社団法人 情報処理学会 研究報告
IPSJ SIG Technical Report

2009－DPS－138 (26)
2009－CSEC－ 44 (26)
2009／3／6

VANET上で孤立端末が生成した位置依存情報の信憑性判定手法の評価

深谷大樹[†1] 石原 進[†2]

車々間アドホックネットワーク（Vehicular Ad hoc Networks:VANET）では，走行車両が生成した特定の位置に関連付けられた情報（位置依存情報）を配信することによる渋滞緩和，車両の衝突回避支援などへの応用が考えられている．このため，位置依存情報に付加された位置の信憑性が重要となる．例えば，渋滞の発生位置を偽ることで，他車両を意図的に誘導し，交通量を操作する等の不正が起こりうる．そのため端末が生成した位置依存情報の信憑性評価が必要となる．しかし，信憑性評価に位置依存情報の発生位置周辺の複数端末を利用する従来手法では，他端末と通信ができない端末（孤立端末）が生成した位置依存情報の信憑性評価ができなかった．本稿では，端末の孤立前後の他端末との遭遇記録を基にして，孤立中に存在していた存在範囲を予測し，それを基に信憑性評価を行う Malicious Isolated Node Detection using Mutual Observation（MIND-MO）を提案する．シミュレーションの結果，合理的な理由に基づき，孤立時に生成された虚偽の位置依存情報の信憑性判定を行う際に有用性があることを確認した．

Evaluation of a scheme for checking the believability of location-dependent information generated by isolated vehicles in VANETs

Daiki Fukaya[†1] and Susumu Ishihara[†2]

Dissemination of location dependent information is one of the important applications of vehicular ad hoc networks (VANETs) which will be used for avoidance of traffic congestion, traffic accident etc. If a position attached to such information is forged, many problems, e.g. vehicular traffic control by malicious users, will occur. Thus evaluation of the credibility of location dependent information is important. One solution for this is to obtain the same information by multiple nodes which can communicate each other. However, the solution can not applied for a case that an isolated node generates a location dependent data item. In this paper, we propose a Malicious Isolated Node Detection using Mutual Observation (MIND-MO) scheme for evaluating credibility of location dependent information generated by an isolated node in VANETs. In the scheme, the credibility is checked by estimating the possible location of the isolated node using records of encounters generated before and after the isolation. The simulation results showed that MIND-MO is useful for evaluating credibility of false location dependent information generated based on rational reasons by isolated nodes.

1. はじめに

近年，無線端末の普及により通信インフラを用いずに，車両に搭載された無線端末を用いて動的にネットワークを構築する Vehicular Ad hoc Networks(VANET) の研究が盛んに行われている．VAENT の利用用途として，コストの高いインフラの導入が困難な地域での高度道路交通システム (Intelligent Transport Systems : ITS) への適用が考えられている．

VANET において各端末の生成した位置依存情報—特定の位置に関連付けられた情報：交通情報や広告情報など—を配信することにより，車両の衝突回避支援や位置を限定した広告配信などを行うことを考える．このようなサービスでは各端末が配信する位置依存情報に含まれる端末の位置情報が大きな意味を持つ．例えば渋滞の発生位置を偽った情報を配信することで，他車両を渋滞箇所を通過しない経路へと意図的に誘導させることが可能となる．このような問題を防ぐために VANET では位置情報の偽りに対する対策が必要である．

VANET において受信した位置情報の信憑性を判定する方法として，相互に直接通信可能な複数端末が，同一地域で同様の情報が取得できたか否かによって信憑性の判定をする方法が提案されている[1)]．しかし，端末が他の端末と通信ができない状態 (孤立状態) において生成された位置依存情報は，文献 1) での前提条件—同一地域で複数の端末が同様の情報を取得する—が成り立たないため，信憑性評価を行うことができない．そこで本稿では端末が孤立した状態で生成した位置依存情報の信憑性を，端末の孤立前後の他端末との遭遇記録に基づいて評価する手法 MIND-MO（Malicious Isolated Node Detection using Mutual Observation）を提案する．またシミュレーションにより提案手法の有用性を検証する．

