「マルチメディア，分散，協調とモバイル
(DICOMO2021) シンポジウム」 令和3年6月-7月

協調型ITSの仮名ID使用環境下における認知情報共有を用いた不正行為検出

有井 慎平[1]　塚田 学[1]　落合 秀也[1]　江崎 浩[1]

概要：協調型 ITS において、周囲車両に自車の状態を伝えるために Cooperative Awarness Message (CAM) という V2V メッセージ規格が標準化されている．また周辺環境に対する認知力の向上を目的として, 自車の状態だけでなく, 自車に搭載したセンサで知覚した情報を伝えるためのメッセージ規格として Collective Perception Message (CPM) が提案されており, 標準化に向けて分析が行われている．協調型 ITS ではセキュリティが重要であり、Public Key Infrastructure (PKI) のような予防的な手法に加え、不正行為検出 (Misbehavior Detection) に関する研究が盛んになってきている．一方で, モビリティデータを扱うという性質から, プライバシー保護のため通信において, 長期的な識別子を用いるのではなく, 仮名 ID（Pseudonym）と呼ばれる短期的な識別子を使用する仕組みが考案されており, 同一識別子によるデータの一貫性検証などが困難となる等, 不正行為検出手法にも対応が求められる．本論文では CAM および CPM の両方のデータを扱った不正行為検出手法を提案する．シミュレーションによる評価では CAM のみを扱う手法と比較し, CAM 内の位置情報改ざんに対して, 真陽率 (不正なメッセージを不正であると検出する確率) の水準を保ったまま、偽陽率 (不正でないメッセージを不正であると検出する確率) を改善した．

1. 序論

近年の自動運転技術の発展に伴い, 自動運転車の導入が進められている．米国の Society of Automotive Engineers (SAE) では, 自動運転のレベルが 6 段階で定義されており [1], 日本では公益財団法人の自動車技術会 (JSAE) がこの定義の日本語参考訳を公開したり [2], 国土交通省が SAE の定義を基に自動運転のレベル分けを発表している [3]．日本国内では, 2020 年 4 月に改正道路交通法, 改正道路運送車両法が施行され, 条件付自動運転を指すレベル 3 の走行が可能となった．

さらに高度なレベルの自動運転を実現するためには, 現在の自動運転において主となっている Stand-Alone な制御では周囲環境の認識力の観点から限界があるため, 欧州や米国, 日本を中心として Cooperative Intelligent Transport Systems (CITS) の研究が進められている．欧州の European Telecommunications Standards Institute (ETSI) や International Organization for Standardization (ISO) では, Vehicular Ad Hoc Network (VANET) と呼ばれる車車間で形成される動的ネットワークや, 路肩に設置された路側機, 周囲の歩行者と通信を行う Vehicle to Everything (V2X) を通して, モビリティデータを共有するシステムの技術標準化が行われており, なかでも ETSI と ISO が協力して策定した ITS 基盤標準 [4] が多くの研究の基盤となり機能している．

欧州における多くの CITS アプリケーションやセキュリティの研究では, 車車間で自車の状態を交換するためのメッセージ規格である Cooperative Awarness Message (CAM)[5] に含まれるモビリティデータを基に進められている．CAM は, 位置や速度などの情報を周囲車両と共有することで, 従来の Stand-Alone の自動運転車両におけるセンサの視覚範囲の限界を超えた周囲環境の認知を可能とする．

ETSI では CAM の他に, 各車両に搭載されているセンサで検知した物体の情報を含むメッセージ規格である Collective Perception Message (CPM)[6] を導入することが検討されている [7]．CAM は自車の状態のみを通信するため, 通信が障害物で一時的に遮断されている場合など, 発信元との通信が確保できない場合には, 周囲車両を認知することができない．CPM では, このような通信的な死角を周囲の車両に搭載されているセンサを使って補うことで周囲環境の認知力を高める．

さらに, CITS の安全性においてセキュリティが不可欠であることから, 従来のネットワークでも用いられている公開鍵暗号方式を利用した Public Key Infrastructure (PKI)

[1] 東京大学

に加え, PKI において認証された内側ノードからの攻撃を検知して攻撃による被害を抑えるために, V2X 通信における不正行為検出 (Misbehavior Detection) 手法の開発が活発に行われている [8].

また, CAM や CPM ではモビリティデータを扱うため, トラッキングによりユーザのプライバシーが侵害される可能性がある. ユーザのプライバシー保護の観点から, 発信元の識別子として従来のネットワークのような長期的な識別子ではなく, Pseudonym という短期的な識別子を使う仕組みを用いることで, CITS 参加者の匿名性を確保する研究が行われており, ETSI においても標準化が進められている [9][10].

現在までに研究が行われている不正行為検出手法は Pseudonym を前提としていない場合が多く, 長期的な識別子を利用してデータの一貫性を検証する手法も少なくない. また, CPM に関する分析, 研究が行われ標準化が進められている中, 不正行為検出手法に関する研究では CAM のみ, または 位置情報や速度のみといった研究者独自のメッセージを扱うことが多い. 本研究では, Pseudonym を考慮した環境下で, CAM と CPM を送受信する車両における不正行為検出手法を提案し, シミュレーションにより CAM 内の位置情報改ざんに対する評価を行なった.

以下, 本論文の構成は第 2 章, 第 3 章で VANET に対する脅威, 関連研究を紹介し, 第 4 章で提案手法の説明を行なう. 第 5 章で提案手法を評価するために構築したシミュレーションモデルを紹介している. 第 6 章でシミュレーション結果をもとに評価を行なっており, 最後に第 7 章で結論を述べている.

