Vol.2019-ITS-78 No.6
2019/9/6

自動車ネットワークにおける位置プライバシ保護のための車両密度を考慮した仮名変更方式の検討

團 皆人[1,a)]　岡部 友介[1]　重野 寛[1,b)]

概要：
高度交通システム（ITS）において，車車間通信や路車間通信などを利用したアプリケーションでは通信に位置情報を含むものがある. 攻撃者に位置情報を含む通信を盗聴された場合, 車両の行動を追跡することにより車両の位置プライバシが侵害される危険性がある. 位置プライバシ保護のための手法として仮名があり, 車両の固有識別子の代わりに時間経過により変化する仮名を通信に用いることで車両の追跡を困難にする. しかし, 単純な仮名変更では攻撃者に変更前の仮名と変更後の仮名を紐づけられる危険性がある. 本研究では, 自動車ネットワークにおける位置プライバシ保護のための車両密度を考慮した仮名変更方式を提案する. 提案方式では, 特定の領域内で複数台の車両が同期して仮名を変更することでプライバシ保護を行う. また, 提案方式のプライバシに関するシミュレーション評価を行った.

A Pseudonym Change Scheme Considering Vehicle Density for Preserving Location Privacy in Vehicular Network

1. はじめに

近年，高度道路交通システム（Intellijent Transport Systems: ITS）の分野において，車車間通信や路車間通信などの通信技術が研究されている．これらの通信技術を用いたアプリケーションでは車両の位置情報や個人情報を利用するものも多く，自動車ネットワークにおけるプライバシ保護が重要となっている．Finn ら [1] はプライバシを行動や位置，思考など 7 つのタイプに分類しており，本稿では位置プライバシに焦点を当てる．

攻撃者に位置情報を含む車車間（V2V）通信を盗聴された場合，車両の位置プライバシが侵害される危険性がある．位置プライバシ保護のための有効な保護手法として，仮名 [2] を用いた手法が知られている．仮名とは，通信の送信者および受信者が固有識別子の代わりに使用する時間経過により変化する識別子である．仮名を識別子に用いて頻繁に変更することで特定車両のデータパケットを追跡することが困難となり，位置プライバシを保護することができる．仮名を用いた方式では仮名変更頻度や仮名変更タイミングが重要なパラメータである．

仮名を自動車ネットワークに仮名を導入する際には，信頼できる機関および車両からの識別化と，攻撃者からの非識別化が要求される．信頼できる機関および車両からの識別化とは，管理機関が車両に対して正当な車両であるか身元の検証ができることであり，暗号文の生成者を特定可能にすることで悪意のある車両からの偽情報発信を防ぐことが可能となる．識別化は，身元を検証する認証性，管理機関のみが検証可能であるという機密性，暗号文の生成者が特定可能である否認不可性を提供する．攻撃者からの非識別化とは，攻撃者に対して身元を隠す仕組みであり，攻撃者の盗聴による車両の走行情報の収集を防ぐことが目的である．非識別化は，攻撃者から身元を隠す仮名性と，車両の追跡を防ぐリンク不能性を提供する．

本稿では，自動車ネットワークにおける位置プライバシ保護のための車両密度を考慮した仮名変更方式を提案する．提案する仮名変更方式では，車両は第三者信頼機関（TA）のコントロールサーバが地図上に一様に定義する円領域内にて仮名変更を行う．車両は任意地点の円領域に参加可能であり，周辺車両と通信することで車両密度を考慮した動

[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
[a)] dan@mos.ics.keio.ac.jp
[b)] shigeno@mos.ics.keio.ac.jp

