「マルチメディア，分散，協調とモバイル
(DICOMO2017) シンポジウム」 平成29年6月

車両位置相互監視によるV2X通信なりすまし検知手法

東 峻太朗[1] 野村 晃啓[1] 塚田 学[2] 佐藤 健哉[1]

概要：
V2V 通信の発展により，衝突防止支援や追従走行支援といった安全運転支援が実現している．さらに近年では，路車間や歩車間通信の他に，携帯回線を用いたクラウドとの通信も可能となり，これらを総じてV2X 通信と呼ぶ．クラウドを介し，V2V 通信可能範囲外の車両と通信可能である他，V2V 通信によって得た情報をクラウドに送信することで，自車両の周辺情報をクラウド上で他車両と共有することも可能である．しかし，不適切な情報がクラウドに与える影響を考慮する必要がある．自身の車両情報を偽ることで，クラウドを利用したシステムを攻撃することができ，故意に渋滞や事故を誘発することが可能である．本研究では，V2X 通信を行い車両の周辺情報を利用することで，クラウドに集約されるデータから，不正データを検知する手法を提案する．クラウドへの送信データに対し，考え得る脅威や求められる要件を分析し，本研究が取り組むべき問題を明らかにした上で，提案手法の実装による評価を算出する．その結果，不正データを 93% 検出することができ，さらに車密度を考慮し提案手法の閾値を増加させることで，検知率を 100% にすることが可能となった．周辺環境に応じてデータの信頼性を保証する効果が高まることを示した他，提案手法のフォールスホジティブや実行処理時間を示し，提案手法が現実的であるかどうかの評価結果も算出した．

A Detection Method for V2X Communication Spoofing with Mutual Vehicle Position Monitoring

SHUNTARO AZUMA[1] TERUAKI NOMURA[1] MANABU TSUKADA[2] KENYA SATO[1]

1. はじめに

近年，ITS の分野において，自動運転や車車間通信の研究が盛んに行われている．車両は，VANET（Vehicular Ad hoc Network）を利用した車車間通信（V2V 通信）を行うことができる他，路側機と通信を行う路車間通信（V2I 通信）や，歩行者の所有しているタブレット端末との通信（V2P 通信），携帯回線を利用したクラウドとの通信（V2C 通信）を行うことができ，これらの総じて V2X 通信という．車両が V2X 通信を行うことで，クラウドは様々な情報を収集することができ，道路情報・車両情報の一括管理から，協調型運転支援のための LDM(Local Dynamic Map) の作成 [1] や，運転実績の集計・運転傾向の分析から集計業務，日報入力の簡素化といった管理業務の簡素化など，様々なシステムやサービスを提供することができる．

一方，クラウドを利用したシステムにおいて，クラウドに対する不正なデータ転送がシステムに大きな影響を与えてしまう [2]．クラウドに対する故意な不正データの転送・クラッキング行為がここ最近で増加の一途をたどっている [3] ことから，クラウドを利用した安全運転支援サービスに対する攻撃も脅威となる．攻撃者が，道路上で事故車両を装ったなりすまし情報をクラウドに送信することで，道路を封鎖，あるいは渋滞を引き起こすことができる．

本論文タイトルにある「なりすまし」とは，車両がクラウドに不正なデータを送信する行為と定義する．車両なりすまし行為として，走行情報の偽装や位置情報の偽装 [4]，車両状態の偽装など様々な偽装行為がある．本研究では，車両が V2X 通信を行うことで，車両の位置情報を周囲と相互監視し，クラウドが車両から受け取るデータから，不正なデータを検知することを目的とする．

[1] 同志社大学大学院 理工学研究科 情報工学専攻
[2] 東京大学大学院 情報理工学系研究科

表 1　データ送信に関する各種分析

脅威		要件	対処例
盗聴		秘匿性	暗号化
改ざん		完全性	暗号化
なりすまし	車両なり代わり	ノード信頼性	PKI
	データ偽装	データ信頼性	本研究の対象