2. VANET に対する脅威

VANET では, 数多くの脅威が存在しており [11][12][13], 効率性の低下だけではなく, これらの脅威は安全性にも影響を与える. そのような脅威には偽の実体を作る Sybil 攻撃や, 送信メッセージの一部を改ざんする攻撃などがある. 存在しないはずの実体が出現することにより, 道路交通の効率性が損なわれたりするだけでなく, 衝突回避のために急ブレーキや進路変更といった動作が誘導され利用者の生死に関わるケースも考えられる. Sybil 攻撃に対するセキュリティ手法として, 無線機器が送受信を同時に行うことができないという仮定に基づいた Radio resource testing や, システムへの参加に認証を要件とする Registration, メッセージ内に含まれる位置情報について検証を行う Position verification がある [14]. VANET では, 複数チャネルの利用や認証された機器が盗まれたりする可能性があるため, メッセージ内の位置情報が正しく実際の環境を反映しているかを確かめることは, Sybil 攻撃を防ぐ有効な手段となり, 位置情報を対象とした不正行為検出が数多く研究されている.

位置情報や速度のような基本的なモビリティ情報は, CITS において根幹となる重要な情報であり, 攻撃者がこれらの情報を改ざんすることで実際の環境を反映しない情報を発信し, 周囲車両がその情報に従い動作すると, CITS 利用者の生死に関わるケースも発生し得る. そこで, 本研究では, 攻撃者が CITS メッセージである CAM の位置情報を改ざんすることを想定し, 位置情報改ざんに対する不正行為検出を扱う.

3. 関連研究

Xiao らの研究 [15] では, 無線信号の分布を分析し, メッセージ内の位置情報が正しいかを検証することで Sybil 攻撃を検出している. この研究では道路の路肩に設置された路側機や Sybil ノードがもつ無線信号分布の静的な分析, VANET の特性であるモビリティの高さや, 交通パターンを利用することで, 無線信号の強さだけで行う位置測定の不正確さや脆弱性を克服できるように試みている.

Golle らの研究 [14] では, 無線信号の強さに加え, hyperbolic position bounding (HPB) と呼ばれるアルゴリズムを用いて, effective isotropic radiated power (EIRP) の情報を持つかに依存せず, 確率的に発信元の位置を推定する方法により, メッセージ内の位置情報が正しいかを検証している.

上記の 2 つの研究はいずれも, 無線信号の強さを元に発信元の位置推定を行う手法を扱っており, ノード識別子への依存がなく Pseudonym を導入しても適応できると考えられる. しかし, 信号の伝達モデルや, Received Signal Strength Indicator (RSSI) に起因する精度の不正確さが伴う.

Sun らの研究 [16] では, カルマンフィルタの一般化である拡張カルマンフィルタの入力に, 受信信号の到来角とドップラー速度の測定値を組み合わせて使用することで, メッセージ送信者の位置を推定している. この推定値とメッセージ内に含まれる位置情報を比較し, 推定誤差から不正行為を検証する. カルマンフィルタは誤差を含む測定値から動的なシステムの状態を推定するための逐次フィルタの一種であり, カーナビゲーションシステムなどで利用されている. 不正行為検出の研究では, メッセージ発信元の位置や速度の推定に用いられることがある. この研究では, Pseudonym は考慮されておらず, 比較的単純な高速道路シナリオにおいてのみ評価が行われている.

Biβmeyer らの研究 [17] ではベイズフィルタの一種であり, センサ測定値から動的システムの状態を推定するために使用されるパーティクルフィルタを用いてメッセージ送信者の状態を推定している. この研究ではローカルでのメッセージ処理だけでなく, 中央機関への不正行為レポートおよび Pseudonym のように短期的に変化する識別子への対応を考慮している.

Jaeger らの研究 [18] では, カルマンフィルタの入力として加速度を採用し, メッセージ送信者の位置と速度を推定し, メッセージ内の位置と速度の情報との偏差が許容されるかによって不正行為検出を行なっている. またこの研究では, Psuedonym を考慮しており, 不正行為検出を行う車両がもつ複数のカルマンフィルタの状態から尤もらしいカルマンフィルタの状態が存在するか, またそのカルマンフィルタの状態で計算される偏差が許容範囲であるかを判断することで, 短期的に送信者の識別子が変化しても対応できるようにしている. ただし, 評価は実機を用いた実験によるもので, 多くの車両が存在する都市交通のようなシナリオについては評価していない.

Azuma らの研究 [19], [20] では, 車両がクラウドに自車両データをアップロードする際に, 車両位置を相互に監視することにより、不正を検知する仕組みを提案した.

上記のいずれの研究も CAM のみ, もしくは位置情報や速度のみを扱う独自メッセージを用いて評価を行なっている. 本研究では, システム内で CAM に加え CPM を導入し, CPM 内の情報を活用しながら Pseudonym を考慮した環境下で動作する不正行為検出手法を提案し, 都市交通シナリオにおけるシミュレーション評価を行った.

4. 提案手法

4.1 要件

本研究では, 次の 3 つを満たす不正行為検出手法を構築する.

- Pseudonym に対応可能
- CPM についても考慮されている
- CAM のみを用いる場合よりも真陽率の水準を保ったまま偽陽率を改善できる

Pseudonym に対応可能というのは, 変化しない車両 ID を基に行う一貫性検証や, ノードの信頼性検証ではなく, 車両 ID が変化することを前提に構築された不正行為検出手法であることを意味している. Pseunonym の目的から, 個々のノードがグローバルに Pseudonynm を解決する事で, ある車両を特定することはできないが, ローカルで Pseudonym を解決する, または Pseudonym 自体に影響されない不正行為検出手法が必要である.

CPM についても考慮されているとは, CAM の不正行為検出プロセスのように, CPM 内の送信元情報を検出プロセスに取り込むことができ, さらに CPM 内に含まれる知覚物体に関する情報を活用することができるということである.

