VANETs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に関する一検討

深谷大樹† 石原進‡

†静岡大学工学部 ‡静岡大学創造科学技術大学院

1 はじめに

Vehicular Ad hoc Networks(VANETs) では, 車両が自身の位置及びその位置で取得した位置依存情報 (位置, 交通, 広告情報など) を他端末に配信することにより衝突回避や広告配信などに利用することが考えられている. そのため VANETs では配信情報に含まれる端末の位置が大きな意味を持つ. 例えば端末が他端末とマルチホップで通信する際に, 本来その通信経路に含まれていない端末が, その通信経路に含まれるようにするため自身の位置情報を偽る. これにより情報を不正に取得することが可能となる.

このような位置情報を偽る端末による問題に対して, 文献 [1] では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によって信憑性の判定を行う手法を提案している. しかし図 1 のように, 端末 A が他端末の通信可能範囲から路地裏のような細い道に入り, 他端末と通信ができない状態 (孤立状態) では, 文献 [1] の前提 (同一地域で複数の端末が同じ情報を取得する) が成り立たない.

そこで本稿では端末が孤立した状態で観測した位置依存情報の信憑性を, その端末が孤立していないときに他端末と交換した情報に基づいて評価する方法について検討する.

2 孤立端末の生成した位置依存情報の信憑性判定手法

2.1 前提

VANETs を構成する全端末は固有の識別子を用い続けると, トラッキングが可能になってしまう等のプライバシーの問題が発生する. このため各端末は認証局から割り当てられた固有の識別子を複数保持し, 定期的に変更する. ただし端末が孤立状態の時に変更すると, 変更前と変更後の識別子を他端末が対応づけすることができなくなり, 自身の生成した情報の信憑性評価ができなくなる. よって, 孤立中には識別子を変更しない. また, 全端末は, 認証局より自身の持つ複数の識別子に対応した証明書を取得し, 保持しているものとする.

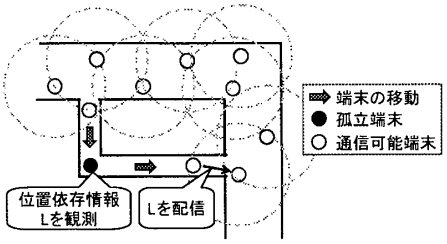

図 1: 孤立端末による位置依存情報の生成・配布

各端末は定期的にビーコンパケット B をブロードキャストするものとする. この B には端末が現在使用中の識別子 i, 時刻 t, 位置 $\boldsymbol{P}(i,t)$, 速度 $\boldsymbol{v}(i,t)$ 及びこれらの情報のデジタル署名 S と自身の電子証明書 C_i が含められ, 以下の式で表わされる.

$$B_{i,t} = \langle (i, t, \boldsymbol{P}(i,t), \boldsymbol{v}(i,t)), S_i(i, t, \boldsymbol{P}(i,t), \boldsymbol{v}(i,t)), C_i \rangle$$

各端末は通信可能範囲内に存在する他端末の位置が分かるものとする. 端末 i は時刻 t に位置 $\boldsymbol{P}(j,t)$ に存在している端末 j からのビーコンを受信し, レーダ等でこの端末の存在を観測すると, その観測情報 I をブロードキャストする. なお, $B_{i,t}$, $I_{i,j,t}$ はブロードキャストされたのち, フラッディング等によって隣接端末以外にも配信されてもよい. 観測情報 $I_{i,j,t}$ は以下の式で表わされる.

$$I_{i,j,t} = \langle (i, j, t, \boldsymbol{P}_i(j,t)), S(i, j, t, \boldsymbol{P}_i(j,t)), C_i \rangle$$

$(i, j, t, \boldsymbol{P}_i(j,t))$ は観測者 i が端末識別子 j の端末が時刻 t に位置 $\boldsymbol{P}(j,t)$ にあること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, $B_{i,t}$ および複数の端末 i による $I_{i,j,t}$ を受信することで, 時刻 t における j の位置を信用する.

端末 i は時刻 t に位置依存情報 $D(\boldsymbol{P}(i,t),t)$ を生成すると, デジタル署名 S_i と電子証明書 C_i を付加したメッセージ L を生成し, 最近受信した k 個の他端末 j

---

A study of credibility evalution of location dependent information generated by isolated vehicles on VANETs
Daiki FUKAYA† and Susumu ISHIHARA‡
†Faculty of Engineering, Shizuoka University ‡Graduate School of Science and Technology, Shizuoka University

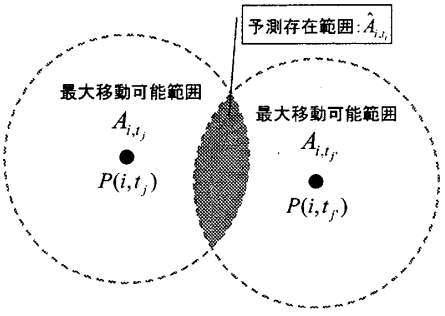

図 2: 位置推測方法

による自身の観測情報 I_{j,i,t_j} と共に他端末へ配布する．この配布方法については問わない．位置依存情報 $L_{i,t}$ は以下の式で表わされる．

$$L_{i,t} = \langle (i, t, \boldsymbol{P}(i,t), D(\boldsymbol{P}(i,t), t), \\ S_i(i, t, \boldsymbol{P}(i,t), D(\boldsymbol{P}(i,t), t)), C_i \rangle$$