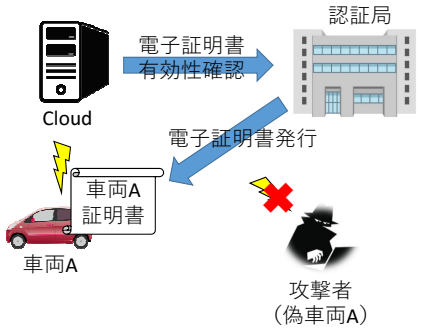


図 1　車両に適応する公開鍵基盤手法 (PKI) の概要

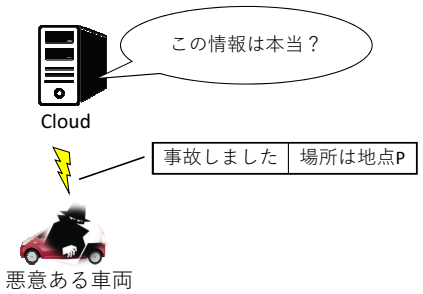


図 2　本研究の対象となる問題

2.　クラウドへのデータ送信に関する各種分析

2.1　脅威・要件・対処例の分析

車両がクラウドへの送信するデータに対し，**表 1** で脅威，要件，対処例の調査結果を示す．送信データに対する盗聴，改ざんとは，車両がクラウドに送信するデータを不正に取得し，その内容を変更することである．この二つに求められる要件は，データの秘匿性と完全性である．対処例として，秘密鍵を使ったデータの暗号化や ID 情報を公開鍵とした ID ベース暗号 [7] などがある．次に，クラウドに偽装情報を発信する車両のなりすまし行為を考える．表 1 で示した車両なり代わりとは，車両 ID などを偽り，自車両を他車両と偽る行為である．自分を他車両と偽ることで，不正にサービスを受けたり，その車両を使いクラウドに対し踏み台攻撃ができる．しかし，これは車両に適応する公開鍵基盤手法 (PKI)[6] により対策可能である．

本研究が対象としているのは，なりすまし行為の中でも，自車両が行うデータ偽装行為である．自車両が行うデータ偽装行為とは，他車両になり代わる行為ではなく，自身の位置情報や車両状態を改ざんすることで，クラウドに対し不正データを送信することである．この行為を防ぐために求められる要件は，車両ノードそのものの信頼性ではなく，送信データの信頼性である．

2.2　ノード信頼性とデータ信頼性

表 1 でのなりすましにおける要件，ノード信頼性とデータ信頼性について，詳しく述べる．ノード信頼性とは，車両そのものを信頼し，別車両になり代われないことを保証しものである．前節で述べたように，対策例として車両に適応する PKI がある．**図 1** で示すような仕組みによって，クラウドは電子証明書を確認することで，発信者情報を確認することができる．しかし，本研究で扱う問題は**図 2** のような，車両が自身の情報を改ざんし，クラウドに対し不正データを送信したときである．送信データに対し偽装行為が行われているかどうかは，データの暗号化や PKI では解決できない問題であり，そもそもこれらが対処している問題と，本研究で解決しようとしている問題とは別物である．車両データの偽装行為において，データの信頼性を保証するという要件を考慮し，本研究でその対処例を提案する．

3.　提案手法

3.1　概要

車両が V2X 通信を行うことで，クラウドに自身の位置情報を送信する際に，位置情報以外の情報も送信する．本研究では，車両がクラウドと V2C 通信する際に経由される基地局の情報と，V2V 通信によって得られる周辺の車両情報を利用し，不正データの検出を行う．ここでは提案手法の動作概要を分かりやすくするため，基地局情報の利用と，周辺車両情報の利用を別々に説明する．

3.2　前提条件

(1) 全ての車両とクラウドは事前の信頼関係によって安全な通信路が確保されている
(2) 車両とクラウドは事前に相互に認証されている
(3) クラウドと基地局の信頼関係は構築されている

3.3　提案手法における用語の定義

- Vehicle ID

車両が車車間通信 (V2V 通信) を行う際に利用する，車両固有の公開 ID を指す．

- V2C Vehicle ID

車両がクラウドとの通信 (V2C 通信) に利用する，車両固有の問い合わせ用の ID である．他者に公開しない秘密 ID であり，V2CVehicleID と VehicleID は一意に関連している．