的な仮名変更を行い，プライバシを保護する．また，提案方式についてプライバシレベルの指標を用いてシミュレーション評価を行う．

以下本稿では，2 章において関連手法について述べ，3 章で仮名変更方式を提案し，4 章でシミュレーションによる評価結果を示す．最後に 5 章で結論を述べる．

2. 関連研究

2.1 仮名

位置プライバシ保護のための有効な手法として仮名 [2] が知られている．仮名とは，通信の送信者および受信者は固有識別子の代わりに使用する時間経過により変化する識別子である．固有識別子を使用している場合，攻撃者は無線媒体を介して送信されているデータパケットを連続的に監視し，特定のユーザが送信しているデータパケットを収集することで，車両の行動を追跡することが可能である．これにより，ユーザの位置プライバシが侵害される危険性がある．しかし，仮名を識別子に用いて頻繁に変更することで特定車両のデータパケットを収集することが困難となり，ユーザの位置プライバシを保護することが可能である．

2.1.1 自動車ネットワークへの仮名の導入

自動車ネットワークに仮名を導入するには攻撃者からの非識別化と，信頼できる機関および車両からの識別化が要求される．

攻撃者からの非識別化は攻撃車に対して身元を隠す仕組みであり，攻撃者の盗聴による車両の走行情報収集を防ぐことが目的である．非識別化は，身元を隠す匿名性，車両の追跡を防ぐリンク不能性を提供する．仮名を識別子に用いて頻繁に変更することで非識別化を達成できるが，仮名の変更タイミングを攻撃者が知っている場合，変更前と後の仮名を紐付けることが可能であり，攻撃車に車両の行動を追跡される危険性がある．たとえば図 1(a) において，攻撃者が仮名 A から仮名 Z への仮名変更タイミングを検知できた場合，仮名 A と仮名 Z を持つ車両が同一車両であることを判別可能である．そのため，仮名変更において変更頻度や変更タイミングは重要なパラメータであり，適切に設定することで攻撃者からの追跡を回避するのに十分なプライバシレベルを保つことができる．たとえば図 1(b) では，仮名 A,B,C をもつ車両の仮名変更タイミングを同期することで，攻撃者による仮名変更前後の各車両の仮名の紐づけが困難となる．

この仮名変更頻度や仮名変更タイミングなどのパラメータを決定するにあたり，さまざまな仮名変更戦略が研究されている．一定時間ごとに仮名を変更する固定時間変化方式 [3] はタイミング予測や単一車両の仮名変更の追跡が容易という問題点がある．本稿では，近隣の車両密度に基づいて変更する密度ベース方式 [4]，近隣の車両と同時に仮名を変更する協調同期変更方式 [5] に焦点を当てる．既存の協調同期変更方式 [5] では，交差点や駐車場などのソーシャルスポットに存在する車両が同期して仮名変更を行うことが想定されているが，本稿では，ソーシャルスポットや路側気などの物理的設備を必要としない仮名変更方式を提案する．

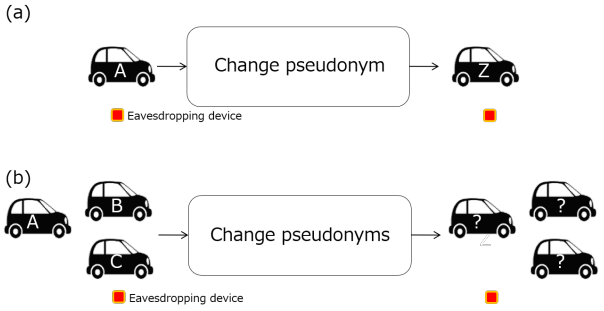

図 1 仮名変更

信頼できる機関および車両からの識別化とは，管理機関がある車両に対して正当な車両であるか検証できることである．通信に用いる暗号文の生成者を特定可能にすることで，サービス外の悪意のあるユーザによる偽情報発信を防ぐことが可能となる．識別化は，身元を検証する認証性と，特定の機関のみが検証可能である機密性，暗号文の生成者が特定可能である否認不可性を提供する．本稿では ID ベース暗号を応用した認証付き仮名 ID[6] 用いることにより識別化を達成する．

2.2 ID ベース暗号

ID ベース暗号（IBS）[7] は，共通パラメータと受信者の ID を用いて暗号化する方式である．ID ベース通信では，受信者の ID を公開鍵暗号方式における公開鍵のように利用することで，受信者のみが復号できる暗号文を生成することが可能である．