真陽率の水準を保ったまま偽陽率を改善できるとは, CAM のみを用いる従来の手法における真陽率の水準を保ったまま, 真のメッセージを攻撃メッセージと誤検出する確率を下げることである. 偽陽率が高くすることで真陽率を上げることは可能であるが, 偽陽率が増加することで許容されるメッセージ数が減少し, 利用効率が下がると, CAM や CPM の情報は周囲環境を把握する主な要素として機能するため, 結果として CITS の安全性が低下する. そのため, 真陽率の水準を保ったまま偽陽率を下げることが重要である.

4.2 提案手法の概要

提案する不正行為検出手法は, 主に既知車両のカルマンフィルタによる検証, 未知車両に見える送信元からのカルマンフィルタによる検証, 未知車両に対する検証の 3 つのプロセスで構成される. カルマンフィルタの位置情報推定による不正行為検出プロセスを, 送信元の車両 ID に紐付けされたカルマンフィルタが存在する場合と, 存在しない場合に分けることで Pseudonym に対応することができる. Pseudonym の仕組みにより, 送信元の車両 ID が変化した場合には, 受信した車両から見ると未知車両に見える. しかし, 受信車両は変化する前の車両 ID に紐付けされているカルマンフィルタを保持しているので, 所持している複数のカルマンフィルタを検証していけば, この変更前の車両 ID に紐付けされたカルマンフィルタの出力が最も尤もらしい値になるはずであり, カルマンフィルタに対する車両 ID の紐付けを更新することで Pseudonym に対応できる.

未知車両に対する検出では, CAM のみを用いた手法でも, 近場の発信元に対して自車のセンサによる検証を行うことが可能である. また, CAM の情報のみを利用した Jaeger らの研究 [18] による不正行為検出手法と同様に, 最大通信範囲と一定のマージン距離で定義されるマージン範囲を設定することで, 通信範囲外から進入してきた未知車両を捉えることができる. しかしこの場合, マージン範囲と車両に搭載されたローカルセンサで認識可能な領域の間にある範囲について考慮されていない. そのため, この範囲で起動された車両のメッセージは, 真のメッセージであるか攻撃メッセージであるかに関わらず, 全て拒否されることになり, 結果として偽陽率が増加する.

そこで本研究では, CPM を用いて周囲車両がもつセンサ能力を活用し, この範囲で起動された未知車両に関する検証範囲を部分的に補填する手法を提案する. 提案手法では, カルマンフィルタの新規生成に用いる情報として, CAM に含まれる発信元の位置情報と速度の情報のみでなく, CPM に含まれる発信元がセンサで知覚した物体の位置情報と速度の情報を使う. そうすることで, 通信範囲内に存在する車両に搭載されているセンサにより考慮されていなかった範囲を部分的に補填することができる (図 1).

ただし, CPM の知覚物体の情報をカルマンフィルタ生成に用いるのは, CPM 内の発信元の位置情報および速度が信頼できる場合に限る. またセンサの知覚範囲の上限を設定し, CPM の知覚物体の位置と CPM の発信元の位置の距離がこの上限を超えていないかを検証するプロセスを

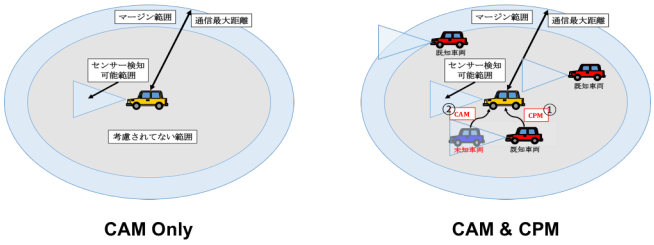

図 1 未知車両に対する検出範囲

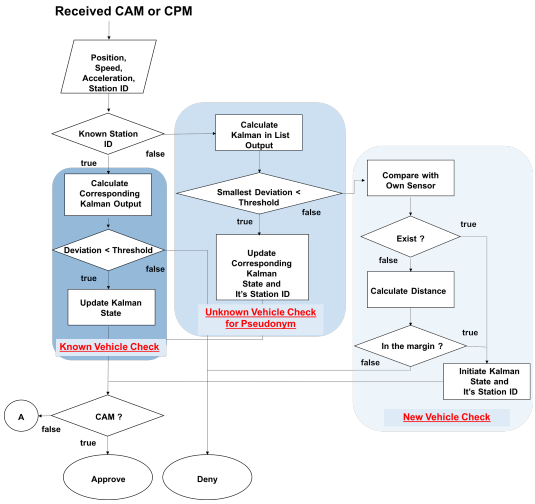

図 2 提案手法のフローチャート (発信元に関する位置情報と速度)

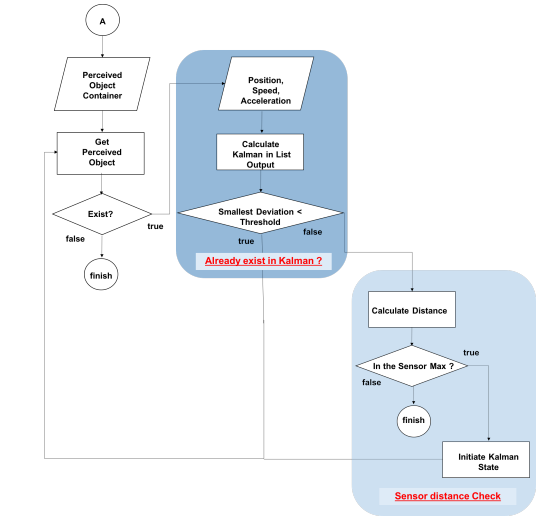

図 3 提案手法のフローチャート (CPM 内の知覚物体に関する位置情報と速度)

取り入れている. こうすることで, 攻撃者が CPM の知覚物体に関する位置情報を改ざんしようとしている場合でもその範囲を限定することができる.

