置される．そのため，ミックスゾーン候補の円領域は重複することが考えられるが，車両は複数のミックスゾーンに同時に参加することが可能で，参加しているミックスゾーン内で生じている全ての仮名変更に参加すると仮定する．また，同期仮名変更を行う車両の数が多いほど位置プライバシの保護の度合いは高まることから，十分な安全性を保つために同時に仮名変更を行うべき最低限の車両台数を閾値 k としてあらかじめ定めておく．

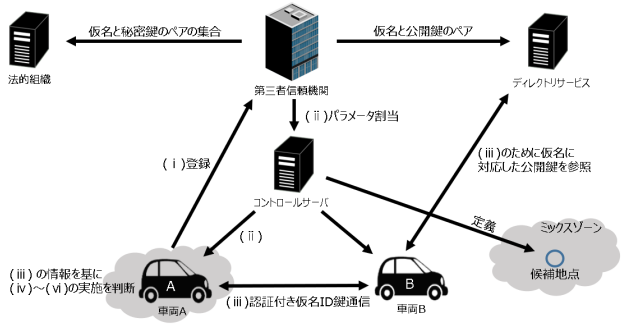

図 3　システムモデル

3.2 2 段階ミックスゾーン

VDMC では，通信遅延に対する許容水準を高めるために 2 段階ミックスゾーンを採用する．2 段階ミックスゾーンでは領域の形成と維持のために使用する半径として形成

半径と離脱半径の 2 種類を定義する．両半径の関係性を図 4 に示す．形成半径はミックスゾーンの形成開始時に領域の内外を隔てる半径を指し，離脱半径はミックスゾーン形成前の判定時や維持動作における判定時に領域の内外を隔てる半径を指す．また，候補地点を中心として形成半径によって形作られる円領域を形成判定領域，離脱半径によって形作られる円領域を維持判定領域と定義する．先行研究では車両速度から計算した予測位置に基づいてミックスゾーンの範囲を決定していたが，VDMC では車車間通信を通じた車両位置の把握によってミックスゾーンの形成と維持を判定することで車両の急な方向変化にも対応可能である等の利点があり，2 段階ミックスゾーンによって通信遅延時間における車両の移動にも配慮している．

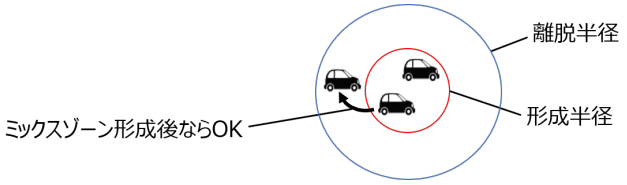

図 4　ミックスゾーン形成に関する 2 種類の半径

3.3　ミックスゾーン形成手順

図 5 に，提案方式におけるミックスゾーンの形成手順の全体像を示す．手順の詳細を以下に示す．なお，図中の番号は以下の手順に対応している．

(i) 各車両は走行中に一定時間間隔で情報収集メッセージを送信して，近隣車両に自身の存在を通知しながら周囲の車両数や位置情報を収集する．情報収集メッセージは送信時の仮名と位置情報を含む．

(ii) 形成判定領域の内部に定めた閾値 k 台以上の車両が存在する場合は，収集した情報を基に自車両が候補地点の最近傍車両であると判断した車両が自律的にミックスゾーンの形成動作を開始する．この際の最近傍車両をリーダ車両，その他のミックスゾーン参加候補車両をメンバ車両と定義する．定義されたリーダ車両は，仮名変更までに候補地点の最近傍車両でなくなった場合でも，維持判定領域の外部に出ない限りリーダ車両の役割を果たし続けるものとする．また，リーダ車両は形成開始時間を記録しておき，一定時間経過後に自分の仮名が変更されていない場合は，ミックスゾーン形成動作の中止のためメンバ車両にメッセージをマルチキャストする．

(iii) リーダ車両は全メンバ車両にミックスゾーンの形成動作を開始したことを伝えるメッセージをマルチキャストし，受信したメンバ車両は応答を返す．

(iv) 応答に含まれた位置情報からメンバ車両が維持判定領域の外部に出たかどうかの判定を行う．維持判定領域の外部に出た車両は近いうちに通信範囲外に出てしまう可能性が高く，応答時点で通信できていてもメンバ車両から除外する．除外することで仮名変更動作の完了の可能性を高めることが可能になる．