以下，2章では VANET における既存のセキュリティ対策手法について述べる．3章では本稿で提案する MIND-

†1 静岡大学大学院工学研究科
Graduate School of Engineering, Shizuoka University
†2 静岡大学創造科学技術大学院
Graduate School of Science and Technology, Shizuoka University

MO について述べる．4 章ではシミュレーション結果を示す．最後に 5 章で本論文をまとめる．

2. 関連研究

VANET での位置依存情報の改ざんに対するアプローチとして，

(1) 情報の転送途中での改ざん

(2) 虚偽の情報の配信

の二点を防ぐ従来手法について説明する．

VANET において情報の転送途中での改ざんを防ぐ手法として，各端末で通信される情報にデジタル署名を加える方法が多数提案されている[2)3)]．各端末は事前に認証局より発行された自身の ID に対応した秘密鍵を用いて情報にデジタル署名を施し，自身の証明書と共に転送する．これによりデータ転送途中のデータの改ざんを防ぐと共に情報の送信端末が認証局より認証された偽りのない端末であると判定できる．本稿で提案する手法においても，データ転送途中の改ざんを防ぐために上記手法を用いる．

VANET での虚偽の位置情報の配信を防ぐ方法として，Raya らは，複数の端末が同一地域で同様の情報を入手できたか否かによって信憑性を判定する方法を提案している[5)]（**図 1**）．この方法では，各端末は常に複数の他端末と通信が可能であるという前提に基づいて，隣接する複数の端末でグループを形成する．同一グループ内で同一の位置依存情報が生成されると，その中から選択された一つの位置依存情報に対して，同一の位置依存情報を生成した複数の端末が生成したデジタル署名を付加する．これにより，複数のデジタル署名が付加された位置依存情報を受信した端末は，複数のデジタル署名を用いて位置依存情報のクロスチェックすなわち信憑性評価を行うことが可能となる．しかし，各端末は常に他端末と通信可能であるという前提に基づいているため，他端末と通信ができない端末（孤立端末）が生成した位置依存情報の信憑性評価を行うことができなかった．

Leinmüller らは，各端末が定期的に配信するビーコンより求められる端末の平均速度，通信範囲，端末密度が閾値を越すとき，およびビーコンに含まれる位置が，建物や海の上など車両が存在しえない位置から送信されたことになっているとき，受信した情報を偽りの情報であると判定する手法を提案している．この手法は，本稿で提案する手法と同様に，データ生成時に存在していた位置の正当性を判定する手法であるが，本稿で提案する手法では，隣接端末が生成した情報のみならず，孤立した端末が過去に生成した記録を用いるという点で異なる．

3. 問題提起

2 章で述べたように従来手法では，孤立端末が生成した位置依存情報の信憑性評価を行うことができなかった．しかし，以下に示す例では端末が孤立中に生成した位置依存情報の信憑性評価が必要となると考えられる．

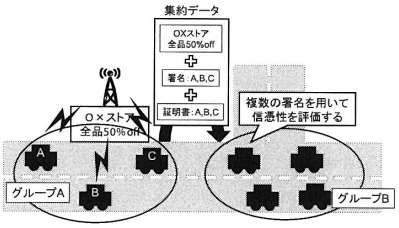

図 1 複数端末の生成した同一の情報に基づいた信憑性評価

例 「抜け道が工事中により通行できない」という位置依存情報を孤立中に生成した端末が，他端末に対してこの情報を配信する．この抜け道を通行したいと考える端末がこの情報を受信した時，従来手法では，孤立中に生成された情報の信憑性判定を行うことが出来ないため，この情報に信憑性があると認めることが出来ない．この結果，偽りのない有益な情報であるにもかかわらず受信者が利用することができないことになる．

次に，悪意のある端末が孤立時に虚偽の位置依存情報を生成する理由を明確にする．悪意のある端末が孤立時に虚偽の位置依存情報を生成する理由として

(1) 合理的な目的：自分の走行する経路の混雑を抑える．特定の店舗のある場所に多くの車両を誘導する．など

(2) いたずら目的

の 2 点が考えられる．仮に，虚偽の情報が発見された際に，その情報を生成したユーザに対して何らかの罰則があるとした場合，リスクを犯してまで，いたずら目的で情報を偽ることは稀であると考えられる．このことから，いたずら目的で虚偽の位置依存情報を生成する端末は，本稿の想定範囲外とし，本稿では合理的な目的で虚偽の位置依存情報を生成する端末についてのみ考える．合理的な目的の例を以下に書く．