図 2, 図 3 に提案手法のフローチャートを示す. 以下のセクションで, CAM と CPM の処理について順に述べる.

4.3 CAM の処理

受信したメッセージが CAM である場合は, CAM 内の ITS PDU header から識別子を, Basic Container と HF Container から位置情報と, 速度, 加速度の情報を取り出す. 取り出した識別子に対応するカルマンフィルタが存在する場合には, そのカルマンフィルタの入力として加速度を用いて検証を行う. カルマンフィルタの出力と, CAM から取り出した位置情報, 速度の差が許容できる範囲内であれば, CAM の受信を承認する.

取り出した識別子に対応するカルマンフィルタが存在しない場合には, 自身がもつカルマンフィルタを使って順に検証していく. 各カルマンフィルタの出力のうち, CAM から取り出した位置情報と速度との差が最も小さい場合を採用し, その値が許容範囲内であれば, 該当するカルマンフィルタの状態と識別子情報を更新し, CAM の受信を承認する. そうでない場合には, 自身の車両に搭載されたセンサで知覚している情報との比較, 設定したマージン範囲内にあるかの検証を行い, いずれかに該当する場合には CAM の受信を承認し, 新たなカルマンフィルターを生成する.

全てのプロセスにおいて, 検証に用いるカルマンフィルタは, メッセージの受信時刻とカルマンフィルタの最後の更新時刻の差に制限を設けることで, 精度の低下と識別子の誤った更新を防ぐ.

4.4 CPM の処理

受信したメッセージが CPM である場合, まず CPM 内の ITS PDU header から識別子を, Management Container と Station Data Container から発信元の位置情報と速度, 加速度の情報を取り出す. 取り出した情報を用いて CAM の場合と同様の検証を行う. ここで, CPM の発信元の情報が承認された場合, 次に発信元の車両が知覚した物体に関する情報の検証を行う.

CPM 内に含まれる Perceived Object の数が 0 でなければ, Perceived Object Container から知覚された物体に関する情報群を 1 つ取り出し, この情報群のから, 知覚物体の位置情報と速度, 加速度を取り出す. ただし, CPM において, 知覚物体に関する位置情報は発信元との距離で表され, 速度や加速度の情報についてもその大きさや方向は発信元が基準となるので, Management Container と Station Data Container から取り出した発信元の情報を用いて, 知覚物体の位置情報と, 速度や加速度の大きさや方向を CAM や CPM の Station Data Container で用いている座標に変換する.

知覚物体の位置情報, 速度, 加速度の基準を変換したら, 次に自身がもつカルマンフィルタを使って順に検証していく. このプロセスは CAM や CPM の発信元情報を検証する場合における, 発信元の識別子に対応するカルマンフィルタの状態を持たない場合と同じである. ただしこのプロ

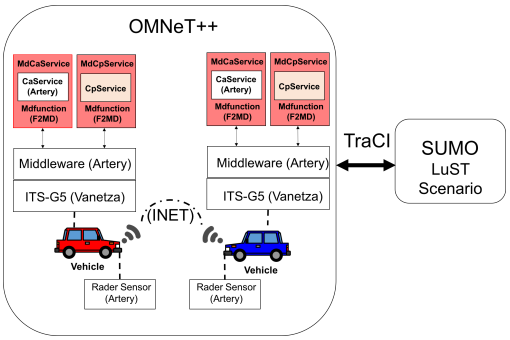

図 4 シミュレーションアーキテクチャ

表 1 シミュレーションパラメータ

Parameter	Configuration
Network Simulation Time	1000 sec
Traffic Simulation Time	1000 sec
Pseudonym Change Period	100 sec
Bitrate	6 Mbps
Tx Power	200 mW
Carrier Frequency	5.9 GHz
CAM DCC Profile	DP2
CAM Channel	CCH
CPM DCC Profile	DP3
CPM Channel	CCH

セスで該当する可能性があるカルマンフィルタが見つかっても, 知覚物体に関する情報は関節的な情報であり, 直接的に情報が伝えられる CAM や CPM の発信元に関する情報との時間的順序が乱れ, 適切にカルマンフィルタが更新されない可能性が高まるので更新は行わない. 検証している知覚物体の情報に対応するカルマンフィルタが存在しないと判断された場合には, 発信元と知覚物体との距離を検証する. 発信元と知覚物体との距離が設定されているセンサの最大知覚範囲内であれば, 該当する知覚物体の情報を用いてカルマンフィルターを新規生成する.

5. シミュレーション

5.1 システムモデル

図 4 にシミュレーションのアーキテクチャを示す.

本研究では都市交通シミュレータとして SUMO[21], ネットワークシミュレータとして Omnet++[22] を使用している. また実装に際して, 車両通信のためのフレームワークである Veins[23] および有線や無線, モバイル通信のためのフレームワークである INET[24], ITS のプロトコル実装をしている Vanetza[25] を統合した Omnet++ 上で動作する V2X 通信フレームワークの Artery[26], 不正行為検出メカニズムをシミュレーションするための様々な機能を提供する F^{2}MD [27] を使用しており, カルマンフィルターの実装は F^{2}MD で提供されているモジュールを用いている. さらに, 車両に搭載するセンサー機能に関しては Artery で提供されているモジュール [28] を使用している.

各車両ノードについて, Artery ですでに提供されている CaService モジュールのように, 文献 [6] の Annex D のフローに従い CpService モジュールを作成している. ただし, CpService について, セグメント化の機構は実装しておらず, Perceived Object Container に含まれる Object の数の最大値を 5 に設定している. また CaService および CpService での CAM や CPM の送受信時において不正検出メカニズムや攻撃の発生が行えるように F^{2}MD で提供されている機能を使いながら, それぞれ MdCaService および MdCpService に拡張している.