2.2.1 mod-IBS

mod-IBS 方式 [8] は，ID ベース暗号に基づいたデータ量の少ない仮名/秘密鍵ペア生成パラメータの割当管理方式である．mod-IBS 方式はコントロールサーバが配布するデータ量が少なく，車両が仮名と秘密鍵を再生成可能という特徴があるため，時間経過で変化する仮名を利用する場合に適している．mod-IBS 方式を応用した認証付き仮名 ID を通信の流れを図 2 に示す．TA などのコントロールサーバは，車両 A と車両 B に対して個別パラメータと共通パラメータを割り当てる．車両は個別・共通パラメータと自身が所有する乱数生成器から，複数個の仮名と秘密鍵のペアを生成することができる．また，生成した情報と信頼できるディレクトリサービスが配布する公開鍵を利用することで，車両同士は仮名による ID ベース通信が可能となる．ディレクトリサービスが信頼できる場合，mod-IBS 方式の安全性は ID ベース暗号と等価である．

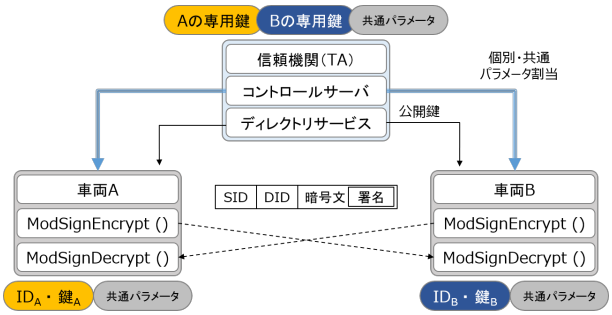

図 2　mod-IBS 方式の流れ

3. 提案

本稿では，自動車ネットワークにおける位置プライバシ保護のための車両密度を考慮した仮名変更方式を提案する．

3.1 提案概要

本稿では 2.1.1 で述べたように攻撃者からの非識別化と信頼できる機関および車両からの識別化を満たす，位置プライバシ保護のための車両密度を考慮した仮名変更方式を提案する．提案方式では，mod-IBS 方式 [8] を応用した仮名 ID を用いた通信を利用することで，認証性，機密性，否認不可性を提供する．管理機関が車両の正当性を検証できることによって，悪意のある情報発信を防ぐことが可能である．また，車両は図 4 に示すような地図上に配置される特定の円領域内にて，複数車両が同期して仮名変更を行うことで，仮名性，匿名性，リンク不能性を提供する．これにより，攻撃車の盗聴による車両の走行情報の収集を防ぐことが可能である．提案方式では特定の円領域をソーシャルスポット（駐車場，交差点）のような物理的な設備に配置するのではなく，コントロールサーバと呼ばれる TA から車両への通知を行う設備によって候補地点が地図上に一様に定義される．候補地点はすべての車両に通知されており，車両は任意候補地点において車両密度ベースの仮名変更が可能となる．

3.2 システムモデル

提案手法のシステムモデルを図 3 に示す．提案手法のシステムモデルは TA(Trustable Authority)，コントロールサーバ，ディレクトリサービス，車両，法的組織，攻撃者の 6 つの要素で構成されている．

TA は第三者信頼機関であり，仮名/公開鍵のペアの生成，および各車両への仮名/秘密鍵生成パラメータの生成をおこなう．生成された仮名は TA によって認証され，後述のディレクトリサービスに格納される．コントロールサーバは TA が生成した仮名/秘密鍵生成パラメータの各車両への割当て，および候補地点定義，車両への通知を行う．ディレクトリサービスは，各車両への仮名と公開鍵のペアの提供，およびすべての仮名のライフタイムの制御を行う．ディレクトリサービスはセキュアに管理されたサービスであると想定する．車両はアプリケーションサービスプロバイダやセルラネットワークオペレータなどの法的組織から認可された組織，および TA に信頼されており，無線通信機器，擬似乱数生成器および GPS デバイスを搭載していると想定する．また，車両はセルラ通信を用いてコントロールサーバと通信可能であり，車車間（V2V）通信では仮名を用いた ID ベース通信を使用すると想定する．

