Integrating Smart Cards with Vehicular Networks: Architecture and Applications

Sriram Chellappan and Vamsi Paruchuri[1]

Abstract

Recently, vehicular networking has received tremendous attention from the research community. The Federal Communications Commission FCC has approved licensing and service rules for Dedicated Short Range Communications (DSRC) Service in the Intelligent Transportation Systems (ITS) Radio Service in the 5.850 - 5.925 GHz band. With these developments, along with development in radio technologies, a lot of research activities have been aimed at the realization of Vehicular AdHoc Networks (VANETs). This paper presents ideas in utilizing *Smart Card* based techniques in VANETs. A brief background on Smart Cards is first presented. A smart card based architecture for VANETs is then presented followed by two applications in this domain, and some critical issues to resolve for the realization of the proposed applications.

Background on Smart Cards

A smart card is a device that includes an embedded integrated circuit chip (ICC) that can be a secure microcontroller or equivalent intelligence with internal memory or a memory chip alone. The card connects to a reader with direct physical contact or with a remote contactless radio frequency interface. With an embedded microcontroller, smart cards have the unique ability to store large amounts of data, carry out their own on-card functions (e.g., encryption and mutual authentication) and interact intelligently with a smart card reader. Smart card technology conforms to international standards (ISO/IEC 7816 and ISO/IEC 14443) and is available in a variety of form factors, including plastic cards, fobs, subscriber identification modules (SIMs) used in GSM mobile phones, and USB-based tokens.

[1] Sriram Chellappan is with the Dept. of Computer Science, Missouri University of Science and Technology, Rolla, MO 65401 USA. Email – chellaps@mst.edu. Vamsi Paruchuri is with the Dept. of Computer Science, University of Central Arkansas, Conway, AR 72035 USA. Email – vparuchuri@uca.edu.

Smart cards are also gaining rapid popularity as a preferred credential for securely controlling physical and logical access. As a cryptographic device, the microcontroller at the heart of the smart card can support a number of security applications and technologies. Smart cards offer a high degree of physical security, secure data storage and support many authentication techniques commonly used to protect physical and logical access, including support for advanced symmetric encryption techniques like DES, 3DES, and asymmetric key services (like 1024 bit RSA) [1], on-card key generation, and protection for the privacy of the user's private key, secure storage for biometric templates, user IDs and passwords, support for one-time password generation, tamper resistant card body.

Smart Card based Architecture and Applications in VANETs

We propose a simple baseline architecture for leveraging smart cards in VANETs. There are three broad entities in the proposed architecture: a centralized (and trusted) key distribution entity; many distributed (and trusted) roadside units[2]; and human users (i.e., drivers). Initially, each user willing to be part of the VANET will register with the centralized entity (say the Bureau of Motor Vehicles). The entity will then issue each user a smart card containing a unique public-private key pair. A smart card reader will also be provisioned to each vehicle. A number of geographically distributed roadside units (RSUs) are to be deployed that will serve as cluster-heads and assist in subsequent key management issues at run-time for vehicles in their vicinity. Each RSU is trusted and connected to each other via a backbone network like the Internet. Two applications on top of this architecture are discussed below.

Application 1: Privacy, Confidentiality and Non-Repudiation in VANETs Communications: This application envisages leveraging smart cards for preserving privacy, confidentiality and non-repudiation of entities in VANETs. In the proposed scheme, each user will first authenticate himself to the smart card using a secret pin (known only to the user and recognized by the smart card). Following successful authentication, the smart card will request a session key from the nearest RSU. A single session key will then be generated and encrypted with the requesting card's public key. All user communication will then be accomplished through the smart card

[2] While a similar architecture has been proposed in [2, 4], this paper incorporates smart cards in the architecture.

and encrypted with the session key. Such an architecture naturally guarantees privacy and confidentiality of communicating parties. Furthermore, non-repudiation can be easily guaranteed if the message sent by each card is encrypted with its own private key, and appended to the message. Critical issues to address are overcome are RSU coverage of a large area, utilizing multi-hop communication to reach RSUs, perform aggregation over encrypted data, addressing limited connectivity among peers, providing location based privacy and security aware services, and finally the cost factor of the cards.

Application 2: Vehicle theft monitoring: Recently, there have been efforts on vehicular theft monitoring from the perspective of theft detection, tracking and recovery [3]. The smart card based architecture can be leveraged for this purpose. First, authentication of users while starting vehicles is straightforward if each driver's license cards are itself smart cards. This will serve as a first level authentication. In the event that driver's licenses are eventually stolen, a further mechanism is authentication via a secret pin. In the event that these two mechanisms fail, drivers whose cars are missing can send a message to nearest RSUs notifying them of a theft. The RSUs can then communicate with the smart card in order to locate its position for subsequent tracking. Critical issues to resolve are the possibility of the radio being tampered with, physical security of the reader, the trade-off between anonymity and verifiability when benign drivers are driving the vehicle, and want to be tracked by malicious entities.

References

1. http://www.101datasolutions.co.uk/wp-content/uploads/2008/07/rsa-smart-card-5200-overview-pdf.pdf

2. R. Lu, X. Lin, H. Zhu, P. Ho and X. Shen “ECPP: Efficient Conditional Privacy Preservation Protocol for Secure Vehicular Communications”, IEEE Infocom 2008.

3. H. Song, S. Zhu and G. Cao "SVATS: A Sensor-network-based Vehicle Anti-Theft System" IEEE INFOCOM mini-conference, 2008.

4. C. Lochert, B. Scheuerman, C. Wewetzer, A. Luebke and M. Mauve “Data aggregation and roadside unit placement for a vanet traffic information system”, Vanets 2008.