- Via BS(Base Station) ID

提案手法における基地局情報であり，車両とクラウドが通信する際に中継される基地局の，基地局固有の ID を指す．この ID は双方向ワンタイム ID 方式を採用し，ID 自体に

生存時間を設ける．

- PV(Peripheral Vehicle) ID

提案手法における周辺車両情報であり，車両が V2V 通信によって他車両から受け取った VehicleID を指す．

3.4 V2C 通信における基地局情報の利用

車両は V2C 通信で自身の位置情報を送信する際，その位置情報に対し V2CVehicleID を添付し，クラウドに送信を行う．V2C 通信の際に中継される基地局は，車両から送られてきた位置情報に，ViaBSID をカプセル化しヘッダ付与する．クラウドには，すべての車両の V2CVehicleID が事前に登録保存されており，どの車両からの問い合わせであるかが V2CVehicleID を確認することでわかる．さらに，基地局エリアカバー範囲である通信可能範囲と，ViaBSID もクラウドに登録されている．

図 3 は V2C 通信における基地局情報の利用例を示している．車両は各々 V2CVehicleID を所有しており，基地局も各々 ViaBSID を所有している．ここでは簡単のため，2 台の車両の V2CVehicleID を V2C_A，V2C_B とし，それぞれ基地局固有の ViaBSID を BS1，BS2 としている．車両が V2C 通信に行った際，基地局を中継してクラウドが得られる情報は，V2CVehicleID，車両の位置情報 (Position)，ViaBSID となる．

図 4 は自車両情報なりすまし行為の一例を，提案手法で対策したものである．V2C 通信における基地局情報を利用することで，別基地局内への位置情報偽装を防ぐことが可能である．

3.5 V2V 通信による周辺車両情報の利用

車両は自身の周辺に存在している車両と V2V 通信を行い，VehicleID を交換する．車両は車車間通信可能範囲内を走行している車両を周辺車両とし，周辺車両から受け取った VehicleID を PVID として扱う．提案手法の V2V

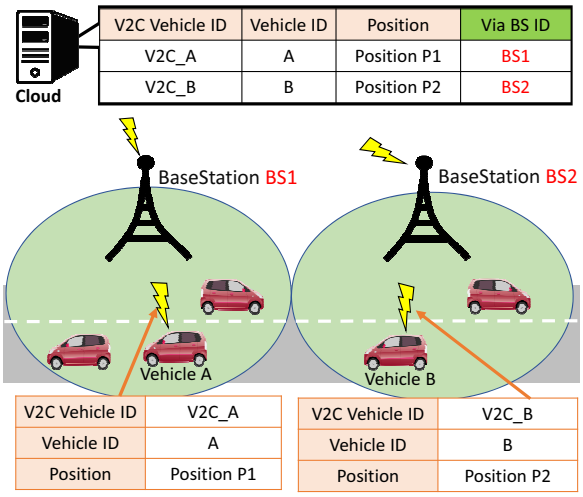


図 3 V2C 通信における基地局情報の利用例

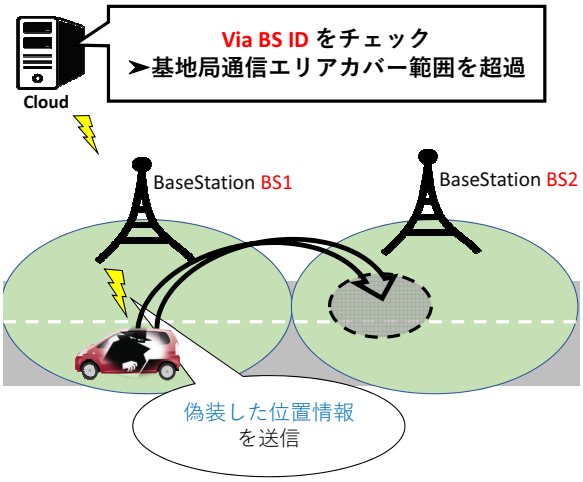


図 4 提案手法における基地局情報利用の利点

通信では，VehicleID の情報のみをやり取りする．

車両が自身の位置情報をクラウドに送信する際，V2CVehicleID と自身の VehicleID，V2V 通信により取得した PVID を添付する．V2CVehicleID と VehicleID は一意に関連しており，PVID により，互いの車両が車車間通信可能範囲内にいるという保証が得られる．**図 5** は V2V 通信による周辺車両情報の利用例を示している．車車間通信可能範囲内を走行している相手車両と通信を行い，VehicleA は VehicleC，D の VehicleID を取得する．取得した VehicleID は PVID として扱い，VehicleA は周辺車両 VehicleC，D と互いの位置情報を保証し合う．