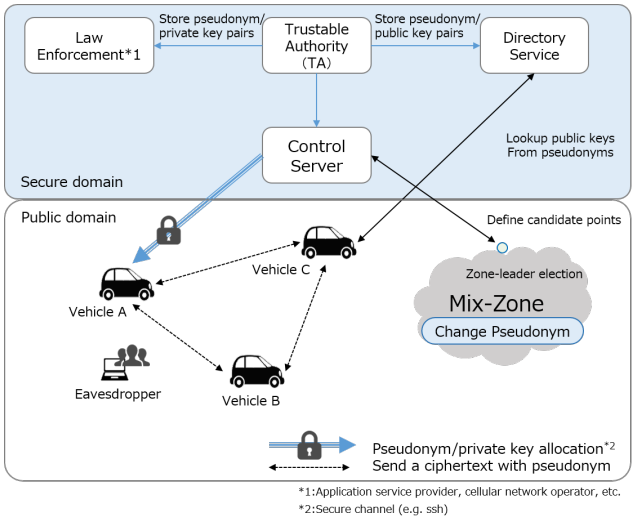

図 3　システムモデル

3.3 仮名変更の手順

提案手法の流れを以下に示す．

(1) 車両の登録

各車両はネットワークに参加時に，保障された認証方法 [9] を使用して TA に登録される．

(2) 車両への仮名 ID/秘密鍵ペア生成パラメータの割当

TA は mod-IBS 方式により軽量な仮名 ID/鍵ペア生成パラメータを生成し，それらを各車両に割り当てる．

(3) 車両による仮名 ID/秘密鍵ペアの生成

車両は TA から割り当てられた生成パラメータと擬似乱数生成器を使用して，複数の仮名 ID/秘密鍵生成パラメータを生成する．また，ID ベース署名暗号を利用した認証付き仮名 ID 通信を行う．

(4) 円領域の形成

コントロールサーバは候補地点を定義する．また，候補地点から最も近い車両は自身をゾーンリーダー車両に自律的に決定する．複数台の車両が円領域に参加可能な場合に円領域を形成する．

(5) 同期仮名変更

円領域内の車両は自身を含む複数台の車両と同期して仮名変更を行う．

3.4 円領域形成

候補地点は図 4 のようにコントロールサーバによって地図上に一様に配置され，候補地点を中心とした半径 R の円領域内に複数台の車両が存在するとき円領域が形成される．円領域は重複しており，車両は複数の円領域に同時に参加可能である．このとき，車両は自身が参加しているすべての円領域の仮名変更に参加するものとする．候補地点から最も近い車両はゾーンリーダー車両に選出され，円領域に参加するその他の車両はメンバー車両となる．円領域維持の条件は，指定された期間 T の間に各時刻 t における最小台数が一定の閾値を下回らないことである．以下に円領域形成の手順を示す．

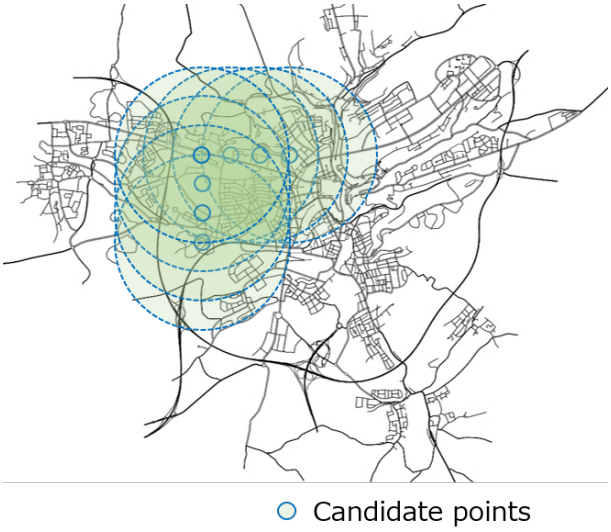

図 4 LuST シミュレーションマップと候補地点

(1) 近隣車両探索

各車両は仮名の有効期限が近づくと，円領域への参加意思表明として隣接車両に仮名と位置情報を含むメッセージを送信して自身の存在の通知し，隣接車両の情報収集を行う．収集した情報は自身の隣接テーブルに格納して，円領域形成に利用する．

