つながる車におけるセキュリティ対策のOSS実装

研究駆動コース 石原匠

協調型ITSが注目されており, 車車間だけでなく路側機, 歩行者, 広域ネットワークなど多くの移動体間で通信を行い繋げる取り組みがされている. 繋がることで交通安全性は向上するものの, セキュリティ的なリスクは大きくなる. セキュリティ対策としてはIEEE1609.2においてPKIを用いた手法が標準化されているが, 既存のOSSで公開されている自動運転OSやシミュレータ上では評価を行う環境がない. 今回はIEEE1609.2に準拠した検証環境を構築しPoC評価を行った.

1. 背景

◆協調型ITSとは[1]

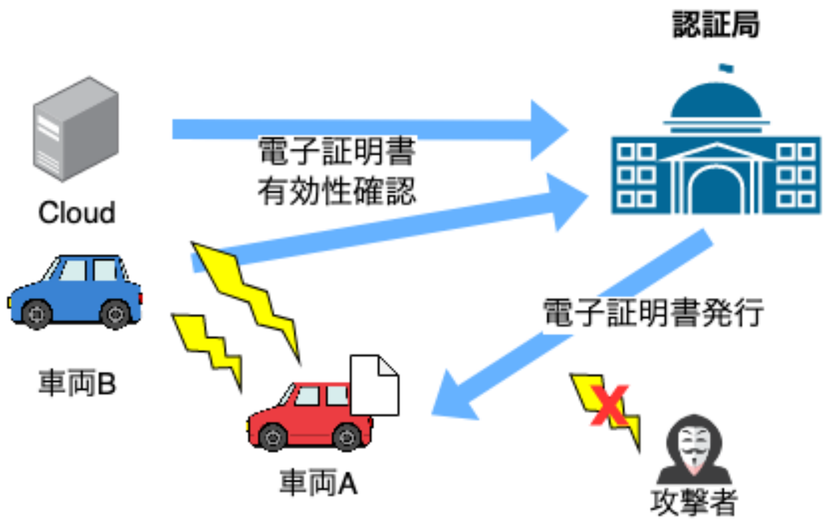
- ✓ 車載器, 路側機, 中央サーバ, 歩行者端末が道路交通を安全・安心・快適にするために情報タスクを共有するシステム
- ✓ DSRCやセルラー通信を用いて自車の情報(e.g. 位置情報, 速度)を送信する

→ **移動体が互いに協調することで交通の高度化が期待される一方でセキュリティリスクが高まることも懸念されている**

2. IEEE1609.2[2]

◆協調型ITS通信のセキュリティ対策

- ✓ **メッセージ送信者の真正性**
  - ➢ 自身が正しい送信者であることを証明するために認証局が発行する電子証明書と秘密鍵を用いる
- ✓ **メッセージ内容が改竄されていないことの保証**
  - ➢ 送信するメッセージ毎に秘密鍵を用いてデジタル署名を施す
  - ➢ デジタル署名はHMS(Hardware Secure Module)で行う



3. 自動運転開発の動向

◆OSSをベースとした開発

- ✓ Autoware
  - ➢ 自動運転オペレーティングシステム
- ✓ Apollo
  - ➢ 自律走行プラットフォーム

4. 課題

- ✓ **コネクテッドカーの通信部分はブラックボックス化されており, 既存のOSS自動運転ソフトウェアには組み込まれていない**

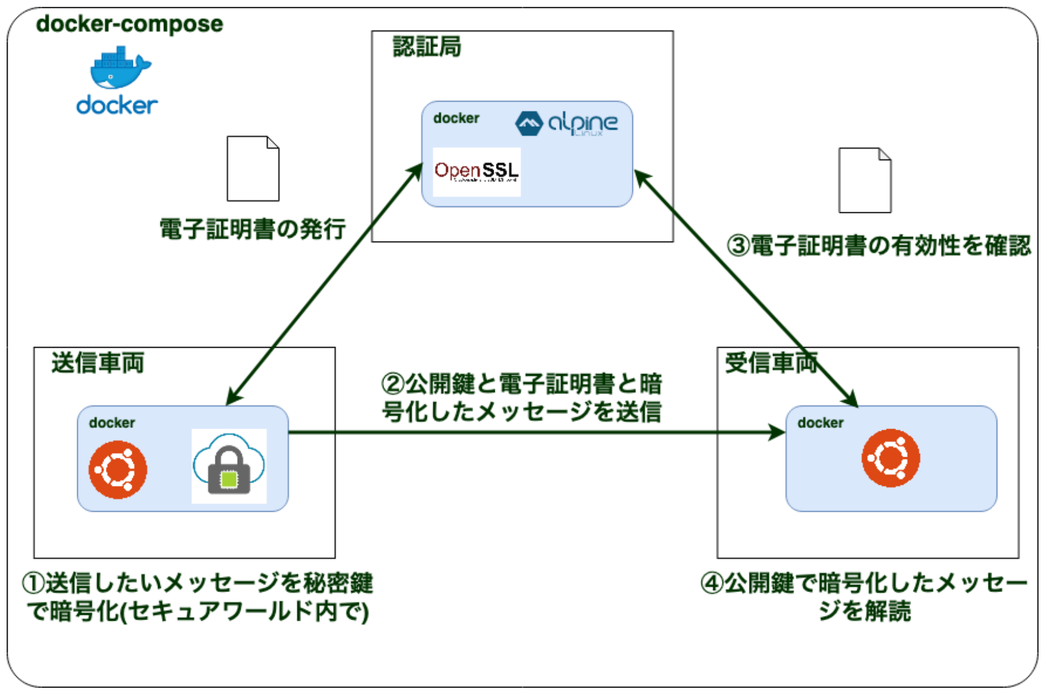
→ **研究として評価をしやすい環境が整っていない**

5. 提案

◆IEEE1609.2に準拠したOSS検証環境の構築

- ✓ 目的: 研究者が気軽にコネクテッドカーに対しての攻撃・検証が行える環境を提供

6. 実装



7. まとめ/今後

まとめ

- Docker上でので検証環境を構築することができた
  - ➢ 手元でセキュリティ対策の流れを再現することが可能になった

今後

- 自動運転OSSへの組み込み
  - ➢ Autowareの拡張としての実装
- MECなど新たなITSにおける要素への対応
  - ➢ 今回は車車間のみに着目した検証環境

[1] 自動走行を支える協調型 ITS と車々間・路車間ネットワークの展望 -https://tlab.hongo.wide.ad.jp/papers/Tsukada_AT2019.pdf
[2] IEEE Standard for Wireless Access in Vehicular Environments--Security Services for Applications and Management Messages-https://standards.ieee.org/ieee/1609.2/6038/