図 6 は自車両情報なりすまし行為の一例を，提案手法で対策したものである．悪意ある車両が，同基地局内における位置情報偽装を行ったと考える．クラウドは車両から位置情報と共に送られてきた周辺車両情報（PVID）を確認し，送信車両の位置情報と周辺車両情報に該当する車両の位置情報を比較する．この際，比較した位置情報が車車間通信可能範囲内を超えていた場合，受信した位置情報は偽

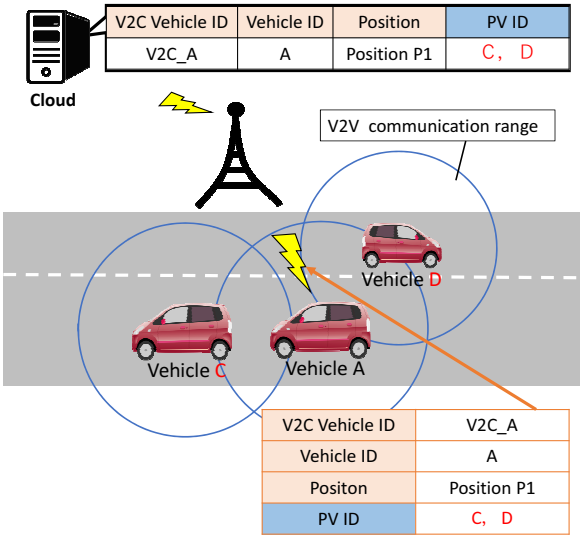


図 5 V2V 通信による周辺車両情報の利用例

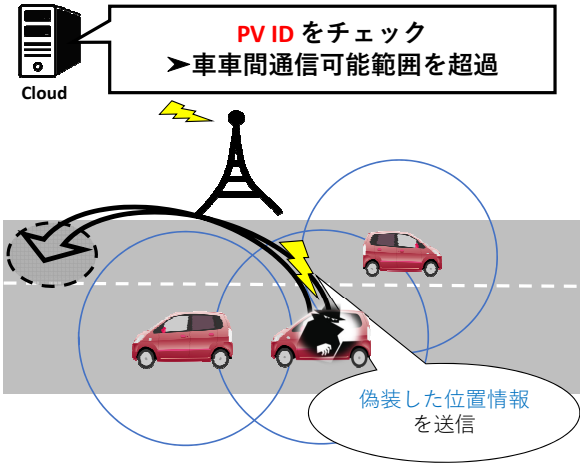
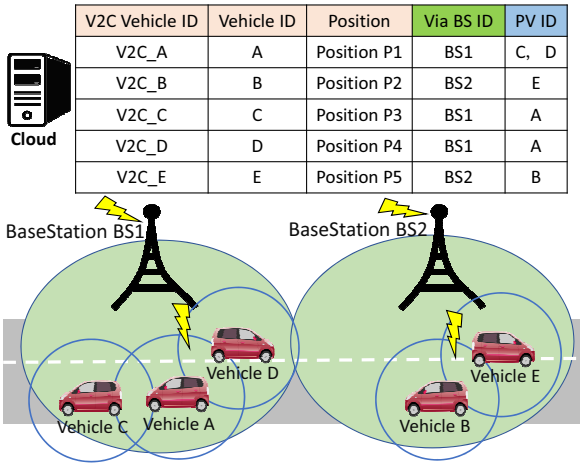


