M-013

基地局情報を利用した車車間通信セキュリティ方式の提案

A Proposal of Security Method for Vehicle to Vehicle Communication Using Base Station Information

東 峻太朗 †　野村 晃啓 ‡　出村 友秀 ‡　佐藤 健哉 ‡
Shuntaro Azuma　Teruaki Nomura　Tomohide Demura　Kenya Sato

1 はじめに

1.1 研究の背景

近年，自動運転や車車間通信の研究が盛んに行われている．車車間通信には，VANET（Vehicular Ad hoc Network）が様々な方式で利用されるが，最近では LTE（Long Term Evolution）回線を用いて VANET との複合通信 [1] も考案されている．これは，クラウドを経由する車車間通信であり，道路情報・車両情報を一括管理し，リアルタイム制御を可能とするものである．

しかしそれに伴い，センサの誤認識や不正なデータ転送が，クラウドを介した車車間通信に大きな影響を与えてしまう．故意な不正データの転送・クラッキング行為がここ最近で増加の一途をたどっている．道路上で事故車両を装ったなりすまし情報をクラウドに送信すると，その道を通行止めにしたり，eCall(車両緊急通報システム) により必要ない緊急車両を呼ぶことさえできる [2]．車車間通信におけるなりすまし行為は，事故の誘発にも繋がり，安全運転支援を実現する上で解決すべき問題である．そこで本研究では，基地局情報・車両情報を利用し，車両のなりすまし行為に対するセキュリティ方式を提案する．

1.2 車両のなりすまし行為

車両のなりすまし行為として考えられるのは，ある車両になり代わる行為と，存在していない車両を存在させる行為である．前者は，ある車両を装うことでその車両しか知りえない情報を不正入手したり，ある車両そのものに影響を与えることができる．ある車両になり代わるためには，車両にクラッキングを仕掛け，クラウドとの通信に用いられている秘密鍵や車両固有の通信番号を入手する必要がある．後者の行為は，道路上に存在していない車両を出現させることで，その道を通行止めにし，渋滞を起こすことができる．クラウドに対し偽の車両情報を送ることで行えるため，前者と比べると容易にできるなりすまし行為と言える．

本研究では，前者のなりすまし行為は車両ディバイスの問題であるとし，クラッキングが行われないものとする．よって車両のなりすまし行為とは，存在していない車両を存在させる行為であるとする．

2 既存対策の問題点

GPS の位置情報と移動体の速度を利用したセキュリティ方式がある [3]．しかし，位置情報や移動体の速度のみを用いたセキュリティでは，その情報をクラウドに送信するだけで簡単になりすまし行為が行えてしまう．さらに，遠隔地からのなりすまし行為が防げない．この方式では，先ほど定義した本研究におけるなりすまし行為を対処できない．クラウドに情報を送信するだけでなりすまし行為が行えると言うことは，遠隔地からの送信を許し，その容易性からなりすまし行為が多発すると言える．

この問題があるために，実際に存在する車両からの情報をどのように信用すればよいのか，といった問題も生じる．すなわち，その場所に存在しているという位置情報を裏付けるものがないのである．車両のなりすまし行為を防ぐには，位置情報を裏付けるものが必要であり，さらに遠隔地からの不正行為も考慮する必要がある．

3 提案システム

3.1 概要

車両は自身の車両 ID をブロードキャストし，受け取った車両はその ID を保持する．クラウドと通信を行う際，車両は保持した ID と自身の車両 ID，クラウドとの通信 ID，位置情報を送信する．また，クラウドに情報が送られてくる過程で，基地局を通る．この基地局の基地局 ID をクラウドは知ることができ，送られてくる情報に添付される．クラウドは送られてきた情報をデータベースに格納しておき，なりすまし行為かどうかを判断する際に利用する．

本提案システムにおける基地局 ID とは，絶対的位置情報を保証するものであり，遠隔地からのなりすまし行為を防ぐ役割がある．しかし，基地局情報だけでは，基地局内からのなりすまし行為を許してしまう．提案システムにおいて，車車間通信における他車両を，自車両の目撃車両として扱うことでこの問題を解決する．目撃車両情報は相対的位置情報であり，基地局内でのなりすまし行為に対して有効である．つまり，基地局情報は遠隔地からのなりすまし行為ではないことを裏付け，目撃車両情報は位置情報を裏付けるものである．

3.2 前提条件

- 全ての車両が，車車間通信可能である
- 全ての車両が，基地局を介した通信が行える
- クラウドとの通信 ID は，盗まれない

3.3 システムの構成

- **クラウドとの通信 ID**
  車両 ID から生成される ID で，UUID(Universally Unique Identifier) である．この ID はクラウドとの通信時にだけ用いられるものであり，他車両は知ることができない．