図 5 LuST Scenario (15000 m × 15000 m) (出典 [27])

5.2 シミュレーションパラメータと交通シナリオ

表 1 に主なシミュレーションパラメータを示す.

全ての車両ノードは, CAM および CPM の両方のメッセージを送受信できる機構を持ち, 搭載されるセンサは半径 80 m, 中心角がノードの直進方向を中心に 60° の扇形の視野をもつ前方 60° センサと半径 80 m の 360° センサを想定している.

交通シナリオについて, 本研究では都市交通環境におけるシミュレーションを行うために, F^{2}MD で提供されているルクセンブルクの現実的なモビリティパターンを反映した LuST Scenario (図 5) と, その縮小版である LuST Mini Scenario (図 6) を採用している. 各シナリオについて, 高密度シナリオと低密度シナリオの 2 パターンでシミュレーションを行なっており, シミュレーション時間内に出現する最大車両数は, LuST Scenario では, それぞれ 243 台, 117 台, LuST Mini Scenario では, 105 台, 23 台 である. LuST Scenario は高速道路の交通量が大きいのが特徴的な交通シナリオであり, LuST Mini Scenario は高速道路を含まない一般道路のみの交通シナリオである.

全てのシナリオにおいてデータの記録は 50 s 毎に行った.

5.3 攻撃者モデル

本研究では, CAM 内の Basic Container に含まれる位置情報である緯度・経度のデータが改ざんされることを

図 6 LuST Mini Scenario (2200 m × 2700 m) (出典 [27])

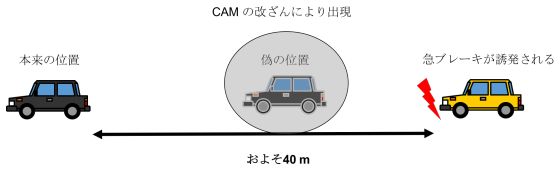

図 7 CAM の位置情報改ざんによる急ブレーキ誘発の例

想定している．攻撃者は, 送信する CAM の内 30 % の割合で Basic Container 内に挿入する緯度・経度の情報を, LuST Scenario では 0.00003° から 0.00050°, LuST Mini Scenario では 0.00003° から 0.00030° の値の範囲で本来の値にランダムに加算して送信する．LuST Mini Scenario の場合, 距離に換算するとおよそ 3 m から 40 m に相当する．一般的な車道の幅が 3.5 m であることから最低の偏差を 3 m 程度に設定している．また, 時速 60 km/h で走行する車の停止距離は約 37 m であり [29], 通常 60 km/h 程度で走行している車の車間距離は約 40 m 程度空いていると想定できる．この本来空いているはずの範囲に攻撃者が偽の位置情報を発信することで, 図 7 のように急ブレーキが誘発される可能性を想定して最大の偏差を 40 m 程度としている．LuST Scenario の場合には, 高速道路での交通量が他の道路の交通に比べ大きくなるため, 平均的な車間距離が大きくなると考えられる．したがって Lust Mini Scenario よりも変化させる緯度・経度の範囲を 0.00020° 大きくしている．またシミュレーションでは, SUMO でロードされる車両ノード全体の内 10 % の確率でノードが攻撃者になるように設定している．

カルマンフィルタは, 動的システムの変化における一貫性の検証には適しているが, 定量的なオフセットを検出することはできず, 他の手法を用いて不正検出を行う必要があるが, 本研究ではこのような定量的なオフセットを本来のデータに加算するような攻撃は想定していない．

表 2 LuST Scenario (高密度シナリオ) の真陽率と偽陽率

	Deny Attack [%]		Deny Genuine [%]	
	Average	Worst	Average	Best
CAM/Front	86.0	79.6	24.0	19.5
CAM/360 degree	85.8	80.9	22.8	18.6
CAM&CPM/Front	87.0	81.8	18.2	15.6
CAM&CPM/360 degree	88.3	82.8	16.1	12.9

表 3 LuST Scenario (低密度シナリオ) の真陽率と偽陽率

	Deny Attack [%]		Deny Genuine [%]	
	Average	Worst	Average	Best
CAM/Front	85.9	78.1	24.4	20.3
CAM/360 degree	84.8	76.7	23.1	19.1
CAM&CPM/Front	86.3	81.1	19.8	16.4
CAM&CPM/360 degree	86.6	79.5	18.8	15.0

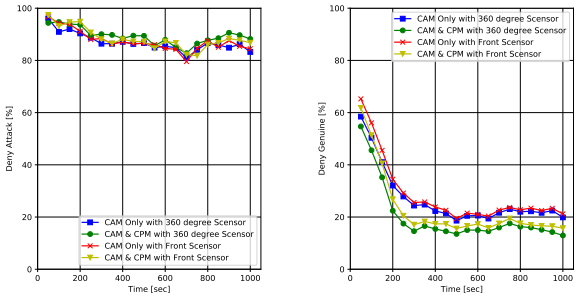

図 8 LuST Scenario (高密度シナリオ) の真陽率と偽陽率 (左:真陽率, 右:偽陽率)

6. 評価

6.1 LuST Scenario

6.1.1 真陽率と偽陽率

表 2, 表 3, 図 8, 図 9 に, 真陽率と偽陽率のシミュレーション結果を示す．表 2, 表 3 の平均はメッセージ数で重み付けした平均である．

図 8, 図 9 の偽陽率の結果から, 提案手法を用いる場合の方が, 前方 60° センサ, 360° センサ, いずれの場合においても偽陽率が低くなっていることがわかる．また, 真陽率について, 平均, 性能が最も悪くなる場合のいずれにおいても, CAM のみを用いる場合と提案手法の差は 3 % 以下と小さく, 提案手法を用いる場合の方がわずかに性能が良い．したがって, 高速道路の交通が特徴的な LuST Scenario において, 提案手法を用いることにより, 真陽率の水準を保ちながら偽陽率を改善できたと言える．