図 6　V2V 通信による周辺車両情報の利用の利点



V2C Vehicle ID	Vehicle ID	Position	Via BS ID	PV ID
V2C_A	A	Position P1	BS1	C, D
V2C_B	B	Position P2	BS2	E
V2C_C	C	Position P3	BS1	A
V2C_D	D	Position P4	BS1	A
V2C_E	E	Position P5	BS2	B

図 7　V2X 通信を利用した提案手法の利用例

装されていることが分かり，超えていない場合は受信した位置情報を信用する．V2V 通信を利用し，周辺車両情報を取得することで，車両は周辺車両と位置情報を相互監視し，不正データの検出を行う．

3.6　V2X 通信を利用した不正データの検出方法

図 7 で示すように，提案手法では前述の二つを組み合わる．クラウドが受信するデータは，送信車両の位置情報や車両 ID だけでなく，V2X 通信によって相互監視された周辺車両情報や基地局情報が付属する．そのため，このデータに対し，図 8 の操作を加えることで不正データの検出が行える．

図 8 の第一段階として，V2CVehicleID を利用し，クラウドが受信したデータが車両から送信されたものであることを検証する．第二に，送信車両の位置情報と ViaBSID を比較し，経由基地局のエリアカバー範囲内に存在しているかを確認する．送信車両の位置情報が，経由基地局のエリアカバー範囲を超えている場合，整合性がとれていないものとし，その位置情報を不正データと認定する．これにより，別基地局内からの偽装行為を対策可能としている．第三，第四段階では，PVID を利用し，送信車両の周辺を走行している車両情報を基に，不正データの検出を行う．第三段階における不整合とは，自身の周辺に存在していない車両を周辺車両とした場合である．V2V 通信によって周辺車両とは互いの VehicleID を交換しているため，自身の周辺車両を偽装することはできない．規定回数に到達しなかったデータ，あるいは周辺車両の位置情報と整合性がとれなかったデータを第四段階で不正データとして認定している．V2V 通信可能範囲を超えての位置偽装に対処することができ，規定回数を設けることでデータをより信用度の高いものにすることができる．第二，第三，第四段階において，条件を満たさなかったデータは，例外なく不正認定とし，そのデータを信用しない．

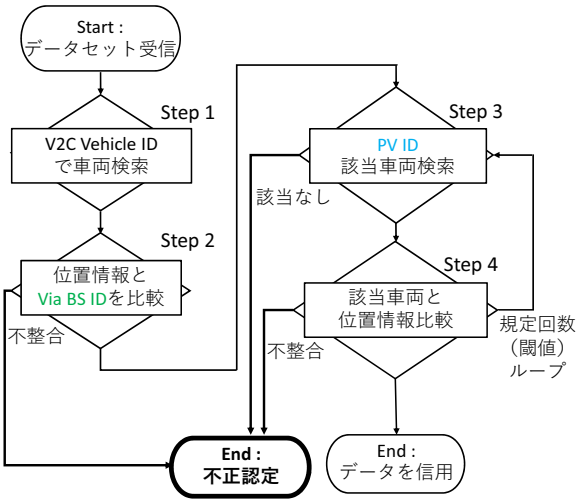


図 8　車両送信データに対する不正データ検出手順

4.　評価・考察

4.1　シミュレータ

本論文では，提案手法の性能評価にシミュレータとして Scenargie[8] を用いた．Scenargie は Space-Time Engineering（STE）社が開発したネットワークシミュレータである．様々な拡張モジュールと組み合わせることで，LTE や車車間通信，マルチエージェントシミュレーションなど多様なモデルを構築することができる．また，近年の通信システムや評価シナリオが複雑になってきていることから，シナリオ作成の作業を大幅に低減する工夫がなされている．その例として，GUI によるシナリオ作成や地図データと通信システムのグラフィカルな情報表示，電波伝播解析機能などが挙げられる．

4.2　評価モデル

評価環境としては，1 平方キロメートル四方のマンハッタンモデルを使用し，表 2 で示したシミュレーションパラメータを用いる．車両台数を 158[台]，範囲を 1[km^2] と

