M-019

V2X 通信における車両走行履歴のブロックチェーン化による位置情報偽装検知モデルの提案

A Proposal of Location Misbehavior Detection Model with Block Chain of Vehicle Trajectory through V2X Communication

中井 綾一 †　畑山 諒太 ‡　佐藤 健哉 ‡
Ryoichi Nakai　Ryota Hatayama　Kenya Sato

1　はじめに

近年, 自動運転や V2X(Vehicle to Everything) 通信の研究が盛んに行われている.V2X 通信は, 様々な方式で利用されており, 車両の位置情報や周辺情報のリアルタイム処理を可能とする.

しかし, 現在 V2X 通信においてサイバーセキュリティに関する懸念がある. 自動運転の場合,V2X 通信に従って, 自動車が運転判断を行うことから, 攻撃者が誤作動を起こさせたい場合には,V2X 通信を使った偽装行為は極めて有効である. 例えば, 遠隔で車両を操作し, 誤った位置情報を送信したとすると, 交通渋滞などを引き起こすことができる. このように, 車両の偽装行為は解決するべき問題となる. また, 最近では車両の走行履歴をクラウドで管理するアプリケーションが増えてきている.V2X 通信でもクラウドと併用した通信が考案されている [1] ので今後も, このアプリケーションの利用が増加すると予想される. しかし, クラウドを利用したサービスでは, クラッキングやサーバがダウンした際の損害が大きいことが課題である.

本研究では, 車両の偽装行為の中で位置情報の偽装に着目する. そして, 暗号通貨であるビットコインなどに用いられているブロックチェーンを参考にし, 位置情報の偽装の検知および車両の走行履歴を保護する手法を提案する. ブロックチェーンは P2P 型のネットワークアーキテクチャである. また, メリットとして, 情報の分散に長けており, データの改ざんがほぼ不可能であることが挙げられる.

2　関連研究

PRESERVE では, 認知局と PKI(公開鍵暗号) ソリューションを用いて, 各車両に証明書と秘密鍵を配布することで,V2X 通信のセキュリティを保護する手法が述べられている [2]. この手法は, 遠隔で車両を偽装する場合には効果的であるが, 車両自身が悪意を持った場合に脆弱であると指摘されている [3]. また, クラウドを利用したサービスでは, クラッキング攻撃を受けたり, サーバがダウンしてしまうと損害が大きいことも問題である.

3　提案システム

3.1　概要

前述の問題点を解決するために, 車両が悪意を持った場合の対策と情報を分散させる仕組みが必要となる. そこで本研究では, ブロックチェーンを用いて, 悪意を持った車両の位置情報の偽装を検知し, 車両の走行履歴の改ざんを防止する手法を提案する.

また本研究では, 車両の位置情報が格納された新しいブロックを前のブロックとつなぐための承認をするために, 新しいブロックのナンスを求める作業をマイニングとする. また, マイニングを行う他の車両のことをマイナー車両と定義する.

3.2　システムの構成

以下に提案システムの構成を示す．また, システムの構成図を図 1 に示す.

- 車両
  各車両は車両走行履歴のブロックチェーンを保有している. また, 位置情報を他の車両に 0.1 秒ごとに送信する.
- 悪意を持った車両
  各車両は車両走行履歴のブロックチェーンを保有している. また, 誤った位置情報を他の車両に送信する.
- マイナー車両
  新しいブロックのマイニングを行い, ブロックチェーンに追加する. マイニングができれば, 他の車両に新しいブロックを送信する.
- ブロック
  ブロックは, 前のブロックのハッシュ値や各車両の走行履歴, マイニングされた際の時間, マイニングの難易度, ナンス, 車両の走行履歴により構成される.
- 固定ノード
  各車両の位置情報の履歴を保存しておくノード. このノードで位置情報を検知する. 各車両から送られてきた位置情報を閾値まで受信を繰り返す. そして, 位置情報の要約値を計算し, 新しいブロックを作成する.

3.3　動作手順

提案手法のシーケンス図を図 2 に示す. 図 2 は車両, マイナー車両, 悪意を持った車両が 1 台ずつの場合を考慮している.

