

車両位置相互監視に基づくなりすまし検知手法のロジスティック回帰分析による性能向上

山村 竜也[†] 奥西理貴[‡] 佐藤健哉[‡]

[†]同志社大学工学部情報システムデザイン学科

[‡]同志社大学大学院理工学研究科情報工学専攻

1 はじめに

近年、コネクテッドカーの研究が盛んに行われており、V2X(Vehicle To Everything) 通信を用いて車車間やインフラ、クラウドとの通信が可能となってきている。その結果、車両位置や速度などのデータを他車やクラウドに送信することで様々なサービスが提供可能である。一方、車載ネットワーク、車車間通信へのなりすまし攻撃などがある。なお、「なりすまし」とは車両が故意に不正なデータを送信することである。なりすましの一つにクラウドへ送信する位置データのなりすましがあり [1]、コネクテッドカーが故意に偽の位置データをクラウドに送信することで、交通渋滞や事故を誘発することが可能となっている [2]。

本論文では、位置データのなりすましを検知する手法としてロジスティック回帰分析を用いた手法を提案する。

2 関連研究

2.1 車両位置相互監視によるなりすまし検知手法

位置データのなりすまし検知手法に東らによる手法(以下、既存手法)があり [3]、動作手順は以下の通りである。

1. 車両が自身の位置データと車車間通信によって得られる周辺車両の ID をクラウドに送信する。
2. その車両が送信した周辺車両の ID に紐づく位置データをクラウドのデータベースから検索し、その車両との距離から車車間通信範囲内か検証する。
3. 2 の検証結果として、車車間通信範囲内の車両台数が閾値を超えれば、その位置データを信用し、データベースを更新する。なお、閾値は基地局の車両密度の 50% とする。

2.2 問題点

既存手法の問題点として、閾値が固定であるため、非なりすまし車両も信用されるのに厳しい条件を満たす必要がある。そのため、非なりすましデータのうち、正しく非なりすましと判断された割合である特異度の指標が小さいことが挙げられる。

3 提案手法

3.1 概要

本研究では、各車両毎の今までにクラウドに送信したデータの信用指標として信用度という概念を導入し、信用度に対してロジスティック回帰分析を用いることで、閾値を動的に補正し、既存研究の問題点を解決する。なお、ロジスティック関数は S 字型の関数で極限として 1, 0 を取り、1, 0 に近づくにつれて増加率、減少率が小さくなる特徴があるので、信用度を用いて閾値補正を行うことに適している。信用度を基に、ロジスティック回帰分析を用いることで、信用できる傾向にある車両の閾値が低くなり、誤検知を抑えることができる。

3.2 信用度に基づいた閾値の補正

クラウドで位置データが信用された時に信用度を加算し、不信の時に信用度を除算することで信用度を更新する。また、ロジスティック回帰分析を用いることで閾値を補正する。ロジスティック回帰は一般的に (1) 式のように表され、本研究では $K=1$, $n_0=0.1$, $r=0.5$, x を信用度とし、 o を基準閾値(基地局範囲内の車両密度の 50%), y を補正閾値として (1) 式、(2) 式を計算することで補正閾値を求める。

$$g(x) = \frac{K}{1 + \left(\frac{K-n_0}{n_0}\right)e^{-rx}} \quad (1)$$

$$y = o/(g(x) + 1) \quad (2)$$

Improving the Performance of Spoofing Detection Methods Based on Mutual Vehicle Location Monitoring with Logistic Regression Analysis

Tatsuya Yamamura[†], Riki Okunishi[†] and Kenya Sato[†]

