高安全自動車

不正侵入検出システムの需要増加

IoT技術の発展にも後押しされ，**ネットワークを介した外部との通信に基づく自動車制御技術（自動運転技術）**が普及

しかし・・・

遠隔でハッキングされたジープ

ANDY GREENBERG SECURITY 07.21.15 06:00 AM

HACKERS REMOTELY KILL A JEEP ON THE HIGHWAY—WITH ME IN IT

ジープをハッキングし
ブレーキを無効とした

実際に遠隔攻撃される事例が発生

https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

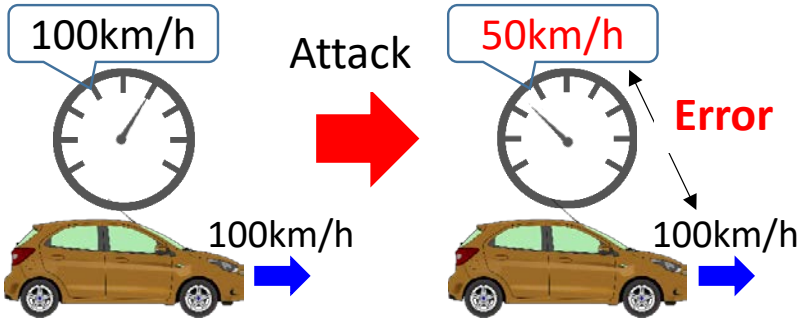
車載ネットワーク不正侵入検出システムの高信頼化が急務

想定される車載ネットワークへの攻撃事例

主に二種類の攻撃が想定される

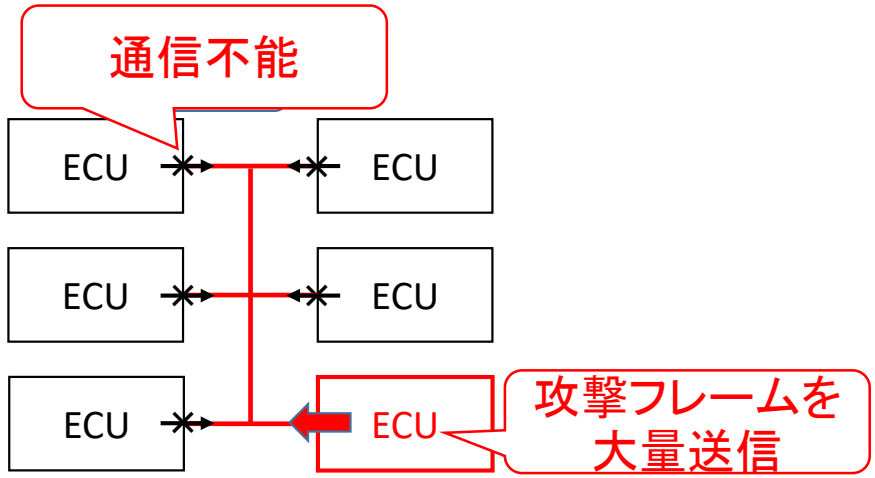
1. データの改ざん

データを改ざんすることで，
スピードメーターの値を狂わせる