(2) ゾーンリーダー車両の決定

各車両は隣接テーブルを参照し，コントロールサーバによってあらかじめ定義された候補地点の最近傍車両をゾーンリーダー車両に決定する．自信が最も候補地点に近い場合，自身を自律的にゾーンリーダー車両に決定する．

(3) リーダーアナウンス

ゾーンリーダー車両が，自身がゾーンリーダー車両であることを近隣の車両に通知する．

(4) 参加リクエスト

ゾーンリーダー車両から通知を受け取った円領域内の車両は，円領域に参加するためにゾーンリーダー車両へ参加リクエストを送信する．そして，参加メッセージを受け取ったゾーンリーダー車両は次に仮名変更を行う時刻を送り返す．仮名変更時刻を受け取った車両はメンバー車両として円領域に参加する．

(5) 円領域形成および維持

ゾーンリーダー車両は，円領域内に自身とメンバー車両が合わせて閾値台以上存在するかを評価する．メンバー車両は Alive メッセージを定期的に送信する．リンクが損失した場合，最初のステップに戻り再度円領域形成を行う．

3.5 同期仮名変更

円領域内の複数台の車両は，あらかじめゾーンリーダー車両から通知された毛名変更時刻に同時に仮名変更を行う．以下に同期仮名変更の手順を示す．

(1) 円領域参加

3.4 節の手順に従い，メンバー車両はゾーンリーダー車両から仮名変更時刻 t_{change} を受け取り，円領域に参加する．

(2) 同期仮名変更

円領域内の各車両は，自身の擬似乱数生成器とネットワーク参加時に TA から割当てられた仮名 ID/秘密鍵ペア生成パラメータを利用して新しい仮名と秘密鍵を生成する．その後，円領域内のすべての車両が時刻 t_{change} に仮名変更を行う．

(3) 仮名/秘密鍵の失効

仮名変更後，各車両が変更時刻 t_{change} までに使用していた仮名は失効される．TA はディレクトリサービスから対応するエントリを削除する．

4. シミュレーション評価

本章では提案手法について都市部を対象としたシミュレーションを行い，プライバシついて評価する．

4.1 シミュレーション環境

評価には交通流シミュレータ SUMO [10] と，ルクセンブルグの 24 時間のトラフィックを再現した LuST 交通シナリオ [11] を用いた．シミュレーションマップを図 4 に示す．全ての車両は無線通信機器を搭載しており，車車間の無線接続性を 300m と仮定し，SUMO から 1 秒周期で出力される車両のトレースデータを解析した．サンプル車両は 24 時間と，ピーク (8:00-8:10am)，オフピーク (3:00-3:10am) の時間帯に存在する車両とし，それぞれ車両台数は 9067 台と 663 台であった．コントロールサーバが定義するシステムパラメータとして，候補地点の配置間隔を $100m$，円領域の半径を $R = 300m$，円領域形成閾値を $k = 3, 10$ で評価した．シミュレーションに用いたパラメータを表 1 に示す．

4.2 匿名セット数

ピーク時とオフピーク時の 10 分間の走行で，車両が円領域内での仮名変更で得た匿名セット数について調査した．仮名の有効期限および変更周期は 60 秒であり，円領域を

表 1　Parameters for Evaluation.