図 10 に未知車両検出における偽陽率の結果を示す．図 10 の結果から高密度シナリオ, 低密度シナリオのいずれのシナリオにおいても, 提案手法を用いることで偽陽率が改善されており, 未知車両検出における偽陽率の改善が検出手法全体における偽陽率の優位性に寄与していることがわかる．

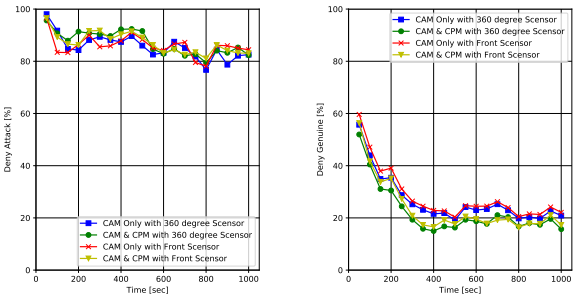

図 9 LuST Scenario (低密度シナリオ) の真陽率と偽陽率 (左:真陽率, 右:偽陽率)

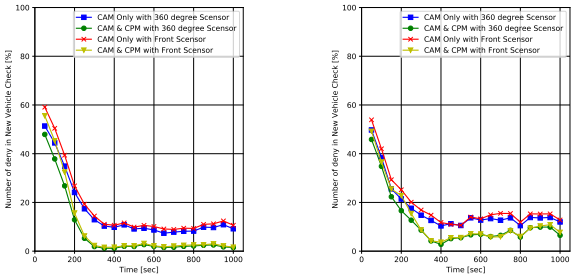

図 10 LuST Scenario の未知車両検出における偽陽率 (左:高密度, 右:低密度)

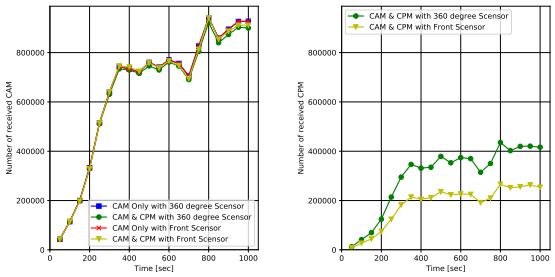

図 11 LuST Scenario (高密度シナリオ) の受信メッセージ数 (左:CAM, 右:CPM)

6.1.2 受信メッセージ数

図 11, 図 12 に, 受信メッセージ数のシミュレーション結果を示す.

CAM の受信メッセージ数は高密度シナリオ, 低密度シナリオのいずれにおいてもほとんど差がない. したがって, 偽陽率が小さい提案手法の方が承認されている真の CAM メッセージ数が多く, 利用効率が高いと言える. 一方, CPM の受信数について, 前方 60° センサと 360° センサの場合を比較すると, 高密度シナリオの方が低密度シナリオよりも差が大きく, 表 2, 表 3 より偽陽率の差も高密度シナリオの方がわずかに大きい. ただし, 提案手法において CPM が活用されるのはカルマンフィルターの新規生成においてのみなので, CPM の受信数が増加しても必ずしも偽陽率の活用に反映されるとは言えない.

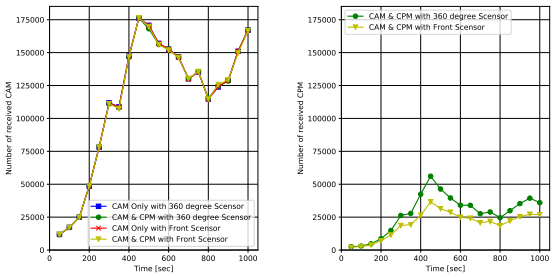

図 12 LuST Scenario (低密度シナリオ) の受信メッセージ数 (左:CAM, 右:CPM)

表 4 LuST Mini Scenario (高密度シナリオ) の真陽率と偽陽率

	Deny Attack [%]		Deny Genuine [%]	
	Average	Worst	Average	Best
CAM/Front	91.2	80.7	45.0	40.1
CAM/360 degree	91.1	83.2	43.6	38.6
CAM&CPM/Front	90.4	80.7	31.0	24.4
CAM&CPM/360 degree	89.9	84.3	29.6	23.0

表 5 LuST Mini Scenario (低密度シナリオ) の真陽率と偽陽率

	Deny Attack [%]		Deny Genuine [%]	
	Average	Worst	Average	Best
CAM/Front	88.2	70.3	43.0	25.0
CAM/360 degree	89.3	69.6	41.3	21.4
CAM&CPM/Front	86.3	71.2	40.2	22.9
CAM&CPM/360 degree	89.0	70.6	38.5	19.7

6.2 LuST Mini Scenario

6.2.1 真陽率と偽陽率

表 4, 表 5, 図 13, 図 14 に, 真陽率と偽陽率のシミュレーション結果を示す. 表 4, 表 5 の平均はメッセージ数で重み付けした平均である.

図 13, 図 14 の偽陽率の結果から, 高密度シナリオの場合には提案手法による偽陽率の改善効果が大きく, 低密度の場合にはわずかな改善に止まっていることがわかる. また, 真陽率について, 平均, 性能が最も悪くなる場合のいずれにおいても, CAM のみを用いる場合と提案手法の差は 1 % 以下と小さい. したがって, 高速道路の交通が特徴的な LuST Scenario において, 提案手法を用いることにより, 真陽率の水準を保ったまま偽陽率を改善でき, その効果は高密度シナリオでより大きくなると言える.

図 15 に未知車両検出における偽陽率の結果を示す. 図 15 の結果から高密度シナリオ, 低密度シナリオのいずれのシナリオにおいても, 提案手法を用いることで偽陽率が改善されており, 未知車両検出における偽陽率の改善が検出手法全体における偽陽率の優位性に寄与していることがわかる.