(v) リーダ車両が全メンバ車両からの応答を確認し，応答数が閾値を上回った場合はミックスゾーンを形成する．一方で，閾値を下回った場合は形成動作を中止する．

(vi) リーダ車両は全メンバ車両にミックスゾーンが形成されたことと仮名変更時間を伝えるメッセージをマルチキャストし，受信したメンバ車両は応答を返す．仮名変更時間は，マルチキャストのタイミングで現在時刻を取得して適切な時間後に設定される．同時に，リーダ車両は仮名変更判定時間を設定する．仮名変更判定時間は仮名変更時間の一定時間前に設定される．仮名変更時間と仮名変更判定時間の設定は 1 度だけ行う．

(vii) 応答に含まれた位置情報からメンバ車両が維持判定領域の外部に出たかどうかの判定を行う．維持判定領域の外部に出た車両はメンバ車両から除外する．

(viii) ミックスゾーン形成以後の動作を仮名変更判定時間まで繰り返し，応答数が閾値を下回った場合は形成動作を中止する．

(ix) 仮名変更判定時間を迎えた場合は仮名変更実施決定フェーズに切り替わり，応答数が閾値を上回ったままであれば以降の閾値の判定は行わずに仮名変更の実施を決定する．

(x) 仮名変更時間を迎えると仮名変更フェーズに切り替わり，同期的に仮名を変更する．同期仮名変更の際，各車両は第三者信頼機関から割り当てられた各パラメータと自身の所有する疑似乱数生成器を用いて新しい仮名を生成する．仮名変更が完了したとき，変更前の仮名は失効してディレクトリサービスから削除される．

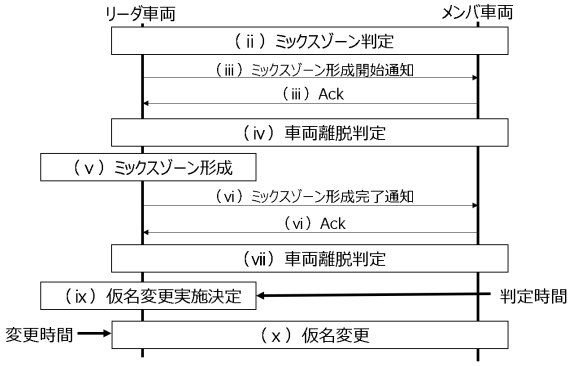

図 5　シーケンス図

4.　評価

本章では，車両が移動する環境を想定したシミュレーションにより，VDMC の性能評価を行う．また，通信完

了率と仮名変更回数を指標として，2 段階ミックスゾーンの有無に関する比較を行う．

4.1 シミュレーション環境

シミュレーションに用いたマップを図 6 に示す．本評価では，ミックスゾーンの単体性能を確認するため，マップの中心にミックスゾーンの候補地点を 1 点のみ設置した．シミュレーション諸元を表 1 に示す．通信シミュレータ Scenargie[10] を用いてシミュレーションを行った．また，代表的な交通シミュレータである SUMO においてシナリオ化されているルクセンブルクの車両密度を参照し，車両台数は 151 台とした．形成半径は最小 10m，最大 300m の範囲を 10m 刻みで変化させた．形成半径の最大値を 300m とした理由は，IEEE802.11p における無線伝播距離の最低限が約 300m となっているためである．1 つの形成半径値に対して 10 種類のシードで各 10 回の計 100 回シミュレーションを実行した．

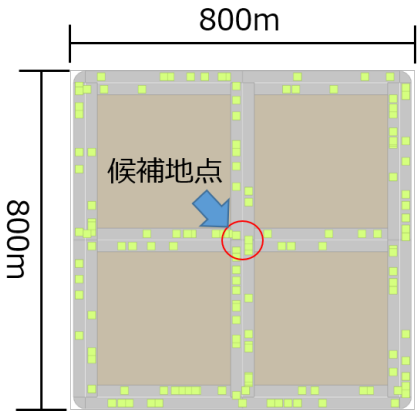

図 6 シミュレーションマップ

表 1 シミュレーション諸元

パラメータ	値
通信シミュレータ	Scenargie
通信規格	IEEE 802.11p
チャネル周波数	5.9GHz
通信帯域幅	10MHz
伝播伝搬モデル	ITU-R_P.141
送信電力	10dBm
シミュレーション時間	1000 秒
車両位置判定周期	0.1 秒
パケットサイズ	256Byte
モビリティ	GIS-Based-Random-Waypoint
車両台数	151 台
閾値	10 台
形成半径	10，20，30，・・・，300m

