Secure Safety Messages Broadcasting in Vehicular Network

Maryam Barzegar[1,3], Nasser Mozayani[2], Mahmood Fathy[2]
[1]Technical and Engineering Faculty of Science and Research, Islamic Azad University, Tehran, Iran
[2]Department of Computer Engineering, Iran University of Science and Technology,Tehran, Iran
m.barzegar@gmail.com, mozayani@iust.ac.ir, mahfathy@iust.ac.ir

Abstract

Vehicular communications by means of exchanging safety message considerably reduces life and property damage. So securing this message is essential. In this paper, we focus on protocols based on a fixed key infrastructure that establish stronger security in comparison with dynamic structures. These protocols have some problems in terms of implementation issues. In effect, a very important issue is high mobility of vehicles over these networks and their change of region.

In this paper, we propose solutions for informing vehicles about region change to obtain new key set before entering next region. We also make key request messages secure by confirming old CA's public key to the message. At the end, a solution for compliance with broadcasting protocols is offered. For evaluation, we compare our method with other security solution based on four performance criteria.

1. Introduction

Regarding to widespread applications of wireless communication and networks in human's daily life, nearly all aspects of people's life deal with such applications. One of these applications is managing traffic and providing safety for the vehicles that complied by Vehicular Ad hoc Network (VANET). In VANET, every vehicle communicates with other vehicles (V2V) and also with roadside infrastructures (V2I) by means of communication equipment [7].

The most important usage of these networks is informing vehicles in emergency cases such as car accident, urgent breaking or traffic jam [9]. In such cases, a vehicle can inform other vehicles by means of broadcasting safety messages before facing the event.

Whereas safety Messages have a substantial role in this network, they should be sent from credible transmitter and contain proper and unaltered information. It is very important to protect vehicles from tracking but in cases of accidents and crimes, it is necessary to identify message sender as it can't repudiate it.

Most of the existing works don't comply all applicable requirements for securing safety message. Thus we first state these requirements and then select the most appropriate security protocol. At the end, we resolve its implementation challenges by proposing solutions to increase its performance in large scale usage.

In this paper, section 2 has a look at the related works about securing safety messages in VANET. Section 3 states security requirements and model. Section 4 selects a distinct protocol as our framework and tries to resolve its implementation challenges. Section 5 brings security analysis and evaluation and finally section 6 concludes the paper.

2. Related Works

Several ideas have been given for securing vehicular networks. In most of them, security is generally considered and less attention was paid to securing safety message as an implementable method in particular. In [7], [10], a routing protocol based on geographical position is used. In this protocol, each vehicle has its neighbor's positions and identity that are saved in a table. This table is exchanged periodically among vehicles. These methods comply security aspects such as authentication, data integrity and non-repudiation based on public key infrastructure (PKI), but the protocols have no concern with privacy and anonymity, so it isn't resistant against tracking attack.

In [2], [3], [6], researchers have used group signature to preserve anonymity and privacy of vehicles. In these methods, each vehicle is assigned to a group of vehicles. This preserves anonymity inside the group because secret information of nodes is only available to the group manager. Group manager is head of a group that's duties are key generation, signature generation, member registration, member verification, member

[3] This research is supported by Iran Telecommunication Research Center (ITRC).

978-0-7695-3639-2/09 $25.00 © 2009 IEEE
DOI 10.1109/WAINA.2009.34