などの誤動作を誘発



2. DoS 攻撃

攻撃フレームでバスを占有すること
により，通常フレームによる通信
を妨害



車は時に人的被害につながる危険性をはらんでおり，これら攻撃への対応が重要な課題となっている

従来手法の問題点

車載ネットワークを対象とした攻撃手法は二種類に大別できる

	*1NNベース手法	*2閾値ベース手法	提案手法
データ改ざん	++	+	+++
DoS攻撃	+	++	+++

それぞれ個別の手法を対象とした手法のみ

→ 複数の攻撃手法への対応が困難

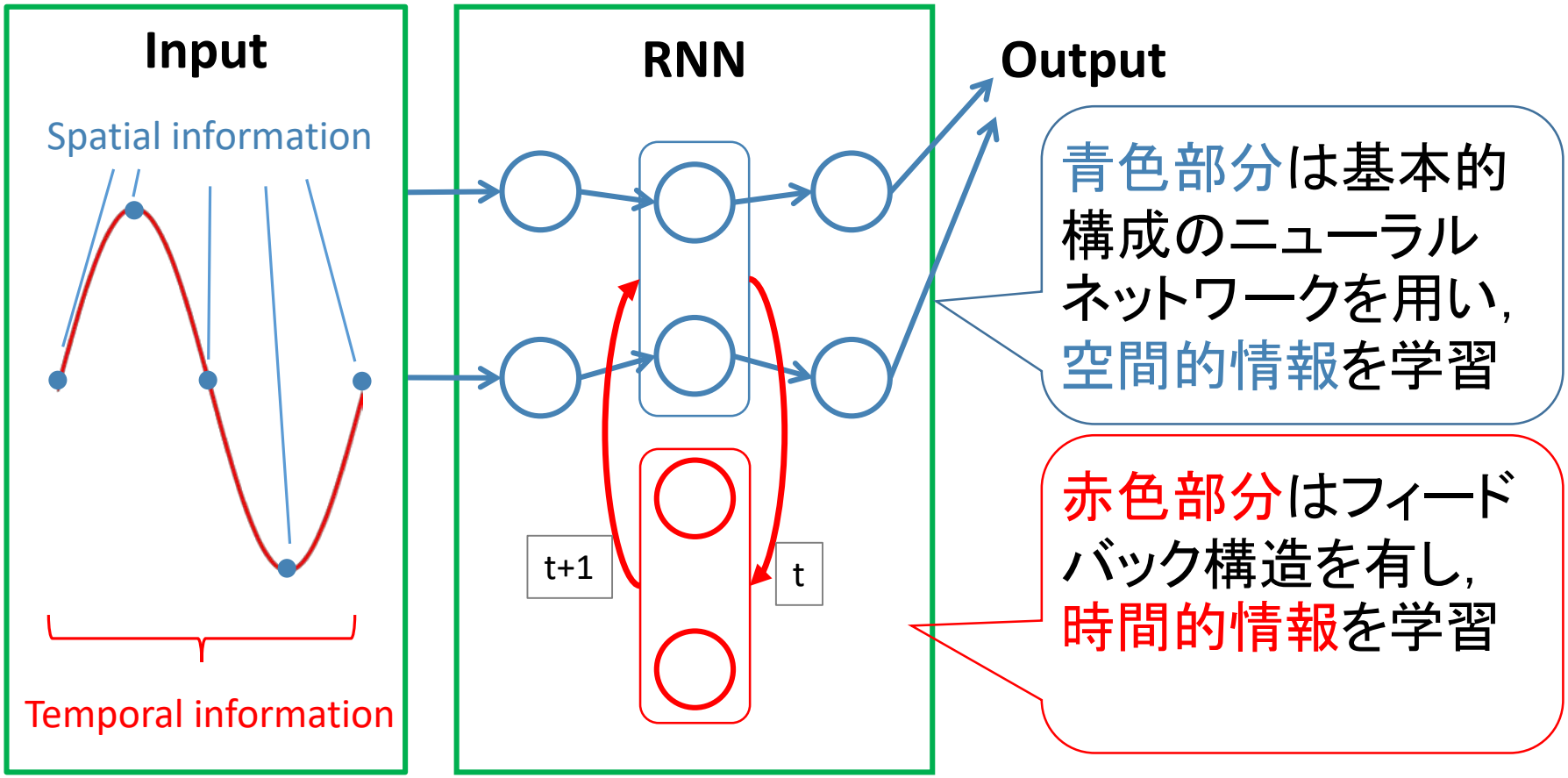
目的：全ての攻撃手法を統一的にカバー可能な手法を提案

**1) M. Kang et al, IEEE 83rd Vehicular Technology Conference, 2016.*

**2) H. M. Song et al, International Conference on Information Networking, 2016.*

RNN (Recurrent Neural Network)