6.2.2 受信メッセージ数

図 16, 図 17 に, 受信メッセージ数のシミュレーション結果を示す.

CAM の受信メッセージ数は高密度シナリオ, 低密度シ

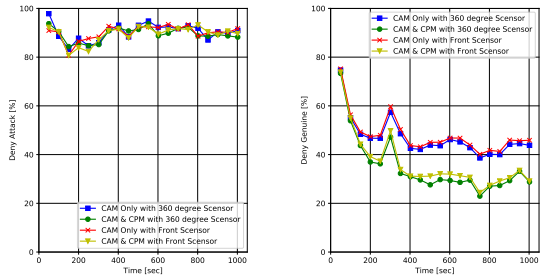

図 13 LuST Mini Scenario (高密度シナリオ) の真陽率と偽陽率 (左:真陽率, 右:偽陽率)

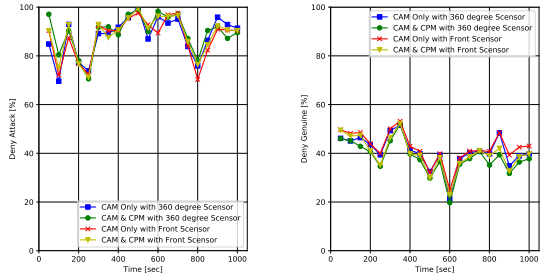

図 14 LuST Mini Scenario (低密度シナリオ) の真陽率と偽陽率 (左:真陽率, 右:偽陽率)

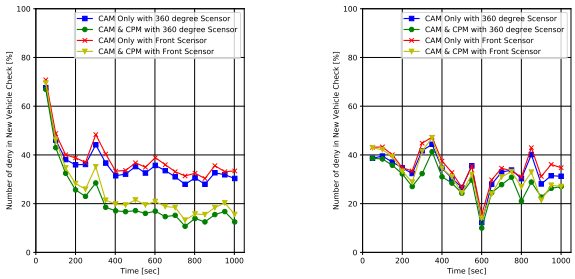

図 15 LuST Mini Scenario の未知車両検出における偽陽率 (左:高密度, 右:低密度)

ナリオのいずれにおいてもほとんど差がない. したがって, 偽陽率が小さい提案手法の方が承認されている真の CAM メッセージ数が多く, 利用効率が高いと言える. ただし, 低密度シナリオにおいては, CPM の受信数が CAM の受信数に比べてかなり少ない場合が多く, 提案手法による CPM の情報活用による偽陽率の改善効果は小さい.

7. 結論

本研究では, Pseudonym が利用され, CAM と CPM の両方が送受信される環境を想定し, CPM を通じて周囲車両のセンサ能力を活用することで, 攻撃メッセージを正しく検出する確率 (真陽率) を保ちながら, 真のメッセージを攻撃メッセージとして検出する確率 (偽陽率) を改善する不正行為検出手法を提案した.

評価を行うために, 都市交通シミュレータの SUMO と

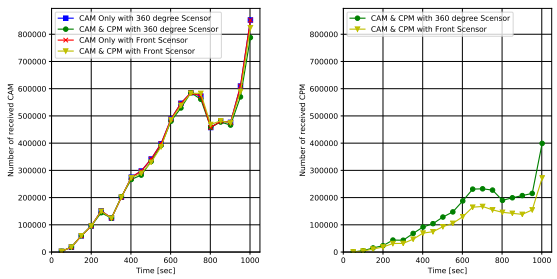

図 16 LuST Mini Scenario (高密度シナリオ) の受信メッセージ数 (左:CAM, 右:CPM)

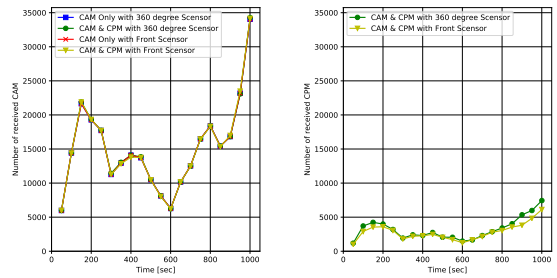

図 17 LuST Mini Scenario (低密度シナリオ) の受信メッセージ数 (左:CAM, 右:CPM)

ネットワークシミュレータの Omnet++, Artery や F^{2}MD といった Omnet++上で利用できるフレームワークを用いてシミュレーション環境の構築を行なった. CPM を送受信するために, Artery の CaService を参考に CpService を実装し, さらにその情報を活用した提案手法の実装を F^{2}MD のカルマンフィルターを用いて行なった. 交通シナリオには, 高速道路での交通量が大きい LuST Scenario と 一般道路のみを含む LuST Mini Scenario を用いて, 現実的な交通パターンでのシミュレーションを行い, 真陽率と偽陽率の観点から評価を行なった.

いずれの交通シナリオにおいても, 提案手法を用いた場合, 真陽率の水準を保ったまま, CAM のみの情報を用いる時に比べて偽陽率を改善することができている. 提案手法は高密度の交通シナリオにおいてより効果が大きくなり, CPM を活用することで, 前方 60° センサから 360° センサに変更しなくても, それ以上の効果が得ることができた.

CAM や CPM は周囲環境の認知力に大きな影響を与え, CITS の効率性や快適さだけでなく, 安全性に関わることから, 不正行為検出手法に関しても, 真陽率だけでなく偽陽率の改善し真のメッセージを拒否せず承認することが重要である. また, CITS の研究において主となる ETSI で CPM の標準化に向け, 様々な分析が行われているにも関わらず, CAM と CPM の両方を包括したシステムにおける不正行為検出手法に関する研究は多くない.