4.2 評価対象と評価項目

従来手法と提案手法に関して以下の 2 点について評価した．2 段階ミックスゾーンを採用しない手法を従来手法，採用する手法を提案手法とする．

形成半径に対するミックスゾーンの性能

形成半径の変化に対するミックスゾーンの性能の変化を評価することによって，ミックスゾーンが性能を十分に発揮するための適切な形成半径値について検討する．

従来手法と提案手法に関しての通信による影響の比較

2 段階ミックスゾーンの有無に関してミックスゾーンの性能を比較することで，従来手法と比べて提案手法が通信遅延による影響を抑制できていることを確認する．従来手法では通信の遅延を考慮していないことから決定したミックスゾーン範囲が変化することはないため，形成半径と離脱半径を等しいものとした．提案手法では形成半径を変化させる一方で離脱半径は 300m で固定した．

ミックスゾーンの性能を評価する際の指標を通信完了率と仮名変更回数にした．

通信完了率

通信を試み，実際に仮名が変更される割合について評価を行った．通信完了率は式（1）で求めた．

$$\text{通信完了率} = \frac{\text{仮名が変更された回数}}{\text{通信試行回数}} \tag{1}$$

ここで通信試行回数は，リーダ車両が形成動作の開始を伝えるマルチキャストの回数に等しいものとした．

仮名変更回数

シミュレーション時間の間での，仮名が変更された回数について評価を行った．

4.3 形成半径に対する通信完了率

図 7 に形成半径に対する通信完了率を示す．形成半径に対するミックスゾーンの性能についての観点では，図より形成半径が 160m 以下の場合，提案手法は通信完了率 50% 以上で達成できることを確認できる．一方で，図より提案手法では形成半径が 240m 以上の場合のみ，通信完了率が 25%を下回ることが分かる．通信完了率が低下する原因として，シーケンスの途中での車両の離脱による形成動作の中止が考えられる．また，従来手法と提案手法に関しての通信による影響の比較の観点では，図より提案手法は形成半径値によらず，従来手法よりも高い通信完了率を得られることが分かる．確率の差分で見ると，通信完了率が平均で約 15%上昇したことが確認できる．これは，提案手法が形成動作の中止を抑制しているためであると考えられる．

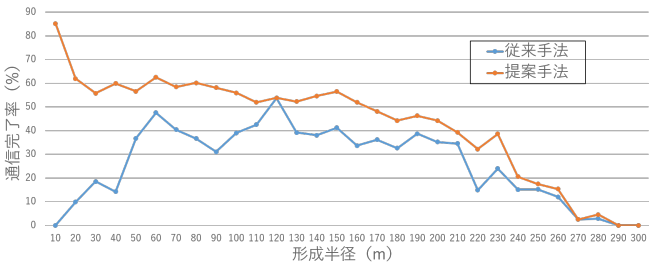

図 7　形成半径に対する通信完了率

4.4　形成半径に対する仮名変更回数

図 8 に形成半径に対する仮名変更回数を示す．形成半径に対するミックスゾーンの性能についての観点では，図より形成半径が 60m 以上 180m 以下の場合，提案手法は仮名変更回数 35 回以上で達成できることを確認できる．一方で，図より提案手法では形成半径が 40m 以下や 210m 以上の場合，仮名変更回数が 20 回を下回ることが分かる．仮名変更回数が減少する原因として，シーケンスの途中での車両の離脱による形成動作の中止や通信試行回数の減少が考えられる．また，従来手法と提案手法に関しての通信による影響の比較の観点では，図より提案手法における仮名変更回数が従来手法を上回っていることが分かる．仮名変更回数の上昇値は平均で約 8.3 倍となったことが確認できる．これは，提案手法が形成動作の中止を抑制しているためであると考えられる．