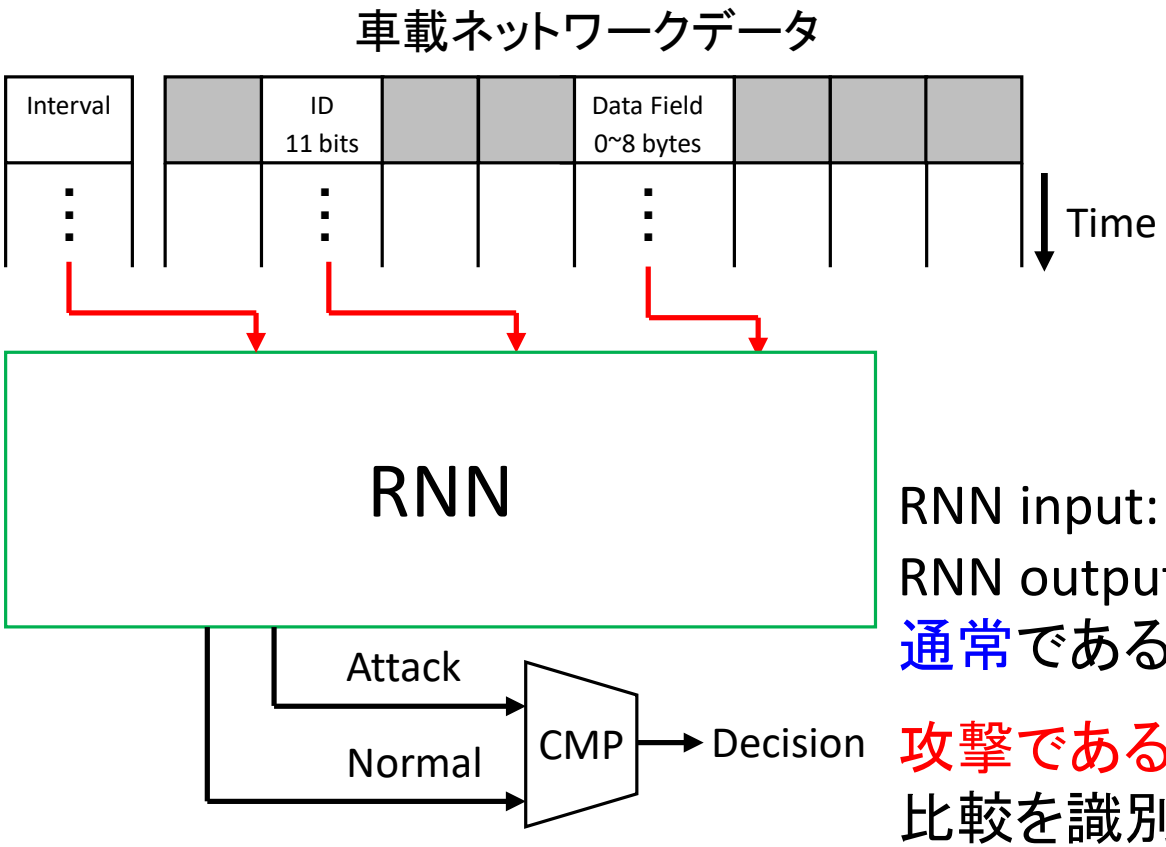
機械学習アルゴリズムの一つである**ニューラルネットワーク**に再帰構造を追加した構成である**RNN**を基本アルゴリズムとして活用