例 車車間で交換した交通情報に基づき，目的地までの移動所要時間が最も短い経路を案内するようカーナビゲーションが行われると仮定する．このとき悪意のある端末が，目的地までの移動経路上で虚偽の渋滞情報を配信する．これを受信した端末は，移動時間のかかる渋滞箇所を避けて通行する可能性が高い．このため，悪意のある端末は目的地までの移動所要時間を短縮することが可能となる．同様の方法で，特定の店舗付近に多くの車両を誘導することも考えられる．

4. Malicious Isolated Node Detection using Mutual Observation (MIND-MO)

本章では，孤立中の端末が生成した位置依存情報の信憑性を評価する手法 Malicious Isolated Node Detection using Mutual Observation（MIND-MO）を提案する．

MIND-MO では，孤立中の端末が位置依存情報を生成した位置がとりうる範囲（予測存在範囲）を，孤立前後の他端末との遭遇記録や，道路毎に定められた車両の制限速度を基に予測し，その予測存在範囲内で位置依存情報が生成されたか否かによって信憑性を判定する．

4.1 想定環境

本稿では以下の環境を想定する．

- 常に他端末と通信可能な程度の車輌密度が存在する都市部において，抜け道などを通行した際に孤立するような環境を考える．
- VANET において複数の端末が自由に移動し，情報（ビーコン，他端末との遭遇情報，位置依存情報）を生成する．
- 各端末は GPS 等を用いることにより，自端末の位置を知ることができる．また，各端末は GPS 情報を用いて時刻同期を行う．
- データ転送途中でのデータ改ざんを防ぐため，各端末間で通信される情報（観測情報，位置依存情報）には，データ生成端末によるデジタル署名を加える．
- 各端末は直接通信可能な他端末の位置を，車両に搭載したレーダ等の装置を用いて知ることが出来る．ただし同装置を用いて端末 ID と位置の対応付けを行うことができない．
- 悪意のある端末（位置情報を偽る端末）はネットワーク全体に対して少数であり，複数の悪意のある端末による共謀は起こらない．
- 他端末からビーコンを受信すると，その端末を隣接車両リストに追加する．ビーコンを受信してからビーコンの TTL 時間だけ経過すると，そのビーコンの送信元車両を隣接車両リストから削除する．

4.2 ビーコンパケットの送信と受信

各端末は定期的に自身の ID i, 現在位置 $P(i,t)$，現在時刻 t，及びこれらの情報のデジタル署名 S_i と自身の証明書 C_i を含んだビーコン $B_{i,t}$ を定期的に 1 ホップブロードキャストする．ビーコンメッセージを交換することによって自己の現在位置を相互に通知することが可能となる．このビーコン $B_{i,t}$ は以下の式で表される．

$B_{i,t} =< (i, P(i,t), t), S_i(i, P(i,t), t), C_i >$

悪意のある端末が共謀すると，ビーコン中の ID を偽ることが可能であるが，本論文ではこのような共謀はないものとしている．虚偽の ID が用いられた場合はデジタル署名によって判定可能である．ビーコンに含まれる時刻情報に関する虚偽は，ビーコンの受信時刻とビーコンに含まれる時刻情報の差を用いて判定できる．

4.3 観測情報の生成と送信

MIND-MO では孤立前後の他端末との遭遇記録を基にして，孤立端末が生成した位置依存情報の信憑性評価を行う．しかし，他端末との遭遇記録を自端末が記録する場合，それを容易に改ざんすることが可能となる．そこで，第三者による自端末への目撃情報（観測情報）を用いることで遭遇記録の信憑性を高める．