† 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

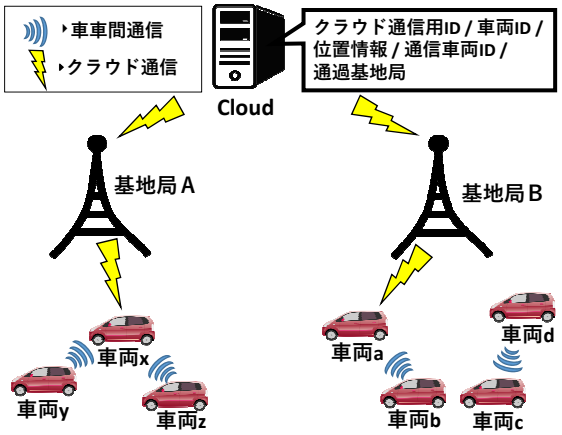

図 1　提案システム概要

- **クラウド**
  基地局から送られてくる車両情報を全て管理する．クラウドは保存してある各車両情報，基地局情報を基に，なりすましの検出を行う．

3.4　提案システム実現の手順

1. 車両は，ブロードキャストされた他車両 ID を入手する．
2. 車両はクラウドと通信時，クラウドとの通信 ID・保持している車両 ID・自分の位置情報を送信する．
3. 基地局は自身の基地局 ID を付加し，クラウドへ送信する．
4. クラウドは送られてきた情報を保存する．

3.5　なりすましの検出

図 1 に示した手順によって，クラウドへは車両情報と基地局情報が送られてくる．この情報を基に，なりすましの検出を図 2 の手順で行う．車両からクラウドへメッセージが送られた場合，クラウドはその車両がなりすましでないか判定する．まず，送信車両に該当するデータをクラウド上で検索し，その車両の位置情報と基地局情報を比較する．これにより，遠隔地からの不正アクセスを防ぐことができる．次に，目撃情報となる車両を検索し，送信車両との位置情報を比較する．位置情報どおりその場にいるのかどうかを，ここで判別することができる．つまり，基地局情報を偽装したとしても，目撃車両がいるのでなりすまし行為ができないということである．以上の操作をあらかじめ定めた規定回数行い，これを満たす車両をなりすまし車両でないと判断する．

4　評価

本評価では，今回提案した手法と，２章で示した既存手法を比較し，定性評価を表 1 に示す．

前述のとおり，基地局情報を使うことで遠隔地からのなりすまし行為を防ぐことができる．そして，車車間通信における相手車両を目撃車両として扱うことで，位置情報の偽装行為を防止できる．既存手法では，送られてきた情報が正しい情報なのか不明確であったが，提案手法では基地局情報と目撃車両情報を使うことで，車両情報の信用度も高くなっているが，周辺車両情報の使用やクラウド内で処理を行うため，システムが複雑となってしまう．

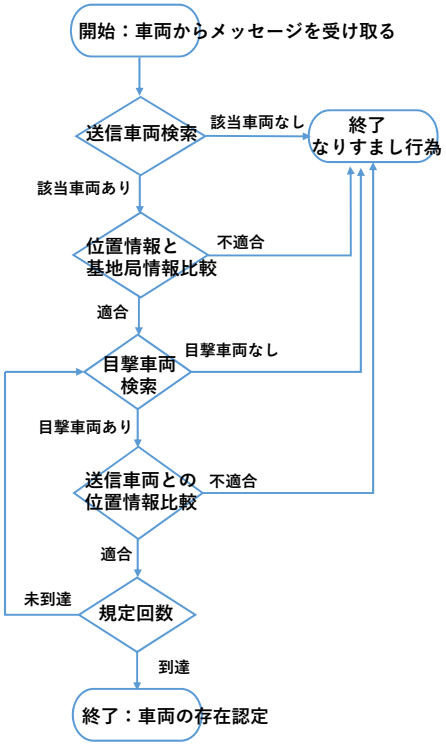

図 2　クラウド上でのなりすまし検出手順

表 1　提案手法と既存手法の比較

	提案手法	既存手法
遠隔地からのなりすまし行為	防げる	防げない
位置情報の偽装行為	防げる	防げない
車両情報の信用度	高い	低い
システムの複雑さ	複雑	単純

5　まとめ

本研究は，停車車両のなりすまし行為を防ぐという目的で進められてきた．停車車両の位置情報を，基地局情報と通信車両情報を用いて裏付けを行い，車両のなりすまし行為を防ぐことができた．本提案システムは，本研究で定義された車両のなりすまし行為に有効であり，有用性を示すことができた．

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] 平井智尚，“ EU における eCall の運用に向けた政策動向 ”，(2015) ＜ https://www.fmmc.or.jp/pdf/report/report_eu_ 20151001.pdf ＞，(参照 2016-05-26)
[3] 角田雅照，伏田享平，三井康平，亀井靖高，後藤慶多，中村匡秀，松本健一，“ 位置と速度を利用した移動体向け認証方式の提案 ”，電子情報通信学会技術研究報告．MoMuC，モバイルマルチメディア通信，106(359)，pp.11-16，(2006)