Journal of Network and Computer Applications 34 (2011) 1942–1955

Contents lists available at ScienceDirect

Journal of Network and Computer Applications

journal homepage: www.elsevier.com/locate/jnca

Review

Security on VANETs: Privacy, misbehaving nodes, false information and secure data aggregation

David Antolino Rivas *, José M. Barceló-Ordinas, Manel Guerrero Zapata, Julián D. Morillo-Pozo

Department of Computer Architecture, Polytechnic University of Catalonia, C. Jordi Girona 1-3, Barcelona 08034, Spain

ARTICLE INFO

Article history:
Received 27 March 2011
Received in revised form
12 June 2011
Accepted 11 July 2011
Available online 20 July 2011

Keywords:
Security
Vehicular Ad hoc Networks
VANETs
Privacy
Certificates
Pseudonyms
Anonymity
Data aggregation

ABSTRACT

This article is a position paper on the current security issues in *Vehicular Ad hoc Networks* (VANETs). VANETs face many interesting research challenges in multiple areas, from privacy and anonymity to the detection and eviction of misbehaving nodes and many others in between. Multiple solutions have been proposed to address those issues. This paper surveys the most relevant while discussing its benefits and drawbacks. The paper explores the newest trends in privacy, anonymity, misbehaving nodes, the dissemination of false information and secure data aggregation, giving a perspective on how we foresee the future of this research area.

First, the paper discusses the use of *Public Key Infrastructure* (PKI) (and certificates revocation), location privacy, anonymity and group signatures for VANETs. Then, it compares several proposals to identify and evict misbehaving and faulty nodes. Finally, the paper explores the differences between syntactic and semantic aggregation techniques, cluster and non-cluster based with fixed and dynamic based areas, while presenting secure as well as probabilistic aggregation schemes.

Contents

1. Introduction

With the massive deployment of wireless technologies on motorized vehicles, automotive industries have opened a wide variety of possibilities for drivers and their passengers. Theoretically, anything from finding out the road conditions ahead to watching a movie through streaming is possible. Different kinds of applications will need different requirements. As mentioned by Reichardt et al. (2002) and Raya and Hubaux (2005a) applications can be categorized as follows:

1. *Safety related*:
   (a) *Traffic information messages*: used to disseminate traffic conditions in a region and thus affect public safety only indirectly—they are not time-critical.

* Corresponding author.
E-mail address: antolino@ac.upc.edu (D. Antolino Rivas).

1084-8045/$ - see front matter © 2011 Elsevier Ltd. All rights reserved.
doi:10.1016/j.jnca.2011.07.006