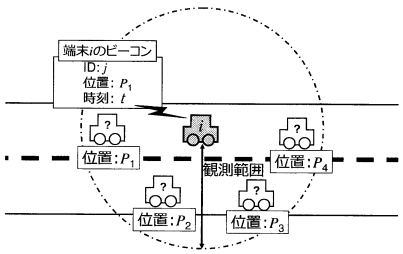

図 2 観測結果と ID の対応づけ

端末 i は他端末からビーコン B を受信した際に，その端末 j に対する観測情報 $I_{i,j,t}$ を生成する．しかし，ビーコンに含まれる位置情報に関しては，ビーコン送信者の通信範囲内の位置ならば，容易に偽ることが可能となるため，他端末から受信したビーコンの位置情報を受信しただけでは，その情報を信用することができない．

そこで，他端末の正しい位置情報を取得するため，4.1 で述べた通り，各端末は直接通信可能な他端末の位置を車両に搭載したレーダ等を用いて取得する．ただし，レーダ単体で観測対象の端末 ID まではわからない．そのため，観測範囲内の他端末からビーコンを受信することで観測結果と端末 ID の対応付けを行い，観測した端末の ID を把握する．

具体例を**図 2** に示す．端末 i が周辺の複数の他端末を時刻 t に観測した結果として，それらの位置が図 2 のように得られたとする．端末 i は，他端末 j からビーコン $B_{j,t} =< i, P(j,t), t >$ を受信したとき，位置 $P(j,t)$ を観測していれば，それが端末 j であると判定する．なおこのとき端末 j から受信したビーコンに含まれる位置が自身の観測結果に存在していない場合，端末 j がビーコン情報を偽っていると判定する．なお，複数の悪意のある端末が共謀すると，虚偽の位置情報を含む偽りのビーコンを通常の端末に送り，それに基づく誤った観測情報を生成させることが可能となるが，このような場合は本論文での想定範囲外である．またデータ転送途中での改ざんを防ぐために，生成した観測情報 $I_{i,j,t}$ に端末 i によるデジタル署名 S_i と端末 i の公開鍵の電子証明書 C_i を付加する．生成された観測情報 $I_{i,j,t}$ は以下の通りである．

$I_{i,j,t} =< (i, j, t, P_i(j,t)), S_i(i, j, t, P_i(j,t)), C_i >$

$(i, j, t, P_i(j,t))$ は観測者 i が時刻 t に位置 $P(j,t)$ で端末 j を観測したことを表す．

端末 j を直接観測しなかった他の端末は，その観測情報を受信することで，時刻 t における端末 j の位置 $P_i(j,t)$ を信用する．また，このようにして生成された観測情報は，一定の時間が経過する毎にまとめて 1 ホップブロードキャストすることで，過度なトラフィックの増加を抑制する．

4.4 観測情報の受信

受信した観測情報を全て保持し続けると，各端末の記

憶領域を圧迫するため，各端末は MIND-MO を利用する際に最低限必要なもののみを保持する．ある端末が受信した観測情報は，それが自端末に対するものであるか否かにより扱いが異なる．被観測者である端末 j に対する観測情報 I_{i,j,t_1} を受信した端末 x が，被観測者 j であるか否かによって，以下のいずれかの動作をする．

4.4.1 端末 x 自身が被観測者 j のとき

端末 i により時刻 t_1 に観測された自分自身に対する観測情報（被観測情報）I_{i,j,t_1} を受信した端末 $x = j$ は，自身が保持する観測情報リストに含まれる自端末に対する被観測情報を更新する．観測情報リストは，自端末もしくは他端末による各端末への観測情報を，各端末毎に保持するもので，他端末から配信された観測情報を受信する度，または自端末が他端末を観測する度に随時更新される．

各端末は，自分自身の被観測情報に関しては，最近の 2 つのみを保持する．この 2 つは，孤立中に自身が生成した位置依存情報 $L_{i,t}$ を他端末に配信するとき，$L_{i,t}$ に付加される．