問題の簡単化のため，これらの情報をブロードキャストする際にパケットロスや通信遅延は起こらないものと仮定する．

以上のような前提条件のもとで，孤立端末の観測した位置依存情報の信憑性の判定手法について検討する．

2.2 情報の信憑性評価

位置依存情報を受信した端末は，情報生成端末が孤立していない時に他端末から受信した観測情報に基づいて，情報生成時の位置を推測することにより信憑性を評価する．

2.2.1 位置依存情報の送信

端末 i が位置依存情報 L_{i,t_1} の観測時点で，他端末と通信可能なとき，文献 [1] の手法を用いて信憑性を評価する．

一方，端末 i は孤立中に位置依存情報 L_{i,t_1} を生成すると，他端末と通信可能になるまで位置依存情報 L_{i,t_1} を保持する．通信可能になると，端末 i は孤立する以前に受信した k 台の他端末 $\boldsymbol{O}_1$ による最も新しい端末自身の観測情報 $I_{j,i,t_j}(j \in \boldsymbol{O}_1)$，および，孤立後に最初に受信した自身に対する k' 台の他端末 $\boldsymbol{O}_2$ による自身の観測情報 $I_{j',i,t_{j'}}(j' \in \boldsymbol{O}_2)$ を位置依存情報 L_{i,t_1} と共に端末 r に送信する．ここで，t_j 及び $t_{j'}$ はそれぞれ端末 j, j' による情報の観測時刻を意味する．

2.2.2 位置推測方法

端末 r は，端末 i が生成した位置依存情報 L_{i,t_1} と $\boldsymbol{O}_1$，$\boldsymbol{O}_2$ に含まれる端末による端末 i の観測情報 I_{j,i,t_j}，$I_{j',i,t'_j}(j \in \boldsymbol{O}_1, j' \in \boldsymbol{O}_2)$ 及び，道路毎に定められた端末の最大移動速度 $v_{\max}$ を用いて，時刻 t_j から t_1 及び t_1 から $t_{j'}$ にかけての端末 i の最大移動可能範囲 A_{i,t_j}，$A_{i,t_{j'}}$ を求める．

求めた移動可能範囲 $A_{i,t_j}, A_{i,i_{j'}}$ の積集合が，端末 i の時刻 t_1 における予測存在範囲 $\hat{A}_{i,t_1}$ である．

$$\hat{A}_{i,t_1} = \bigcap_{j \in \boldsymbol{O}_1, \boldsymbol{O}_2} A_{i,j}$$

2.2.3 信憑性評価

孤立端末 i が観測した位置依存情報 $L(i,t_1)$ の位置 $\boldsymbol{P}(i,t_1)$ が予測存在範囲 $\hat{A}_{i,t_1}$ 内に存在していない時，観測情報は信頼できない．また $\hat{A}_{i,t_1}$ 内に存在しているとき，$\hat{A}_{i,t_1}$ の面積 $S(\hat{A}_{i,t_1})$ が，閾値 α よりも小さいとき，観測された情報は信憑性があると判定する．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される．

3 位置依存情報生成端末自身によって提供された観測情報の信頼性に関する検討

悪意のある孤立端末が位置依存情報を観測した際に，その情報に付加する自身に対する観測情報を，複数保持している自身の識別子を用いて作成するという可能性がある．このようなことがなされていないかを確認するための方法として，位置依存情報の信憑性を評価する端末が，受信した位置依存情報の生成端末が同一端末であるかを，端末の識別子を管理している認証局に問い合わせることが考えられる．しかし，認証局を介したこのような確認を許容すると，定期的に変更される各ノードの一連の ID について調べることによって，第三者が容易に端末の位置トラッキングが可能になってしまう．従って，このような機能を認証局が提供することは適切ではない．

そこで，フラッディング等により配信された端末に対する観測情報ならびにビーコンを，位置依存情報生成端末以外の端末からマルチホップで受信することにより，位置依存情報の信憑性評価を行う方法が考えられる．しかし，この手法ではネットワークにかかる負荷が大きいため，観測時刻からの経過時間，観測地点からの距離，観測端末からのホップ数などにもとづいて，観測情報とビーコンを間引きながら配布するなどの工夫が必要である．

4 まとめ

本稿では，VANETs における孤立端末が観測した位置依存情報についての信憑性評価手法を検討した．今後，特に孤立端末の送信する自身への観測情報を信用しない場合に注目して，シミュレーション等によって提案手法を適用可能な条件について検討する予定である．

参考文献

[1] M. Raya, et al. “Efficient Secure Aggregation in VANETs,” in proc.of VANET’06, 2006.