2X-01

ビーコンレンジ署名によるV2X通信なりすまし検知手法

西川瑳亮† 中田輝‡ 滕睿§ 佐藤健哉‡

†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
§同志社大学モビリティ研究センター

1 はじめに

近年，ITS の分野において，自動運転や V2X 通信の研究が盛んに行われている．その中で，クラウドを利用した安全運転支援サービスがあり，注目されつつある．

一方で，クラウドを利用したシステムにおいて，クラウドに対する不正なデータ転送などの攻撃がシステムに大きな影響を与える [1]．そういった攻撃の一つに車両がクラウドに走行データや位置データを偽装した不正なデータを送信する行為がある [2]．なお，本論文において走行データや位置データを偽装した不正データを送信する行為を「なりすまし」と定義する．位置情報を偽装し，事故車を装って渋滞を巻き起こすなど，なりすまし攻撃は安全運転支援サービスにとって脅威であり，対策が必要である．

本研究では，車両の位置データと道路に設置しているビーコンの署名されたタイムスタンプ付きのデータを併せて送信することにより，特定の時間にビーコン通信範囲（レンジ）内に存在したことを証明するといったビーコンレンジ署名という考えを用いて，車両のなりすましを検知することを目的とする．

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

関連研究に車両位置相互監視によるなりすまし検知手法の研究がある．具体的には車両はクラウドに自身の位置データを送信する際に，周囲の車車間通信可能な車両の ID を取得し，併せて送信する．クラウドはそれらのデータセットを利用し，不正なデータの検出を行っている [3]．

なりすまし検知の流れは以下の通りである．

V2X Communication Spoofing Detection Using Beacon Range Signatures
Sasuke NISHIKAWA†, Hikaru NAKATA†, Rui TENG†and Kenya SATO†
†Doshisha University

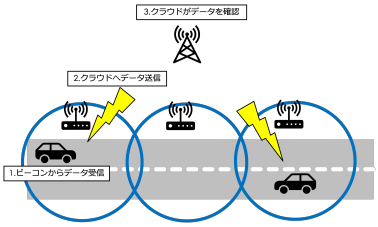

図 1: 提案手法のなりすまし検知の概要

1. 各車両は，自車の周辺を走行する車車間通信範囲内の車両と車両 ID を交換し，他車両の ID 情報をクラウドに送信する．
2. クラウドは，受信した 1 のデータセットをデータベースから検索し，そのデータから紐付く位置データから送信してきた車両が周囲の車両の車車間通信範囲内に存在するか検証する．
3. 2 の検証方法として，車車間通信範囲内の車両台数が閾値を超えていればその位置データを信用する．なお閾値は基地局の車両密度によって変化する．

2.2 問題点

先行研究の問題点として，周囲車両と位置情報を相互監視するという性質上，周囲に車両が存在しなければ検知できないという問題がある．

3 提案手法

3.1 概要

本研究の概要を図 1 に示す．本研究では，車両の位置情報と道路に設置されたビーコンの ID を併せて送信し，車両の位置情報のなりすましを検知する．また，ビーコンがデータを発信する際に，ビーコン ID に加えてタイムスタンプとデータの ID を付け，ビーコンの秘密鍵で暗号化する．検知できる状況としては車両が特定のビーコンの通信範囲内に存在し，かつその特定のビーコンの通信範囲外へのなりすまし攻撃である．な

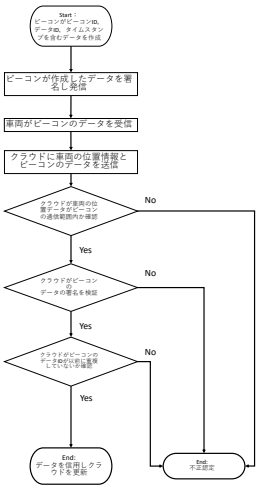

図 2: 検知までのフローチャート

お，ビーコンは，ビーコン ID，時刻情報，データ ID，秘密鍵を所持している．

3.2 動作手順

なりすまし検知までのフローチャートを図 2 に示す．検知の方法は以下の通りである．

1. ビーコンは，ビーコンの ID，タイムスタンプ，データの ID の 3 つを含んだデータを作成する．
2. ビーコンは，1 で作成したデータをビーコンの秘密鍵で暗号化し，車両に送信する．
3. 車両は，自車の V2X 通信範囲内のビーコンから 2 の暗号化されたデータを受け取る．
4. 車両は，自車の位置情報と 3 で得たビーコンのデータをクラウドに送信する．
5. クラウドは，受信した 4 の車両の位置情報から，付属しているビーコンのデータを受けとれる範囲内か確認する．
6. 2 つの情報に矛盾があればなりすましと認定し，なければその情報を信用する．

3.3 評価

本研究では，ネットワークシミュレーターである NS-3 上で実施する．提案手法のシステムにおいて想定している環境では，ビーコンは約 70m 間隔で隙間なく複数台設置する．これは一般の電波ビーコンの通信範囲が約 70m だからである．2 つのビーコンの通信範囲が重なっている位置を検証する際には，道路を一定区間に分け，通信範囲が重なっている区間内であればどちらのビーコンの情報であっても通信範囲内と認識するようにする．そしてビーコンがデータを発信する際に，ビーコン ID に加えてタイムスタンプとデータの ID を付け，ビーコンの秘密鍵で暗号化する．これは別のビーコンの通信範囲へのなりすましをする場合，なりすます位置のビーコンの情報をあらかじめ保持しておいて，攻撃するタイミングで併せて送信すれば検知されなくなるという問題，および，ビーコンのデータをコピーし，他の車両に転送することで，ビーコンの通信範囲という物理的制約を突破されるという問題を解決するためである．また，クラウドはビーコンの公開鍵を持っており，どのビーコンから送られてきたかが判る．これによって，対応したビーコンの公開鍵で復号できれば，ビーコンのデータは正しいものだと判断できる．

本研究では，関連研究における手法と，本研究の提案手法を用いた場合のなりすましの検知率と検知までの遅延時間を評価する．

4 まとめ

ITS の分野において，クラウドの利用は必要となりつつある．クラウドを利用した安全運転支援サービスを提供する上で，車両データを偽装して事故車両になりすまして渋滞を引き起こすことなどが可能であり，なりすまし攻撃は脅威となる．そのため，なりすましを検知する手法が必要となってくる．本研究では，車両がクラウドに送信するデータから不正データを検出する過程においてビーコンの位置情報と通信範囲を用いた手法を提案し，周囲に車両が存在しない場合においても，なりすましを検知することを目指す．

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] 押田大介，竹森敬祐，川端秀明，磯原隆将，山梨晃，塩田茂 雅，横田雅勝，“繋がる車のセキュリティ”，コンピュータセ キュリティシンポジウム 2014 論文集，No.2，pp.651-658，(2014).

[2] Aljawharah Alnassera，Hongjian Sunb，Jing Jiang，”CyberSecurity Challenges and Solutions for V2X Communications: A Survey”，Compuer Networks，Volume 151，pp.52-67，(2019)

[3] 東峻太朗，野村晃啓，塚田学，佐藤健哉，“車両位置相互監視による V2X 通信なりすまし検知手法”，マルチメディア，分散，協調とモバイル (DICOMO2017) シンポジウム，pp.325-331，(2017).