車両ネットワークにおける蓄積運搬転送方式の公開鍵更新方法の検討

情報科学科　仙石 大明　　指導教員：井手口 哲夫

1　はじめに

近年, 車両ネットワークで通信を行う研究が盛んに行われている. そのネットワークを構成する一つの方法として, 蓄積運搬転送方式がある. しかし, 車両ネットワークを構成する際にセキュリティの確立が重要である. 本研究では蓄積運搬転送方式を用いる際のセキュリティ機能として, 公開鍵暗号方式を用いたシステム設計を行い, 利用頻度を考慮したシステムの提案を行う.

2　蓄積運搬転送方式

ノードは情報を保持・蓄積しながら移動し, 他のノードと遭遇すると蓄積している情報を転送する方式である. 劣悪な環境でのデータ伝送性能が向上し, 明確なパスがない場合に有効である.

3　公開鍵配布システム

車両ネットワークにおけて考えられる脅威として,ITS フォーラムにおけるリスク分析の結果から, 誤メッセージ・メッセージの改ざん, なりすまし, リプレイ攻撃の 3 つの脅威がある. この対策として公開鍵暗号方式と電子署名を利用する公開鍵の配布システムを考える. この公開鍵配布システムでは先行研究 [1] の方式を利用する (図 1).

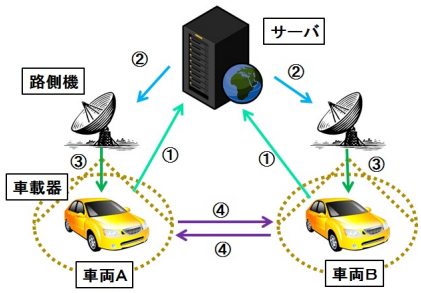

図 1　公開鍵配布システムの構成図

① ログイン要求を行い, サーバは車両 A の公開鍵を作成する.
② 車両 A の公開鍵を周辺の路側機に配布する.
③ 周辺の車両の公開鍵を一定量自身のバッファに蓄積する.
④ 車両 B の公開鍵で暗号化し, 車両 B へデータを送信する.

4　公開鍵更新方法の提案

公開鍵配布システムでは路側機通信範囲に入ると一定量の公開鍵を蓄積するが, ノードに蓄積できる公開鍵の数や, 公開鍵の更新する方法について考えなければならない. 本研究ではノードに保持できる最適な公開鍵の数から,4 つの公開鍵更新方法について検証し, シミュレーションによりその有効性を評価する.

検証 1　利用頻度を考慮したデータ配布手法 [2] を用いる方法
検証 2　常に最新の公開鍵に更新する方法
検証 3　路側機範囲内に入った時に公開鍵を更新する方法
検証 4　使用した公開鍵を優先的に保持して更新する方法

5　検証実験

表 1 にシミュレーションのパラメータを示す. シミュレーション時間は 30 分,1STEP は 0.01 秒刻みとする.

この実験での路側機範囲内と範囲外での最大通信回数は 5.4 回,4.6 回であるため, ノードに蓄積できる公開鍵の数は平均の 5 とする. 通信開始から通信終了までにかかる通信時間, 公開鍵が車載器のバッファにヒットする確率（hit 率）の 2 項目について,4 つの更新方法の比較評価する.

表 1　シミュレーションパラメータ

道路	片側一車線
車両台数	24 台,32 台,40 台,48 台,56 台
路側機間隔	$300m$,$400m$,$500m$,$600m$,$700m$
送信データサイズ	$100byte$
通信範囲	$100m$
車両速度	$50km/h(\pm 10km/h$ で変化)
システム遅延時間	$0.3s$

6　シミュレーション結果

シミュレーションは 10 回行い, その通信時間とバッファの公開鍵にヒットする確率の平均を求める. 図 2,3 に 4 つの更新方法の平均通信時間,hit 率を示す.

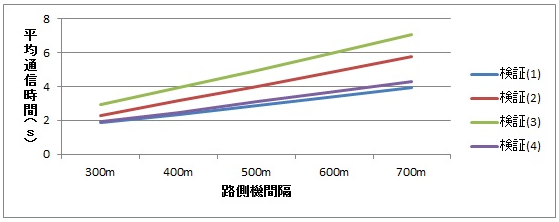

図 2　各路側機間隔における平均通信時間

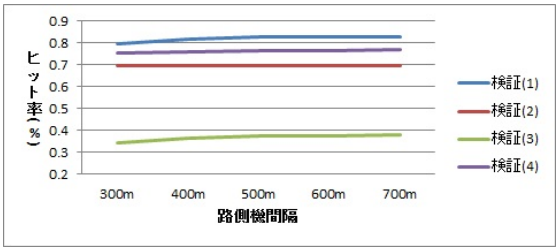

図 3　各路側機間隔の hit 率

この結果から, 検証 (1) が最も平均通信時間,hit 率が優れている. これは, 検証 (1) が利用頻度を考慮した更新を行ったことで, 通信相手の公開鍵の多くが自身のバッファに蓄積されるようになったため,hit 率や通信時間が向上したことが分かる. また路側機間隔が離れるほど路側機範囲外での通信回数が多くなるため,hit 率は路側機間隔が広くても変化しない. このことから利用頻度を考慮した方式の有効性が示されている.

7　おわりに

本研究では公開鍵配布システムの 4 つの公開鍵更新方法について検証した. 利用頻度を考慮することで, 路側機間隔が離れても通信時間が極端に増加しないことが分かる. 今後の課題として, 車両の出入りや複雑な道路状況の下で検証が必要である.

参考文献

[1] 佐藤 雅也: 車両ネットワークの蓄積運搬転送方式のセキュリティの検討, 平成 24 年度卒論研究
[2] 三浦 浩一, 掛田 悟史, 戸出 英樹, 瀧 寛和: 車両ネットワークにおける利用頻度を考慮したデータ配布手法, 電子情報通信学会 信学技報, NS2009-252,pp.507-510,2010.3