M-014

車両相互監視と位置外れ値検出による V2X 通信なりすまし検知手法

Misbehavior Detection by Vehicle Mutual Monitoring in V2X Communication and by Anomaly Detection

岡村 俊樹 †　　佐藤 健哉 †
Toshiki Okamura　Kenya Sato

1　はじめに

現在，V2X(Vehicle to Everything) 通信を用いて，車両間やインフラ，クラウドなどと通信を行うことができるコネクテッドカー (以下，CV) が開発されている．CV は，自車両の位置・速度情報や道路情報などを他車両やクラウドに送受信することで，様々なサービスが提供可能である [1]．しかし，ネットワークに繋がることで CV に関するセキュリティの問題が生ずる．CV の脆弱性を狙った攻撃として車載ネットワークへの攻撃や V2X 通信を用いた攻撃などがある．その 1 つに車両による位置情報のなりすましがある [2]．位置情報のなりすましは，犯罪を目的とした CV が他車両やクラウドに対して，故意に誤った位置情報を送信する攻撃である．位置情報のなりすましの結果，交通渋滞や事故などを誘発することが可能である [3]．CV 社会において，偽装された位置情報の検知は重要である．

本研究では，「なりすまし」を，車両が故意にクラウドに不正データを送信することと定義する．位置のなりすましは図 1 のように行われる．車両 A は，実際には P-a にいるが，クラウドに P-a' であると送信することで，位置のなりすましが可能である．

本論文では，位置のなりすましを検知する手法を提案する．

2　関連研究

位置情報のなりすまし検知手法に Wang らによる手法がある [4]．この手法では，車車間通信における RSSI(Received Signal Strength Indicator) を特徴量の 1 つとし，オートエンコーダーにて機械学習を行い，位置のなりすまし検知を行っている．この手法では，実際の位置となりすまし位置が 20 m 以内といった近い場合や，通信相手に対して，実際の位置での RSSI 値となりすまし位置での RSSI 値が近い場合になりすましの検知が困難であるという問題がある．

また，他の位置情報のなりすまし検知手法に東らによる手法 (以下，車両相互監視手法) がある [5]．車両相互監視手法は以下の通りである．

1. 各車両は，V2X 通信可能な自車両の周辺を走行する周辺車両と車両 ID を交換する．
2. 各車両は自車両の位置情報と 1 で得た他車両の ID 情報を基地局に送信する．その時，基地局は基地局 ID を付加する．
3. クラウドは，受信した 2 の車両情報が他車両から送られてくる情報と矛盾が無いかを確認する．矛盾がある場合，なりすましを行なっているとみなす．

当該手法では周辺車両が存在しない場合，なりすましが検知できないことが問題点である．

3　提案手法

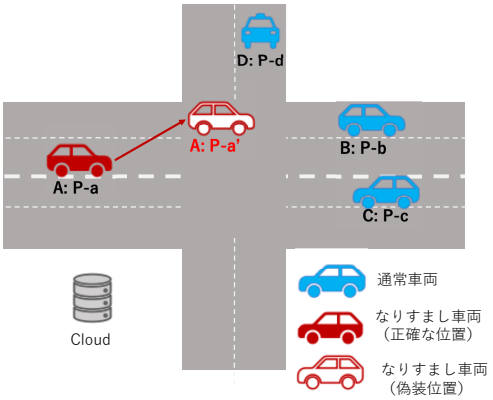
3.1　概要

本研究では，周辺車両が存在しない場合もなりすましの検知を行う手法を提案する．図 2 に車両相互監視手法と外れ値検出によりなりすましが検知されている様子を示す．車両 A，B，C は周辺車両がそれぞれ存在するため，車両相互監視手法を用いる．また，車両 D，E，F では周辺車両が存在しないため，外れ値検出を用いる．

3.2　外れ値検出

本研究では周辺車両が存在しない車両の時系列データに対して位置情報の急激な変化を外れ値検出を用いて検出し，なりすましを検知する．なお，外れ値検出とは，統計学において，ある母集団から以上標本を見つけ出すことである．

外れ値検出の手法には，特異スペクトル変換を用いる．時系列データの分布に依存せず様々な形状のデータに適用することができ，データに混入するノイズに強い



車両	A	B	C	D
クラウドが知る位置	P-a'	P-b	P-c	P-d

図 1　なりすましが行われている様子

† 同志社大学大学院 理工学研究科 情報工学専攻　Division of Information and Computer Science, Graduate School of Science and Engineering, Doshisha University

ためである．

式 (1) から (6) は特異スペクトル変換を表す．式 (1) において D は，位置の時系列データであり，$\xi^{(t)}$は時刻 t における (x, y) を要素とした位置データである．時系列データ D から，式 (2)，(3) の窓幅 M，列数 n の履歴行列 $X^{(t)}$とラグ L の列数 k のテスト行列 $Z^{(t)}$を生成する．

$$\boldsymbol{D} = \{\xi^{(1)}, \xi^{(2)}, ..., \xi^{(t)}\} \tag{1}$$

$$\boldsymbol{X}^{(t)} = [\boldsymbol{x}^{(t-n-M+1)}, ..., \boldsymbol{x}^{(t-M-1)}, \boldsymbol{x}^{(t-M)}] \tag{2}$$

$$\boldsymbol{Z}^{(t)} = [\boldsymbol{x}^{(t-k+L-M+1)}, ..., \boldsymbol{x}^{(t-M+L-1)}, \boldsymbol{x}^{(t-M+L)}] \tag{3}$$