† 同志社大学 理工学部 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

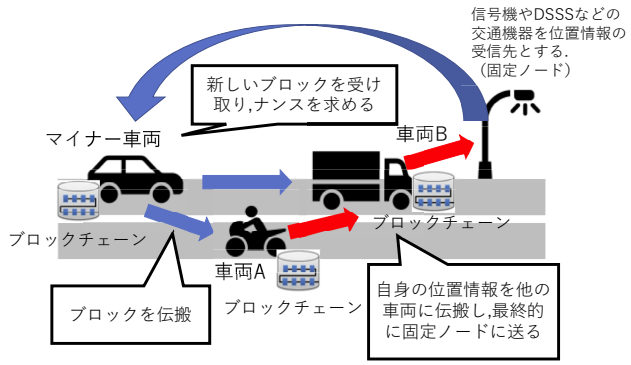

図 1　提案システムの構成図

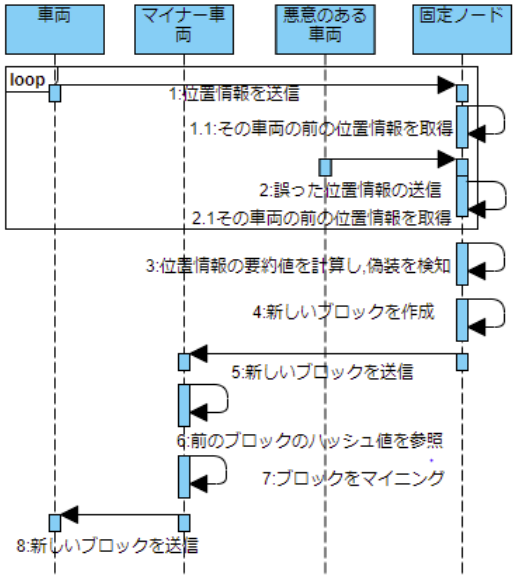

図 2　提案システムのシーケンス図

4　評価

4.1　評価項目

位置情報の偽装を検知する閾値, マイニングの難易度 (マイニングにかかる時間), 車両台数のパラメータを変化させながら, 車両の位置情報の偽装の検知率と全てのノードにブロックチェーンを追加されるまでの処理時間を評価する.

4.2　定性評価

前述のパラメータを変化させた場合の処理時間と検知率の定性評価を表 1 に示す. ここで, 表 1 は車両, マイナー車両, 悪意を持った車両が 1 台ずつの場合と比較したものである. また, 閾値の初期値は 5m/0.1s とし, マイニングの難易度 (マイニングにかかる時間) は約 10 分とする.

5　考察

位置情報の偽装を検知する閾値は, 直接処理時間と関係しないので, 出来るだけ小さい方が好ましいが, あまり

表 1　パラメータごとの処理時間と検知率

パラメータ		検知率	処理時間
閾値	小	向上	変化なし
	大	低下	変化なし
難易度	小	変化なし	向上
	大	変化なし	低下
車両台数	多	変化なし	低下

に小さすぎると位置情報を偽装していない車両まで位置情報を検知してしまう点が問題である.

マイニングの難易度に関しては, ブロックチェーンのデメリットとしてリアルタイム性がないということが挙げられるが, 難易度を簡単にすることでリアルタイム性が向上する. 暗号通貨に使われているブロックチェーンでは, 信用が大きく通貨の価値に関わっており, あまりに難易度が低いと改ざんされやすいブロックチェーンとして認識されるために, 通貨としての価値が大きく低下してしまう. しかし, 提案システムでは, 通貨としての価値が存在しないため, ブロックチェーンへの信頼性が必要なく, 位置情報の偽装を検知するという観点とデータの改ざんを防止する手法として用いることを考慮すれば, 難易度はできるだけ簡単にすることが望ましい.

車両台数を増やした場合は, 位置情報を送る回数が多くなるために, 新しいブロックを作成する時間が早くなる. そのために, マイナー車両の負担が大きくなり次第に新しいブロックが溜まり, 処理時間がかなり遅くなる. そこでマイナー車両の台数を増やすことで, マイナー車両の負担を軽減できる. また, 車両台数が多くなることで, 信頼できるノードが多くなるので, 固定ノードに送られる位置情報の信頼性が向上すると考えられる.

6　おわりに

本研究では, 情報の分散化, 暗号化, 否認防止という技術に長けているブロックチェーンの技術を参考に, 車両の位置情報の偽装を防止する手法を提案した. 今後, 自動運転が本格化するにつれて, サイバー攻撃の対策は大いに強化される必要がある. また, クラウドでの処理も増えるために, クラウドの負担を低減させることも重要になる.V2X 通信へのサイバー攻撃は多数存在するが, 提案手法では位置情報の偽装を防止し, クラウドを用いずに, 車両の走行履歴の改ざんへの対策ができるという点で期待できる.

謝辞

本研究の一部は JSPS 科研費 (JP16H02814) の助成を受けたものである.

参考文献

[1] 勝田将太, 屋代智之, “LTE の負荷を軽減して渋滞情報を提供する NAvi システムの提案”, 研究報告高度交通システム (ITS),Vol.56,No.9,pp.1-7,(2014)
[2] PRESERVE（2015）“PRESERVE - Preparing secure V2X communication systems
[3] Kaigui Bian,Gaoxiang Zhang,Lingyang Song (2017) ”Security in Use Cases of Vehicle-to-everything Communications” IEEE 86th Vehicular Technology Conference, 2017