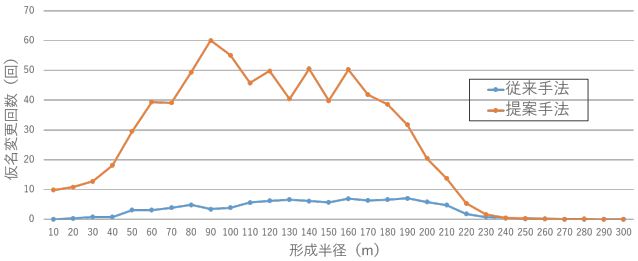

図 8　形成半径に対する仮名変更回数

5.　おわりに

本稿では通信遅延を考慮した密度ベースの動的仮名変更手法である VDMC を提案した．自動車ネットワークへの参加から車車間通信を行うまでの過程において Mod-IBS 手法を適用した認証付き仮名 ID 鍵通信を用いることで，ミックスゾーンの形成における路側機の必要性を取り除いた．また，ミックスゾーンを 2 段階に設けることで通信遅延発生時にミックスゾーンの形成が失敗することを防いだ．

特性評価にて，形成半径が 160m 以下の場合には，提案手法は通信完了率 50%以上で達成できることを確認できた．また，従来手法と比較した場合，提案手法において通信完了率の約 15%の上昇が確認できた．同様に，形成半径が 60m 以上 180m 以下の場合には，提案手法は仮名変更回数 35 回以上で達成できることを確認できた．また，従来手法と比較した場合，提案手法において仮名変更回数が約 8.3 倍となることが確認できた．

以上より，VDMC は形成半径を適切に設定することで十分なミックスゾーン性能を発揮し，従来手法と比較して通信遅延の影響も抑えることで，位置プライバシの保護が可能となっていることを確認した．

謝辞　本研究は JSPS 科研費 JP20H04180 の助成を受けたものです．

参考文献

[1] R.L. Finn, D. Wright, and M. Friedewald, ”Seven Types of Privacy,” Springer Netherlands, Dordrecht, pp.3-32, 2013.

[2] D. Makrakis, B. Ying, and H.T. Mouftah, ”Dynamic mix zone for location privacy in vehicular networks.,” IEEE Communications Letters, Vol. 17, No. 8, pp.1524-1527, Aug 2013.

[3] S. Zhao, A. Aggarwal, R. Frost and X. Bai, ”A survey of applications of identity-based cryptography in mobile ad-hoc networks,” IEEE Communications Surveys Tutorials, vol. 14, no. 2, pp.380-400, Second 2012.

[4] L. Zhang, C. Hu, Q. Hu, J. Domingo-Ferrer and B. Qin, ”Privacypreserving vehicular communication authentication with hierarchical aggregation and fast response,” IEEE Transactions on Computers, vol. 65, no. 8, pp. 2562–2574, Aug 2016.

[5] V.P. Kafle, Y. Fukushima, P. Martinez-Julia and H. Harai, ”Design of scalable directory service for future iot applications,” InProceedings of 2016 ITU Kaleidoscope: ICTs for a Sustainable World (ITU WT), pp.1-7, Nov 2016.

[6] Y. Fukushima, V.P. Kafle, and H. Harai, ”Pseudonym and key management scheme for supporting social smart applications,” IEICE Transactions on Communications, Vol. advpub, 2018.

[7] M. Li, K. Sampigethaya, L. Huang and R. Poovendran, ’Swing & swap: user-centric approaches towards maximizing location privacy,” InProceedings of the 5th ACM workshop on Privacy in electronic society, pp.19-28, 2006.

[8] L. Buttyán, T. Holczer, and I. Harai, ”On the effectiveness of changing pseudonyms to provide location privacy in vanets.” In Stajano, F. Meadows, C. Capkun, S. Moore, and Tyler, editors, Proceedings of Security and Privacy in Ad-hoc and Sensor Networks, pp.129-141, Berlin, Heidelberg, 2007. Springer Berlin Heidelberg.

[9] R. Lu, X. Lin, T.H. Luan, X. Liang and X. Shen, ”Pseudonym changing at social spots: An effective strategy for location privacy in vanets,” IEEE Transactions on Vehicular Technology, Vol. 61, No. 1, pp.86-96, Jan 2012.

[10] 大和田泰伯, 前野誉, 金田茂, 久永良介, 高井峰生. ”Scenargie を用いた its シミュレーション,” マルチメディア通信と分散処理ワークショップ論文集, pp.233-234, Dec 2008.