表 2　シミュレーションパラメータ

シミュレータ	Scenargie2.0	
車両台数	158[台](内 5[台] は偽装位置情報を送信)	
範囲	1000[m] × 1000[m]	
通信方式	ARIB STD T109	LTE
使用周波数帯	700[Mhz]	2.5[GHz]
通信インターバル	100[ms]	1.0[s]
電波伝播モデル	ITU-R P.1411	LTE-Macro
基地局地上高	1.5[m]	

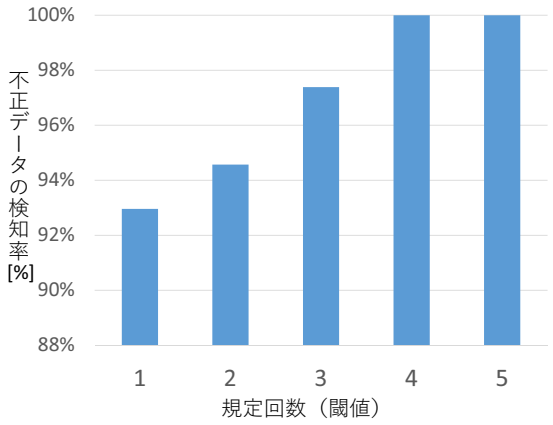


図 9　クラウド集約データにおける不正データの検知率

したのは，日本全土における平均車密度が 158[台/km^2] であることを考慮したためである．ITU-R P.1411 モデルは，道路マップ情報を考慮した電波伝播モデルであり，道路の形状に応じて電波が減衰するので，直接波と地面からの反射波を考慮した Two-Ray モデルと比べると現実に近いモデルとなっている．

4.3　不正データ検知率の評価

図 9 はクラウドに集約されるデータから，偽装されたデータの閾値別検知率を示している．悪意ある車両がクラウドに送信する不正データを，提案手法の閾値を増加させることで 100% 検知することが可能となった．しかし閾値が低い場合において，不正データを完全検知できなかった．その理由を，**図 10**，**図 11** に示す．

図 10 は，周辺車両と車車間通信可能範囲内であれば，その可能範囲において位置情報の偽装が可能となってしまう例を示している．この場合，周辺車両が悪意ある車両の位置偽装情報を保証してしまうため，位置情報の偽装行為が可能となってしまう．図 11 は悪意ある車両どうしの結託である．悪意のある車両が互いの位置偽装情報を保証し合うことで，クラウドに対し悪意のあるデータを信用させようとする行為である．これらの問題は，図 8 で示した規定回数（閾値）を増加させることで，対策できる．閾値を増加させることで，**図 12** のような状況を作ることができ，悪意ある車両の偽装行為を制限することができる．