4.4.2 端末 x が被観測者 j 以外のとき

端末 x は，他の端末 j に対する観測情報 $I_{i,j,t}$ を受信すると，自身が保持する観測情報リストに含まれる端末 j に関する観測情報を更新する．

他端末に関する観測情報リストは，その端末が最近通過した道路セグメント 2 つの中心に最も近い位置での観測情報および，最新の観測情報の 3 つを保持する．

4.5 位置依存情報の生成と送信

端末 i は時刻 t_{gen} に位置 $P(i, t_{\mathrm{gen}})$ に関する位置依存情報 $D(P(i, t_{\mathrm{gen}}), t_{\mathrm{gen}})$ を生成すると，この情報に端末 i によるデジタル署名 S_i と端末 i の公開鍵の電子証明書 C_i を付加したメッセージ $L_{i,t_{\mathrm{gen}}}$ を生成する．

$$L_{i,t_{\mathrm{gen}}} =< i, D(P(i, t_{\mathrm{gen}}), t_{\mathrm{gen}}), S_i(D(P(i, t_{\mathrm{gen}}), t_{\mathrm{gen}})), C_i >$$

$L_{i,t_{\mathrm{gen}}}$ の生成後に端末 i が初めて他端末 x_{after} により観測された時 (t_{after})，その時の観測情報 $I_{x_{\mathrm{after}},i,t_{\mathrm{after}}}$ と，時刻 $t_{\mathrm{before}}(< t_{\mathrm{gen}})$ における他端末 x_{before} から自端末への最新の観測情報 $I_{x_{\mathrm{before}},i,t_{\mathrm{before}}}$ を $L_{i,t_{\mathrm{gen}}}$ に付加し，1 ホップブロードキャストする．

位置依存情報を生成直後に他端末に配信することで，孤立後の位置情報の偽りを抑制することが出来る．配信したデータは，Epidemic アルゴリズム等を用いて遭遇した端末へ配布するか，Geocast 等で送られる要求に応答することで他端末に渡す．

4.6 受信した位置依存情報の信憑性判定

4.6.1 予測存在範囲の計算

$L_{i,t_{\mathrm{gen}}}$ を受信した端末 j は，以下に示す情報を用いて時刻 t_{gen} における端末 i の予測存在範囲 $A_{i,t_{\mathrm{gen}}}$ を計算する．

- 各道路に設定された端末の最大移動速度 $V_{\max}$
- 端末 i に対する時刻 t_{gen} 以前の最も新しい観測情報 $I_{a,i,t_{\mathrm{before}}}$
- 端末 i に対する時刻 t_{gen} 以後の最も古い観測情報 $I_{b,i,t_{\mathrm{after}}}$

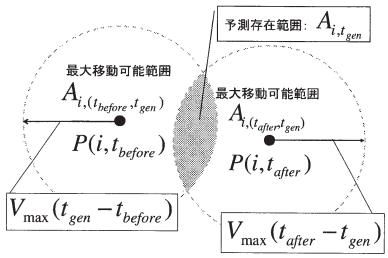

図 3 端末の予測存在範囲

端末 j は，位置 $P(i, t_{\mathrm{before}})$ から時間 $t_{\mathrm{gen}} - t_{\mathrm{before}}$ で移動可能な範囲 $A_{i,(t_{\mathrm{before}},t_{\mathrm{gen}})}$ と位置 $P(i, t_{\mathrm{after}})$ から移動可能な範囲 $A_{i,(t_{\mathrm{after}},t_{\mathrm{gen}})}$ を求める．これより端末 i の時刻 t_{gen} における予測存在範囲 $A_{i,t_{\mathrm{gen}}}$ は以下の式で求められる．(**図 3**)

$$A_{i,t_{\mathrm{gen}}} = A_{i,(t_{\mathrm{before}},t_{\mathrm{gen}})} \cap A_{i,(t_{\mathrm{after}},t_{\mathrm{gen}})}$$

予測存在範囲 $A_{i,t_{\mathrm{gen}}}$ を計算する際に用いた端末 i への観測情報は，位置依存情報 $L_{i,t_{\mathrm{gen}}}$ に付加されたもの，および端末 j が保持する観測情報リストの中から選出される．

4.6.2 信憑性の判定

端末 j は，受信した位置依存情報 $L_{i,t_{\mathrm{gen}}}$ が以下の条件を満たすとき，$L_{i,t_{\mathrm{gen}}}$ に信憑性があると判定する．