Parameters	Settings
Traffic flow simulator	SUMO[10]
Data set	LuST[11]
Map	Luxembourg
Map size	$156km^2$
Time	24 hours, peak and off peak
Communication range	$300m$
Number of vehicles	663-9067
Interval of candidate points c_i	$100m$
Zone radius R	$300m$
Zone formation threshold k	$3, 10$

形成する閾値 $k = 10$ を設定した．図 5 は仮名変更と平均匿名セット数のグラフである．ピーク時では変更を重ねる毎に匿名セット数が増加しており，10 回の仮名変更で系内の車両は平均匿名セットサイズ 263 を得ている．これは車両が円領域に十分にアクセス可能であり，周辺車両と協調仮名変更が可能であること示す．一方，オフピークでは円領域の形成が困難であるため，匿名セット数は仮名変更を繰り返しても低い値で推移する．オフピークのような車両数が少ない時間帯では，形成閾値 k の調整やより頻繁な仮名変更が必要であることが分かった．

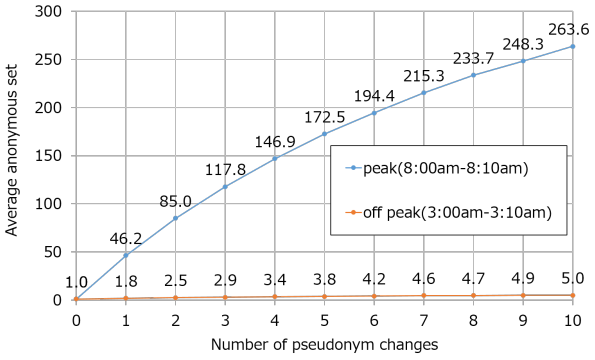

図 5　仮名変更と匿名セットの関係

4.3　エントロピー

円領域内でターゲットを特定するエントロピー H_p を評価する．エントロピーは車両の匿名化度合いを表し，数値が大きいほど匿名化されている．A はゾーン内の全ての車両の集合，P はターゲット車両，p_i が車両 i が P である確率，H_p が集合 A 内のターゲット P を特定するエントロピーとする．

エントロピーの計測結果を図 6 に示す．仮名の有効期限および変更周期は 60 秒であり，円領域を形成する閾値を $k = 3, 10$ に設定した．グラフによると，オフピーク時では円領域の形成閾値 $k = 10$ の場合，条件を満たした候補地点は 5 つであった．そのため車両が円領域にアクセスするのは難しく，エントロピーは 0 付近の値を推移する．オフピーク時のような車両が少ない状況では，円領域形成閾値 k を低く設定する必要がある．また，形成閾値を $k = 3$ に設定したとき円領域を形成可能な候補地点は 137 に増加したことを確認した．同時にエントロピーも増加し，1 付近を安定して推移している．この結果より，ゾーン形成閾値の調整がエントロピーを増加させ，プライバシレベルに寄与することが確認できた．ピークでは車両が円領域に容易にアクセス可能で複数の車両が同期仮名変更に協力できるため，車両は 5 回の仮名変更を経てエントロピーが 5 を超えている．エントロピーが増加することで，ターゲット車両の識別性が低下している．

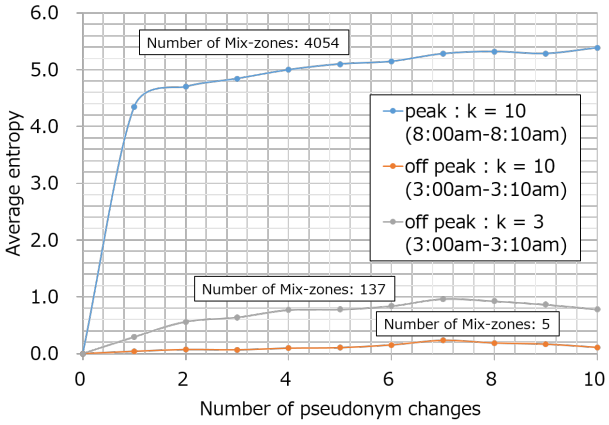

図 6　仮名変更とエントロピーの関係

5.　おわりに

本稿では，自動車ネットワークにおける位置プライバシ保護のための車両密度を考慮した仮名変更手法を提案した．提案方式では仮名を用いた通信を利用することで管理機関からの識別化を達成し，提案した仮名変更方式により攻撃者からの非識別化を達成する．また，車両は円領域内で複数台の車両と同期して仮名変更を行うことでプライバシ保護を行う，

