要 旨

路車間通信システムへの
SAS-2 相互認証方式の適用

岡崎 公大

近年，自動車事故の防止や交通情報などのサービスを提供する路車間通信システムの実用化に向けた取り組みが期待されている．路車間通信システムでは機器のなりすましや，偽の情報による交通秩序の乱れは脅威として大きく，各機器の真正性やメッセージの完全生の確保が必要である．対策として公開鍵暗号方式を用いた機器認証及び鍵の共有が挙げられる．しかし，低リソースが想定される車載器との通信を行う路車間通信システムでは，処理負荷による影響が大きいと考えられる．

本研究では，路車間通信システムの機器認証と鍵共有に，ワンタイムパスワード認証方式 SAS-2 を用い，高速かつ安全な相互認証方式の提案を行う．また，機器認証に要する時間を既存方式と比較し，提案方式の有用性を示す．

キーワード　SAS-2，認証，路車間通信システム

Abstract

SAS-2 Mutual Authentication method for Infrastructure Communication System

Kohdai Okazaki

In recent years, commercialization of an infrastructure communication system is expected. This is to prevent traffic accidents and provide traffic information. In the infrastructure communication system, traffic disturbance caused by fake information and fake devices andis serious as a threat and it is necessary to ensure reliability. As a countermeasure, device authentication and key sharing using the public key cryptosystem can be cited. However, in the Infrastructure Communication System that communicates with an on-vehicle device that is assumed to be low in resource, it is thought that the influence by the processing load is great.

In this research, we adopt an one-time password authentication method SAS-2 for device authentication of an infrastructure communication system, and realize high - speed and secure authentication. In addition, the time require for device authentication also shows the usefulness of the proposed method compared with the conventional method.

key words SAS-2, Authentication, Infrastructure Communication System