時系列特徴を用いた識別に広く用いられているRNNを使用

不正侵入検知システムの構成

RNNを用いることで時系列特徴を有効活用した識別を行う



時系列情報を用いた学習を行うことで，従来手法では識別が難しい攻撃も，統一的に検出

RNN input: Interval, ID, Data Fields

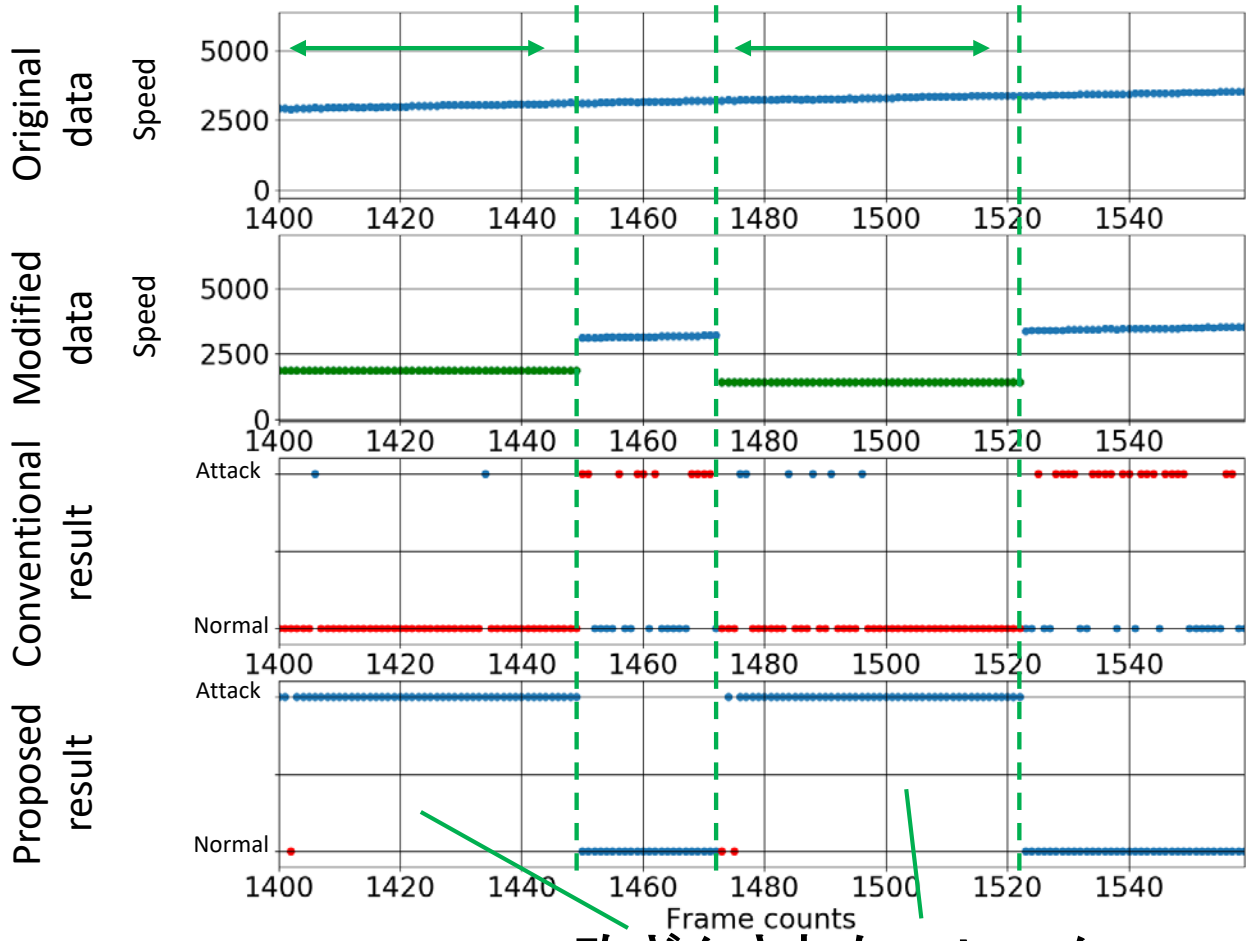
RNN output: フレームが攻撃であるか通常であるかの確率

攻撃である確率と通常である確率の比較を識別結果とする

以上の構成で各フレームが通常か攻撃かを識別