提案手法について都市部を対象としたシミュレーションを行い，プライバシについて評価を行った．ピーク時では変更を重ねる毎に匿名セット数が増加しており，10 回の仮名変更で系内の車両は平均匿名セットサイズ 263 を得た．この結果から，車両が円領域に十分にアクセス可能であり，周辺車両と協調仮名変更が可能であることを確認した．また，車両は円領域内で仮名変更をすることでエントロピーが増加し，識別性が低下することを確認した．

以上より，提案方式はプライバシの観点から有用であることを示した．

謝辞　本研究は JSPS 科研費 16H02811 の助成を受けたものです．

参考文献

[1] Finn, Rachel L.and Wright, Davidand Friedewald, and Michael. *Seven Types of Privacy*, pp. 3–32. Springer Netherlands, Dordrecht, 2013.

[2] J. Petit, F. Schaub, M. Feiri, and F. Kargl. Pseudonym schemes in vehicular networks: A survey. *IEEE Communications Surveys Tutorials*, Vol. 17, No. 1, pp. 228–255, Firstquarter 2015.

[3] D. Eckhoff, C. Sommer, T. Gansen, R. German, and F. Dressler. Strong and affordable location privacy in vanets: Identity diffusion using time-slots and swapping. In *Proceedings of 2010 IEEE Vehicular Networking Conference*, pp. 174–181, Dec 2010.

[4] B. K. Chaurasia and S. Verma. Optimizing pseudonym updation for anonymity in vanets. In *Proceedings of 2008 IEEE Asia-Pacific Services Computing Conference*, pp. 1633–1637, Dec 2008.

[5] R. Lu, X. Lin, T. H. Luan, X. Liang, and X. Shen. Anonymity analysis on social spot based pseudonym changing for location privacy in vanets. In *Proceedings of 2011 IEEE International Conference on Communications (ICC)*, pp. 1–5, June 2011.

[6] John Chen, Liqunand Malone-Lee. Improved identity-based signcryption. In Serge Vaudenay, editor, *Proceedings of Public Key Cryptography - PKC 2005*, pp. 362–379, Berlin, Heidelberg, 2005. Springer Berlin Heidelberg.

[7] L. Zhang, C. Hu, Q. Wu, J. Domingo-Ferrer, and B. Qin. Privacy-preserving vehicular communication authentication with hierarchical aggregation and fast response. *IEEE Transactions on Computers*, Vol. 65, No. 8, pp. 2562–2574, Aug 2016.

[8] Yusuke Fukushima, Ved P. Kafle, and Hiroaki Harai. Pseudonym and key management scheme for supporting social smart applications. *IEICE Transactions on Communications*, Vol. advpub, , 2018.

[9] Hasnaa Moustafa, Gilles Bourdon, and Yvon Gourhant. AAA in vehicular communication on highways with ad hoc networking support: A proposed architecture. In *Proceedings of the 2Nd ACM International Workshop on Vehicular Ad Hoc Networks*, VANET '05, pp. 79–80, New York, NY, USA, 2005. ACM.

[10] Daniel Krajzewicz and Jakob Erdmann and Michael Behrisch and Laura Bieker. Recent Development and Applications of SUMO - Simulation of Urban MObility. *International Journal On Advances in Systems and Measurements*, Vol. 5, No. 3&4, pp. 128–138, 2012.

[11] L. Codeca, R. Frank, and T. Engel. Luxembourg sumo traffic (lust) scenario: 24 hours of mobility for vehicular networking research. In *Proceedings of 2015 IEEE Vehicular Networking Conference (VNC)*, pp. 1–8, Dec 2015.