式 (2)，(3) を特異値分解すると，左特異ベクトルの行列，式 (4)，(5) をそれぞれ得る．最後に式 (6) を用いて変化度 a を計算する．変化度 a は外れ値の度合いを示し，変化度 a の値が閾値以上となった場合，外れ値であるとみなす．

$$\boldsymbol{U}_r^{(t)} = [\boldsymbol{u}^{(t,1)}, \boldsymbol{u}^{(t,2)}, ..., \boldsymbol{u}^{(t,r)}] \tag{4}$$

$$\boldsymbol{Q}_m^{(t)} = [\boldsymbol{q}^{(t,1)}, \boldsymbol{q}^{(t,2)}, ..., \boldsymbol{q}^{(t,m)}] \tag{5}$$

$$\begin{aligned} a(t) &= 1 - \|\boldsymbol{U}_r^{(t)T} \boldsymbol{Q}_m^{(t)}\|_2 \\ &= 1 - (\boldsymbol{U}_r^{(t)T} \boldsymbol{Q}_m^{(t)}\text{の最大特異値}) \end{aligned} \tag{6}$$

3.3 動作説明

CV に対して以下の処理を行う．

1. 車両は，クラウドに自車両の位置情報と周辺車両 ID を一定周期毎に送信する．
2. クラウドは各車両の位置情報と周辺車両 ID を保持する．そして，車両毎に周辺車両が存在するか確認する．
3. 周辺車両が存在する場合，車両相互監視手法を適用し，周辺車両が存在しない場合は外れ値検出を行う．

外れ値検出を行う場合，以下の処理を行う．はじめに，クラウドは各車両の履歴行列 $X^{(t)}$ を作成する．その後，車両が周辺車両が存在しない状況になった時からテスト行列 $Z^{(t)}$ を作成する．履歴行列 $X^{(t)}$ とテスト行列 $Z^{(t)}$ に特異スペクトル変換を適用することで変化度を計測し，閾値以上の変化度になった場合になりすましが行われたと判断する．

4 提案手法の評価

4.1 評価環境

ネットワークシミュレーターである Space-Time Engineering(STE) 社が開発した Scenargie[6] を用いてシミュレーションを行う．Scenargie 上で 1 km 四方のマンハッタンモデルを作成する．日本の平均車両台数を参考に 162 台の CV 車両をシミュレーションする．なお，なりすまし車両は 5 台とし，クラウドに 1.0 s 間隔に位置の偽装情報をランダムに送信する．

4.2 評価方法

車両のなりすましの検知率と誤検知率を計測する．検知率と誤検知率は，以下の 2 つのケースで計測する．

1. 車両相互監視手法のみ
2. 車両相互監視手法 + 外れ値検出

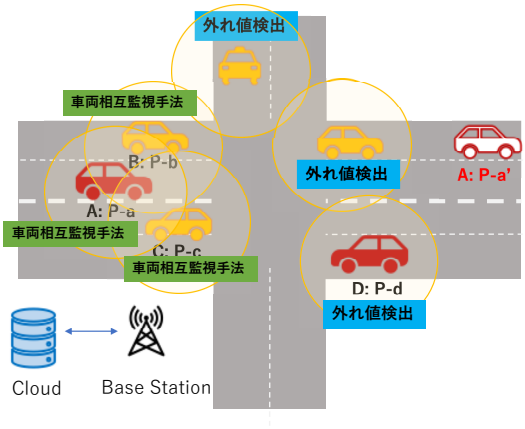


図 2　車両相互監視手法と外れ値検出によりなりすましが検知されている様子

なりすましの検知率は，行われたなりすまし行為に対して，クラウドが検知ができた比率である．誤検知率は，式 (7) のなりすまし検知の際の適合率を用いる．TP はなりすましが行われた際に，クラウドがなりすましだと判断した回数であり，FP はなりすましが行われていない際に，クラウドがなりすましだと誤って判断した回数である．

$$\text{適合率} = \frac{TP}{TP + FP} \tag{7}$$

5 まとめと今後の課題

本研究では，周辺車両が存在しない CV に，外れ値検出を用いてなりすましの検知を行う手法を提案した．シミュレーションでは，関連研究である車両相互監視手法と外れ値検出を用いてなりすましの検知率と誤検知率を計測し検討した．位置情報のなりすましは CV 社会において交通渋滞や事故を誘発する原因となる．本提案手法では周辺車両の存在に依存せず，位置情報のなりすましを検知することができ有用であると考える．

今後は，位置のなりすましが行われる状況を考慮し，外れ値検出のより適切なパラメーター設定を行い誤検知の軽減を行う必要がある．

参考文献

[1] 総務省, ”Connected Car 社会の実現に向けて” (2017)
[2] Aljawharah Alnassera, Hongjian Sunb, Jing Jiang, ”Cyber Security Challenges and Solutions for V2X Communications: A Survey”, Compuer Networks, Volume 151, Pages 52-67 (2019)
[3] 長谷川 慶太, 原田 貴史, 彈 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)
[4] X. Wang, I. Mavromatis, A. Tassi, R. Santos-Rodriguez and R. J. Piechocki, ”Location Anomalies Detection for Connected and Autonomous Vehicles,” 2019 IEEE 2nd Connected and Automated Vehicles Symposium (CAVS), Honolulu, HI, USA, 2019, pp. 1-5, doi: 10.1109/CAVS.2019.8887778.
[5] Shuntaro Azuma, Manabu Tsuakda, Kenya Sato, ”Improvement of False Positives in Misbehavior Detection”, VEHICULAR2018 (2018)
[6] ”SPACE - TIME Engineering”, URL:https://www.spacetime-eng.com/jp/products, (参照:2020-6-6)