本研究により提案した手法は, CAM と CPM を包括したシステムで作動し, 現実的な交通シナリオにおいて, 真

陽率の低下を抑えながら偽陽率の改善を示していることから, さらなる交通シナリオや攻撃に対する分析, 真陽率, 偽陽率の改善に関する研究を行うのに値すると言える.

参考文献

[1] SAE International. Taxonomy and definitions for terms related to driving automation systems for on-road motor vehicles. *SAE International,(J3016)*, 2016.

[2] 公益財団法人自動車技術会. Jaso テクニカルペーパ「自動車用運転自動化システムのレベル分類及び定義」. https://www.jsae.or.jp/08std/ (2020-12-24).

[3] 国土交通省. 「自動運転のレベル分けについて」. https://www.mlit.go.jp/common/001226541.pdf (2020-12-24).

[4] Etsi En. 302 665 v1. 1.1: Intelligent transport systems (ITS), communication architecture. *ETSI EN 302 665 V1*, Vol. 1, , 2010.

[5] EN Etsi. Intelligent transport systems (ITS); vehicular communications; basic set of applications; part 2: Specification of cooperative awareness basic service. *ETSI, Sept*, 2014.

[6] Tcits Etsi. Intelligent transport system (ITS); vehicular communications; basic set of applications; analysis of the Collective-Perception service (CPS).

[7] 学塚田. 自動走行を支える協調型 its と車車間・路車間ネットワークの展望 (車車間・路車間通信の開発動向と自動運転へ向けた展望). 車載テクノロジー = Automotive technology, Vol. 6, No. 11, pp. 1–7, aug 2019.

[8] R W van der Heijden, S Dietzel, T Leinmüller, and F Kargl. Survey on misbehavior detection in cooperative intelligent transportation systems. *IEEE Communications Surveys Tutorials*, Vol. 21, No. 1, pp. 779–811, 2019.

[9] T R Etsi. 103 415,". *Intelligent Transport Systems (ITS)*.

[10] Jonathan Petit, Florian Schaub, Michael Feiri, and Frank Kargl. Pseudonym schemes in vehicular networks: a survey. *IEEE COMMUN SURVEYS TUTORIALS*, Vol. 17, No. 1, pp. 228–255, March 2015.

[11] Maxim Raya and Jean-Pierre Hubaux. The security of vehicular ad hoc networks. In *Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks*, SASN '05, pp. 11–21, New York, NY, USA, November 2005. Association for Computing Machinery.

[12] Bryan Parno and Adrian Perrig. Challenges in securing vehicular networks. In *Workshop on hot topics in networks (HotNets-IV)*, pp. 1–6, 2005.

[13] Z Lu, G Qu, and Z Liu. A survey on recent advances in vehicular network security, trust, and privacy. *IEEE Trans. Intell. Transp. Syst.*, Vol. 20, No. 2, pp. 760–776, February 2019.

[14] Philippe Golle, Dan Greene, and Jessica Staddon. Detecting and correcting malicious data in VANETs. In *Proceedings of the 1st ACM international workshop on Vehicular ad hoc networks*, VANET '04, pp. 29–37, New York, NY, USA, October 2004. Association for Computing Machinery.

[15] Bin Xiao, Bo Yu, and Chuanshan Gao. Detection and localization of sybil nodes in VANETs. In *Proceedings of the 2006 workshop on Dependability issues in wireless ad hoc networks and sensor networks*, DIWANS '06, pp. 1–8, New York, NY, USA, September 2006. Association for Computing Machinery.

[16] M Sun, M Li, and R Gerdes. A data trust framework for VANETs enabling false data detection and secure vehicle tracking. In *2017 IEEE Conference on Communications and Network Security (CNS)*, pp. 1–9, October 2017.

[17] N Bißmeyer, S Mauthofer, K M Bayarou, and F Kargl. Assessment of node trustworthiness in VANETs using data plausibility checks with particle filters. In *2012 IEEE Vehicular Networking Conference (VNC)*, pp. 78–85, November 2012.

[18] Attila Jaeger, Norbert Bißmeyer, Hagen Stübing, and Sorin A Huss. A novel framework for efficient mobility data verification in vehicular ad-hoc networks. *International Journal of Intelligent Transportation Systems Research*, Vol. 10, No. 1, pp. 11–21, 2012.

[19] Shuntaro Azuma, Manabu Tsukada, Teruaki Nomura, and Kenya Sato. A method of detecting camouflage data with mutual vehicle position monitoring. In *The Sixth International Conference on Advances in Vehicular Systems, Technologies and Applications (VEHICULAR 2017)*, pp. 48–53, Nice, France, 2017. Best Paper Award.

[20] Shuntaro Azuma, Manabu Tsukada, and Kenya Sato. A method of misbehavior detection with mutual vehicle position monitoring. *IntTech18v11n12, International Journal On Advances in Internet Technology*, Vol. 11, No. 12, pp. 82–91, 2018.

[21] Sumo - simulation of urban mobility. http://sumo.sourceforge.net/ (2020-09-01).

[22] Omnet++ discrete event simulator. https://omnetpp.org/ (2020-09-01).

[23] Veins - vehicles in network simulation. https://veins.car2x.org/ (2020-09-01).

[24] Inet. https://inet.omnetpp.org/ (2020-09-01).

[25] Vanetza. https://www.vanetza.org/ (2020-09-01).

[26] Artery. http://artery.v2x-research.eu/ (2020-09-01).

[27] Framework for misbehavior detection(f^2md). https://www.irt-systemx.fr/en/f2md/ (2020-09-01).

[28] Hendrik-Jörn Günther, Julian Timpner, Martin Wegner, Raphael Riebl, and Lars Wolf. Extending a holistic microscopic IVC simulation environment with local perception sensors and LTE capabilities. *Vehicular Communications*, Vol. 9, pp. 211–221, July 2017.

[29] World Health Organization and Others. Speed management: a road safety manual for decision-makers and practitioners. 2008.