(1) 孤立端末 i が生成した位置依存情報 $L_{i,t_{\mathrm{gen}}}$ を生成した位置 $P(i, t_{\mathrm{gen}})$ が予測存在範囲 $A_{i,t_{\mathrm{gen}}}$ に存在する．

(2) 予測存在範囲 $A_{i,t_{\mathrm{gen}}}$ の面積 $|A_{i,t_{\mathrm{gen}}}|$ が，閾値 α よりも小さい (閾値 α は各端末が任意に設定したセキュリティレベルにより決定)

5. 性能評価

JiST/SWANS[6] シミュレータを用いて，孤立端末が生成した虚偽の位置依存情報に対する MIND-MO の効果を，虚偽の位置依存情報の検出率を求めることで検証した．

5.1 シミュレーションモデルの概要

3000 × 3000 [m] の領域上に，東西・南北方向の道路を 500 [m] 間隔に 7 本ずつ計 14 本配置した．この道路上を走行する車両は，無線 LAN IEEE802.11b を用いて通信を行う．通信帯域幅を 11 [Mbps] に固定し，通信可能半径は 100 [m] とした．各車両はビーコンを 1 [s] 間隔で 1 ホップブロードキャストし，その TTL は 1 [s] とする．また同一端末からビーコンを 5 回受信する度にその端末に対する観測情報を生成する．他端末に対して生成した観測情報は 5 [s] 毎にまとめて 1 ホップブロードキャストし，その TTL は 60 [s] とする．観測情報を受信した端末は，MIND-MO の仕組みに基づいて自身の保持する観測情報リストを更新する．各車両が孤立である

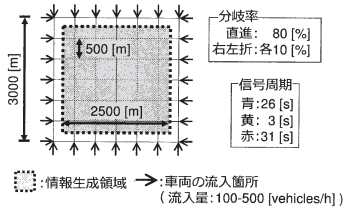

図 4 道路構造

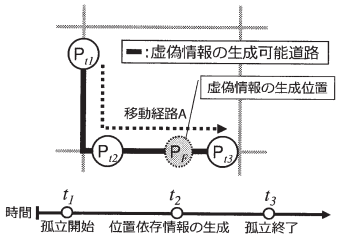

図 5 虚偽情報の生成モデル

か否かの判定は，隣接車両リストに車両情報が存在しているか否かで判定する．隣接車両リストに車両情報が存在しないということは，ビーコンの TTL 時間の間，自端末の通信範囲内に他端末が存在していなかった，すなわち孤立していたことになる．

市街地における交差点において，ビルなどの障害物による車両間の通信への影響を考慮するため，車両の位置を基に他車両と通信可能であるか判定する．直交する道路にいる車両同士が通信を行う際には，共通する交差点からの距離が閾値 10 [m] 以内である場合にのみ車両間の通信が可能であるものとした．

シミュレーションはシミュレーション時間 3600 [s] 行った．ただし安定したデータを計測するためシミュレーション開始から 600 [s] の間データの計測は行っていない．また，各データの結果はシミュレーション 20 回の平均値である．

5.2 移動シナリオ

交通シミュレータ NETSIM を用いて車両の移動シナリオを作成した．

各車両は，**図 4** に示す各道路の両端から流入し，領域内の道路上を自由走行速度（各道路に設定された制限速度）60 [km/h] で走行する．車両の走行速度は渋滞や信号待ちなどにより，自由走行速度を超えない範囲で適宜変化する．

シミュレーション領域内に流入した車両は，交差点において各方向に設定されている分岐率（直進：80%，右左折：各 10%）に基づいて移動し，道路の端点に来た時点でそのまま領域から流出する．各道路は両側 1 車線道路とする．また，各交差点には青 26 [s]，黄 3 [s]，赤 31 [s] の 60 [s] 周期で点灯する信号が設置されている．