[†]Doshisha University

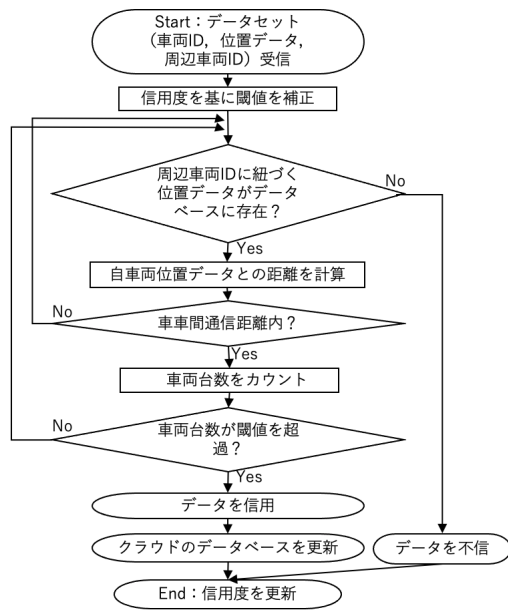


図 1: 提案手法のクラウドにおけるフローチャート

3.3 提案手法の動作手順

提案手法における動作手順は以下の通りであり、フローチャートを図 1 に示す。

1. 車両が自身の位置データと車車間通信によって得られる周辺車両の ID をクラウドに送信する。
2. その車両の信用度を基に補正閾値を計算する。
3. その車両が送信した周辺車両の ID に紐づく位置データをクラウドのデータベースから検索し、その車両との距離から車車間通信範囲内か検証する。
4. 3 の検証結果として、車車間通信範囲内の車両台数が閾値を超えれば、その位置データを信用し、データベースを更新する。
5. 信用度を更新する。

4 評価

4.1 評価方法

本研究では、ITS シミュレーションツールである Scenargie[4] を使い、1km 四方のマンハッタンモデルを作成して既存手法と提案手法の評価を行う。各車両は 0 km/h~30 km/h で速度を変更しながら走行する。車両台数は、日本の平均車密度を参考に 162 台とする。なお、なりすましパターンは、車車間通信外へのなりすましと車車間通信内へのなりすましで、なりすまし車両台数は 5 台とし、クラウドへ 1.0s 間隔になりすました位置データを送信する。また、提案手法によって処理が増えたことによる処理遅延の発生を確認するために、クラウドがデータセットを受信してから信用度を更新し終えるまでを処理時間として計測する。

表 1: 車車間通信外へのなりすましの評価結果

	既存手法	提案手法
特異度	67 %	90 %
再現率	93 %	91 %
F 値	82 %	91 %
平均処理時間	193 μ s	159 μ s

表 2: 車車間通信内へのなりすましの評価結果

	既存手法	提案手法
特異度	69 %	91 %
再現率	42 %	8 %
F 値	49 %	13 %
平均処理時間	175 μ s	178 μ s

4.2 評価結果

既存手法と提案手法の評価結果を表 1, 表 2 に示す。車車間通信外へのなりすましは、なりすましデータのうち、正しくなりすましと判断された割合である再現率は 2% 低下したが、特異度が 23% 向上し、F 値も 9% 向上した。平均処理時間は提案手法の方が短いので、処理遅延は発生していないことがわかる。車車間通信内へのなりすましは、提案手法では特異度は向上するが、再現率、F 値が低下することから、なりすましを正しく検知できていないことがわかる。このことから、閾値の補正が適切ではない可能性が考えられる。

5 まとめ

本研究では、ロジスティック回帰分析を用いて、動的に閾値を補正する手法を提案し、既存手法と提案手法の特異度、再現率、F 値と平均処理時間を比較した。評価の結果、提案手法により特異度を改善することを確認した。今後の課題としては、車車間通信内へのなりすましを検知できる適切な閾値の補正方法の検討が挙げられる。

本研究の一部は JSPS 科研費 20H00589 の助成を受けたものである。

参考文献

- [1] Aljawharah Alnassera, Hongjian Sunb, Jing Jiang, "CyberSecurity Challenges and Solutions for V2X Communications: A Survey", Computer Networks, Volume 151, Pages 52-67 (2019)
- [2] 長谷川 慶太, 原田 貴史, 弾 雄一郎, 鷲尾 知暁, "プローブ情報を用いた動的経路決定に対する虚偽情報混入に関する影響評価", 第 16 回 ITS シンポジウム (2018)
- [3] Shuntaro Azuma, Manabu Tsuakda, Kenya Sato, "Improvement of False Positives in Misbehavior Detection", VEHICULAR2018 (2018)
- [4] "SPACE-TIME Engineering", URL: <https://www.spacetime-eng.com/jp/products>, (参照:2021-1-6)