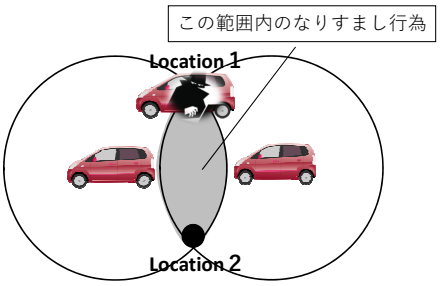


図 10　周辺車両との車車間通信可能範囲におけるなりすまし行為

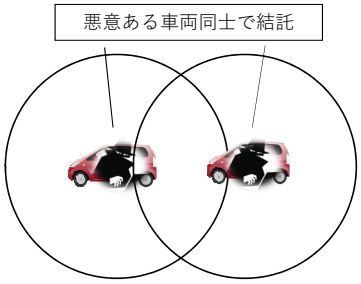


図 11　なりすまし車両同士の結託

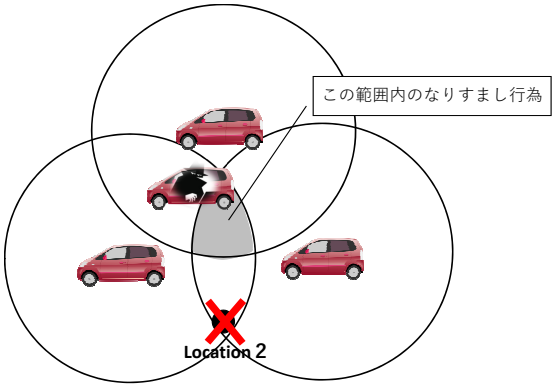


図 12　周辺車両情報の増加による，なりすまし行為の制限

4.4　誤検知率の評価

図 13 は，日本の平均車密度を考慮した場合におきる，提案手法の誤検知率（フォールスポジティブ）を表している．提案手法における閾値とは，クラウドが情報を信用するために必要な周辺車両情報のデータ数である．前節で，閾値の増加が，不正データの検知率向上に繋がることが分かった．ここでは，不正行為を行っていない車両の情報をクラウドは信用しているのかという，誤検知率，すなわちフォールスポジティブを考察する．表 2 で示したシミュレーション環境において，車両 158[台] 全てが不正行為を行っていないとし，フォールスポジティブを測定した結果が図 13 である．閾値を増加させることで，誤検知率が上昇していることがわかる．日本の平均車密度において，閾値を上げることは正常な通信を誤って異常と検知してしまう．

そこで，日本の平均車密度より高い，大阪での平均車密度環境下におけるフォールスポジティブを**図 14** で示す．車密度の高い地帯では，V2V 通信によって取得できる周

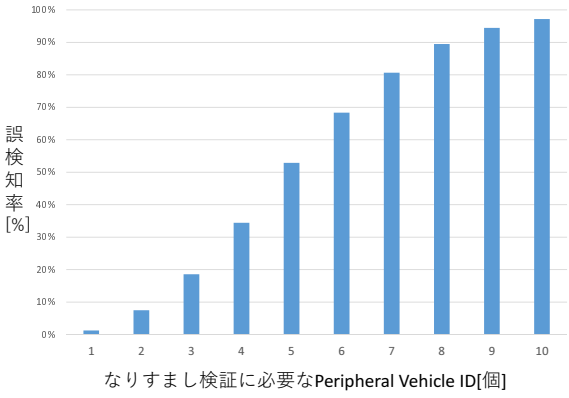


図 13 日本平均車密度（158[cars/km^2]）環境下における PeripheralVehicleID 別フォールスポジティブ

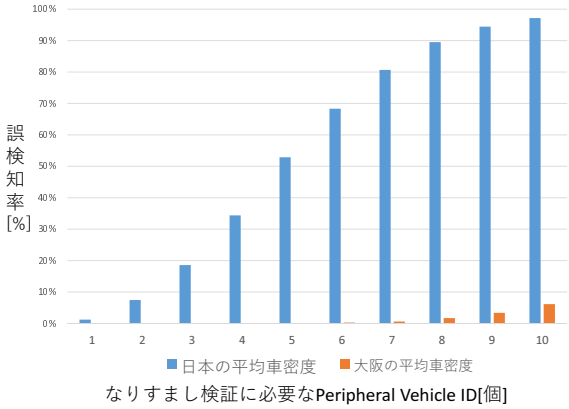


図 14 大阪平均車密度（1128[cars/km^2]）環境下とのフォールスポジティブ比較

辺車両情報が多数存在しているため，閾値を増加させても誤検知率の上昇を抑えることができる．従って，提案手法は車密度の高い地域でより効果を発揮することが分かった．実際，車密度の高い地域において，車両情報の偽装行為が与える影響は大きい．提案手法では，周辺車両が少なくなってしまう地帯よりも，周辺車両が多く存在する地帯の方が，車両がクラウドに送信する情報をより保証することができ，自車両なりすまし行為が甚大な影響を与える交通過密地帯において，提案手法は有用であると言える．

4.5 処理時間の計測

表 3 で示す評価環境において，不正データの検出に所要する処理時間を**表 4** で評価している．この評価は，図 8 の不正データの検知手法に基づき評価したものであり，1 車両における処理時間を示している．BSID を使用することで，提案手法では不正データを処理の序盤で検知することができ，処理時間は比較的早くなる．PVID を用いた検知手法では，閾値別に処理時間が異なる．閾値を増加させることで，PVID による不正データの検知手順が繰り返される．その繰り返し中でも，比較的序盤に不正データが発見できるか，終盤で発見できるかによって処理時間が変わるため，Step4 までの処理時間には範囲を設けた．不正データが検出されなかった場合を通常終了とし，その閾値における上限の処理時間を示している．提案手法閾値の増加に伴い，通常終了するためにかかる処理時間は増加する．V2C 通信の遅延や，安全運転支援システムの遅延時間の許容範囲を考慮した閾値の決定が重要となる [9]．