各道路端からの車両流入量は 100-500 [vehicles/lane/h, 以下 vlh] まで 100 [vlh] 刻みで変化させた．

5.3 位置依存情報の生成モデル

各端末は定期的な位置依存情報の生成間隔毎に，その時に存在する道路セグメントに関する情報を生成する．ただし，位置依存情報を生成する道路セグメントをシミュレーション領域の中心 2500 [m] 四方に制限する．位置依存情報の生成間隔は 100 [s] とし，TTL は 300 [s] とした．なお，今回の評価では孤立端末が生成した位置依存情報に対する提案手法の効果を検証するため，孤立端末は，生成位置を偽った位置依存情報（虚偽の位置依存情報）のみを生成するものとした．MIND-MO では，位置依存情報を生成直後に配信する．同時に，孤立時に生成された位置依存情報は，その情報の信憑性評価を行うために，孤立前後の被観測情報を付加する必要がある．このため，孤立時に生成された位置依存情報は，情報生成後に初めて被観測情報を受信した後，1 ホップブロードキャストされる．このとき配信される位置依存情報には，孤立前後の被観測情報を付加する．これを受信した端末は，これに付加された孤立前後の被観測情報を基に，受信した位置依存情報の信憑性判定を行う．

5.4 虚偽情報の生成モデル

悪意のある端末は提案手法の仕組みを知らないものとする．悪意のある端末が，時刻 t_1 に位置 P_{t_1} で孤立し，時刻 $t_2(t_2 > t_1)$ に位置 P_{t_2} で位置依存情報を生成する．その後，時刻 $t_3(t_3 > t_2)$ に位置 P_{t_3} で他端末と通信可能になった際に，位置 P_F で位置依存情報を生成したと偽る（**図 5**）．このときの位置 P_F は孤立前後 $[t_1, t_3]$ に移動した経路 A 上からランダムに選択する．

5.5 評価指標

孤立端末が配信した虚偽の位置依存情報を受信した端末が，受信したそれを虚偽の情報であると判定できるか否か，すなわち虚偽の位置依存情報の検出率を用いて MIND-MO の評価を行う．

- 虚偽の位置依存情報の検出率
  シミュレーション期間中に，虚偽の位置依存情報が検出された回数を虚偽の位置依存情報が生成された回数で割った商
- 虚偽長
  位置依存情報の本当の生成位置と偽りの生成位置間の距離（例：図 5 の例での虚偽長は，P_{t_2} から P_F までの距離）

5.6 結　　果

図 6 に，MIND-MO を用いた虚偽の位置依存情報の検出率を示す．また**図 7**, **図 8** の (a)(b) にそれぞれ虚偽の位置依存情報を検出できた場合と出来なかった場合の，車両の孤立時間と虚偽長との相関関係を示す．

図 6 より，悪意のある端末が，MIND-MO を未知であるという条件において，端末の流入台数が 200 [vlh] 以上の時に 80%以上の検出率があることがわかる．端末の流入台数が 100 [vlh] のときには，流入台数が 200 [vlh] の時に比べて，検出率が 10%小さい．この一因として車両の孤立時間が関係していると考える．孤立時間が長くなると，予測存在範囲の面積，すなわち位置依存情報の

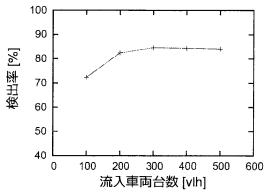

図 6 虚偽の位置依存情報の検出率

生成位置を偽ることが可能な範囲が拡大し，それに伴い検出率が低下する．

図 7,8 に流入車両台数 100,200 [vlh] のときの車両の孤立時間と虚偽長との相関関係を示す．このうち (a) はシミュレーション時間内に生成された虚偽の位置依存情報が MIND-MO により検出できた場合のデータのみをプロットしたもの．(b) は検出が出来なかったもののみをプロットしたものである．(a)(b) の図を重ねたものが，全虚偽データにおける孤立時間と虚偽長との関係を示すこととなる．(a)(b) より，孤立時間が長くなるにつれて，その虚偽長が長くなることがわかる．図 7,8 の (b) を見ると，虚偽を検出できなかったもののみに関しても，孤立時間が長くなると，虚偽長が長くなっているが，その大半は虚偽長が短い範囲に収まっていることがわかる．虚偽の位置依存情報の配信で他の車両を意図的に誘導しようとする場合，この虚偽長が長い情報を用いることが自然と考えられるが，MIND-MO ではこのような虚偽長が長い虚偽情報の検出が可能である．

