A Survey on Secure Safety Applications in VANET

Ruqayah Al-ani*, Bo Zhou*, Qi Shi*, Ali Sagheer+
* Department of computer Science Liverpool John Moores University Liverpool, UK
+Al Qalam College, Kirkuk, Iraq
Email: R.A.Alani@2015.ljmu.ac.uk

Abstract—Providing an efficient secure authentication scheme in safety applications in Vehicular Ad-hoc Networks (VANETs) is a challenging issue. This is because these applications need to react to their messages, in a timely manner, before their respective deadlines. Preserving the privacy of the exchanged messages is also important since these messages include sensitive information, such as geographical locations. In this paper, we review the existing schemes that aim to meet the requirements of security and privacy. Then, we specify these requirements with a view to design an efficient scheme for secure real-time applications in VANET environments.

Index Terms— security, privacy preserving, VANET, safety applications

I. Introduction

Due to the increasing demands to improve traffic safety, Vehicular Ad-hoc Networks (VANETs) have attracted attention from governments, car manufactures, and researchers. In VANETs, vehicles equipped with on-board units (OBUs) are able to collect, process and exchange traffic-related messages with nearby vehicles through Vehicle-to-Vehicle (V2V) communications, or communicate with nearby road-side units (RSUs) through Vehicle-to-Roadside (V2R) communications.

Most VANET safety applications require timely reactions to the broadcasted messages. Relying on a Dedicated Short-rang communication (DSRC), instead of a cellular network communication, would reduce delays when uploading and downloading traffic-related messages. Accordingly, the IEEE 1609.2 standard mandates a DSRC system when developing VANET applications which supports both V2V and V2R

The designed scheme should achieve an acceptable balance between security and privacy requirements. Moreover, the scheme should be highly efficient in supporting applications with real-time requirements.

pseudonym-based authentication schemes are widely used in order to enable the authentication of the broadcast messages anonymously [1]. This is when aauthentication between vehicles is conducted through dummy identities, which are authenticated by the trusted authorities (TAs) in order to reveal the real identity in case of a dispute.

The unique characteristics of VANETs, such as their high mobility and their large number of nodes, would challenge the exiting security schemes. For example, most of pseudonym-based authentication schemes employ digital signatures to offer secure communication between VANET entities, which leads to processing delays of traffic-related messages.

In this paper, we highlight the security and privacy requirements of safety applications. First, some safety applications are given in subsection II.A. Then, the security, privacy requirements and their main challenges in VANET are outlined in II.B, II.C, and II.D, respectively. In section III, the well-known pseudonym schemes, along with their changing strategies, are illustrated. After this, some existing work to enhance the efficiency of the verification process is given in section III. Finally, in section IV, we discuss and conclude the main requirements to designing an efficient privacy preserving authentication scheme for VANET safety applications.

II. VANET Applications, Requirements and its