Wireless Networks for Vehicular Support

Pietro Manzoni
Technical University of Valencia, Spain

Carlos T. Calafate
Technical University of Valencia, Spain

Juan-Carlos Cano
Technical University of Valencia, Spain

Antonio Skarmeta
University of Murcia, Spain

Vittoria Gianuzzi
University of Genova, Italy

INTRODUCTION

Vehicular Ad hoc NETworks (VANETs) is an area under intensive research that promises to improve security on the road by developing an intelligent transport system (ITS). The main purpose is to create an inter-communication network among vehicles, as well as between vehicles and the supporting infrastructure. The system pretends to offer drivers data concerning other nearby vehicles, especially those within sight.

The problem of information sharing among vehicles and between the vehicle and the infrastructure is another critical aspect. A general communication infrastructure is required for the notification, storage, management, and provision of context-aware information about user travel. Ideally an integrated vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication paradigm enriched with an information management system would solve the problem. The infrastructure should manage all the collected safety events garnered from vehicles and the interesting information to be provided to the user, which is adapted to the car context and driver preferences.

Finally, security issues should be considered. Since the information conveyed over a vehicular network may affect critical decisions, fail-safe security is a necessity. The first directive for any V2V communication scheme is, therefore, that every safety message must be authenticated. Because of the high speed and therefore short duration within which communication between two cars is possible, communication must be non-interactive, and message overhead must be very low. The urgency of safety messages implies that authentication must be instantaneous without additional communication.

Moreover, providing strong security in vehicular networks raises important privacy concerns that must also be considered. Safety messages include data that is dangerous to the personal privacy of vehicle owners. Most relevant is the danger of tracking a vehicle through positional information. A set of security basics to address these challenges should be proposed that can be used as the building blocks of secure applications.

In this article we will focus on the aforementioned technologies and engineering issues related to vehicular ad-hoc networks, emphasizing the challenges that must be overcome to accomplish the desired vehicular safety infrastructure.

BACKGROUND

Ubiquitous computing is nowadays an emerging research field in mobile communications, due to more and more integration of heterogeneous services over different operation environments. The capacity of customizing services to the client, and the adaptation of its behavior according to the context, will offer the user value-added features in the new age of computer communications. Taking into account this premise, in this article our aim is to create a feasible environment for providing integrated services in the vehicle field.

Wireless communications in the vehicle field through ad hoc networks (or Vehicular Ad hoc NETworks–VANETs) are currently being used as a novel and promising technology to improve driving safety. Mainstream research usually considers these communication patterns to offer intelligent transportation systems (ITSs), where one of the most important aims is the creation of communication networks among vehicles, in vehicle-to-vehicle transmissions (V2V),

but without forgetting communications between vehicle and infrastructure (V2I). The usefulness of these developments is focused on providing every vehicle with information about the surrounding vehicles, and especially the ones not located in the field of vision.

Due to the continuous improvements of communication technologies, a great number of considerations must be taken into account when a network system is elected. Although VANET developments have predominated in V2V communications, it is necessary to study whether the facilities offered by the network design cover the requirements collected from the future deployable services. Collision avoidance applications have been the main safety service implemented for the vehicle field. However, a great number of non-safety services are appearing. When the amount of services for the vehicle side grows, more consideration is needed. It is mandatory to research in technological solutions which deal with the requirements of a generic and flexible architecture for service provisioning and usage.

For a correct design of such systems, it is necessary to take into account the vehicular environment. Here, high-speed mobility and special movement patterns can be found, where the creation and breakage of links between nodes appear continuously. The presence of an excessive or null rate of equipped vehicles is another important factor which must be considered. This fact and the need for reliable end-to-end communication make the design of a vehicular communication system a complex task.

The main objective of any project in this area is to offer an integrated solution for the deployment of an ITS using the VANET communication technology overall. The schema considered can be seen in Figure 1. The system should apply techniques inside the field of ubiquitous computing in the vehicle field, where numerous programmatic devices can interact with the user in a transparent way. This way, the system should have enough intelligence to analyze the context and efficiently detect hazardous and emergency situations, generate driver warnings in critical cases, and interact with the infrastructure when a global knowledge can be useful.

A CROSS-LAYER APPROACH TO VANET DESIGN

The design of a complete VANET solution must cover different technological areas, and several disciplines are involved in the development of such a system. In the following we will outline all the interrelated layers that must work together to provide a comprehensive architecture.

Modeling, Evaluation, and Simulation

In classical MANETs, researchers often use a typical set of simulation parameters. These parameters are inadequate for

Figure 1. Overall scheme of the proposed architecture