図 8 の (a) より，孤立時間が 25 [s] 以上のときに虚偽の位置依存情報の生成数が少ないことがわかる．交差点付近では車両密度が高く，車両は隣り合う交差点間で孤立する可能性が高くなる．このため，車両が隣り合う交差点間を移動する時間（例：時速 40 [km/h] 移動距離 300 [m] の場合 27 [s]）を超えたときに，孤立時の位置依存情報の生成数が少なくなる．

5.7 MIND-MO を知る悪意のある端末に対する効果

MIND-MO を知る悪意のある端末が，予測存在範囲内で位置情報を偽ることを考える．このとき，MIND-MO の特徴—位置依存情報の生成位置が予測存在範囲内に存在するか否かにより信憑性を判定—より，虚偽の位置依存情報を検出することが出来ないという問題がある．しかし 3 章で述べた，悪意のある端末が合理的な理由により虚偽の位置依存情報を生成することを想定した場合，この問題を許容できると考えられる．

ある車両が移動時間の短縮をするために，他の車両に虚偽の渋滞情報を伝え，それに基づいて他の車両の移動経路を変更させるためには，情報の伝達遅延とその情報に基づく車両の経路変更までの遅延，虚偽の渋滞情報が与えられた位置へ自身が移動するために必要な時間を考慮に入れる必要がある．したがって，虚偽情報の発信元となる車両の位置と，虚偽の位置依存情報に与えられた位置との間の距離は十分に長くなければならない．これに対して MIND-MO では，虚偽長が長いほど位置依存

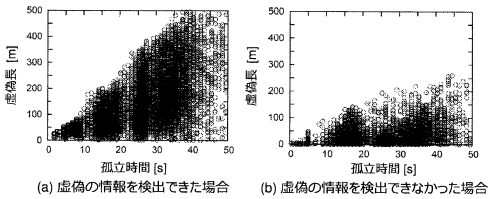

図 7 流入車両台数：100[vlh] における
虚偽長と虚偽の位置依存情報の相関関係

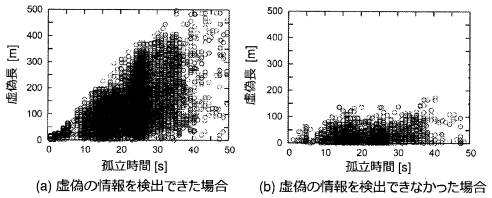

図 8 流入車両台数：200[vlh] における
虚偽長と虚偽の位置依存情報の相関関係

情報を多く検出できるという特徴がある．従って，合理的な目的達成のために生成した虚偽長の長い虚偽情報は MIND-MO によって検出される．このため，悪意のある端末が MIND-MO の存在を知っていたとしても，その目的の達成は困難である．

6. ま と め

本稿では，VANET における孤立端末が生成した位置依存情報の信憑性評価を行う手法を提案した．提案手法では，位置依存情報の生成位置の信憑性を，それに付加された端末の観測情報，およびネットワークの中で配布された観測情報を用いることで判定する．シミュレーション結果より，悪意のある端末が他端末の移動経路を意図的に変更させるといった，合理的な理由により虚偽の位置依存情報を生成する悪意のある端末に対して，MIND-MO を用いることで，その虚偽長を短く抑えることが可能であることが確認できた．しかし，虚偽長が短い際に検出率が低くなるという問題は残る．

謝　辞

本研究は，科学研究費補助金若手研究 A(18680008) の研究助成金によるものである．ここに記して謝意を示す．

参 考 文 献

1) T. Leinmüller, et al.: “Improved security in geographic ad hoc routing through autonomous position verification,” VANET ’06, 2006.
2) M. Raya, et al.: “The security of vehicular ad hoc networks,” SASN ’05, 2005.
3) M. El Zarki, et al.: “Security issues in a future vehicular network,” European Wireless, 2002.
4) G. Calandriello, et al.: “Efficient and robust pseudonymous authentication in VANET,” VANET ’07, 2007.
5) M. Raya, et al.: “Efficient secure aggregation in VANETs,” VANET ’06, 2006.
6) JiST – Java in Simulation Time / SWANS – Scalable Wireless Ad hoc Network Simulator: http://jist.ece.cornell.edu/index.html