表 3 処理時間測定における環境

OS	macOS Sierra
プロセッサ	1.6GHz IntelCorei5
メモリ	8GB 1600MHzDDR3
言語	Python
データベース	MySQL

表 4 1 車両の送信データに対する不正検知の処理時間 [ms]

閾値	図 8 の Step2 で検出	Step4 で検出	通常終了
1	0.1	0.31	0.31
2	0.1	[0.31,0.53]	0.53
3	0.1	[0.31,0.76]	0.76
4	0.1	[0.31,0.96]	0.96
5	0.1	[0.31,1.2]	1.2
6	0.1	[0.31,1.4]	1.4
7	0.1	[0.31,1.6]	1.6
8	0.1	[0.31,1.8]	1.8
9	0.1	[0.31,2.0]	2.0
10	0.1	[0.31,2.2]	2.2

5. おわりに

ITS（Intelligent Transport Systems）の分野において，クラウドの利用は必至である．クラウドを利用した安全運転支援サービスを提供する上で，車両情報を偽装する行為や，車両のなりすまし行為は脅威となる．本研究では，車両が V2X 通信を行い，様々な対象から情報を得れることを利用し，車両なりすまし行為を対策し，車両がクラウドに送信する情報から不正データを検出する手法を提案した．V2C 通信における中継基地局の情報と，V2V 通信を利用した周辺車両情報を利用することで，車両情報の偽装行為を対策し，提案手法の閾値を増加させることで，不正データの検知率を向上させることができ，車両情報をより信頼度の高いものにすることができる．検知率の向上に伴い必要となる周辺車両情報のデータ数は，車密度を考慮し変化させることで，過疎地帯にも提案手法を適応させることは可能であり，車両過密地帯において，提案手法は最も効果を発揮することが考察より確認できた．

謝辞

本研究の一部は JSPS 科研費 (JP16H02814) および文部科学省私立大学戦略的研究基盤形成支援事業の助成を受けたものである．

参考文献

[1] 渡辺 陽介，高木建太朗，手嶋 茂晴，二宮 芳樹，佐藤 健哉，“協調型運転支援のための交通社会ダイナミックマップの提案”，DEIM，Forum，F6-6，(2015)．

[2] 押田大介，竹森敬祐，川端秀明，磯原隆将，山梨晃，塩田茂雅，横田雅勝，“繋がる車のセキュリティ”，コンピュータセキュリティシンポジウム 2014 論文集，No.2，pp.651-658，(2014)．

[3] 総務省，“サイバー攻撃（サイバーテロ）の統計情報”，http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h25/html/nc132110.html，(2017-1)．

[4] Daniel P. Shepard，“Evaluation of the vulnerability of phasor measurement units to GPS spoofing attacks”，Vol.5，No.3-4，pp.146-153，(2012)．

[5] Shihao Yan1，Robert Malaney1，Ido Nevat2，Gareth W. Peters3，“Location Spoofing Detection for VANETs by a Single Base Station in Rician Fading Channels”，Vehicular Technology Conference(VTC Spring)，IEEE 81st，(2015)．

[6] 小谷誠剛，“OKI の新しい活躍の場=繋がる車．そこで生まれる恩恵と脅威，それらへの方策”，電子署名 WG 主催セミナー資料，第 3 部，(2015)．

[7] レスアンヒウ，井手口哲夫，奥田隆史，田学軍，“高速道路における車々間通信システムへの ID ベース暗号の適用とその評価”，DICOMO2013，pp.404-409，(2013)

[8] SPACE-TIME Engineering，Scenargie；http://www.spacetime-eng.com/jp/index.html，(2016-4)．

[9] 総務省，“700MHz 帯安全運転支援システムについて”，http://www.soumu.go.jp/main_content/000281445.pdf，(2016-7)．