Data Field 改ざん攻撃 — 識別結果

図中緑色で示された部分に攻撃を入力



● Attack frames

● Misclassified data

従来のNNベース手法:
識別エラーが多数発生

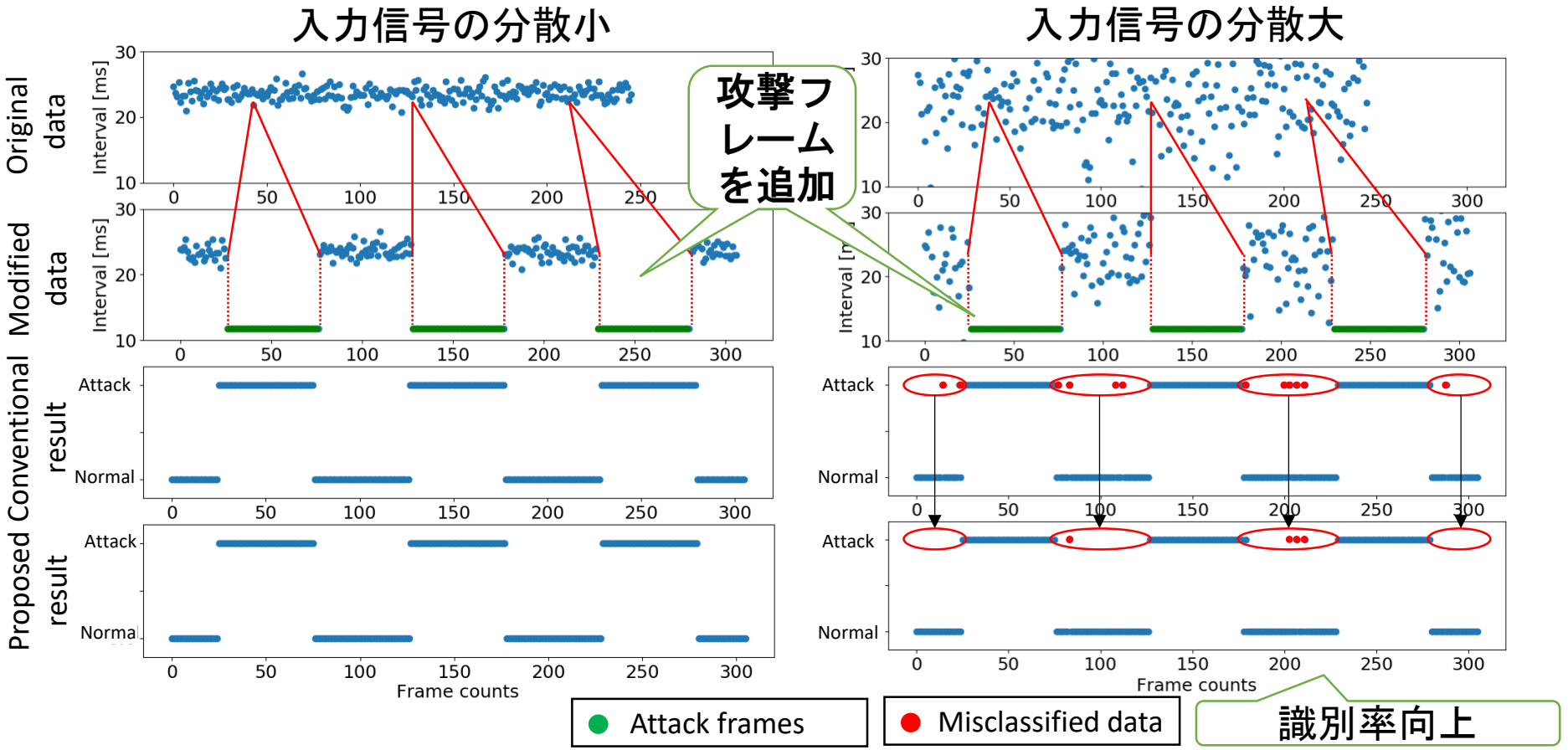
提案手法:
ほとんどの攻撃フレームを正しく検出

値が改ざんされたフレームを正しく識別

DoS 攻撃 — 識別結果

図中緑色で示された部分に攻撃を挿入

CANバスの混雑状況により，入力信号の分散が変化する



DoS攻撃の識別率を従来手法より向上