Chapter 6
Medium Access Protocols for Cooperative Collision Avoidance in Vehicular Ad-Hoc Networks

Md. Imrul Hassan
Swinburne University of Technology, Australia

Hai L. Vu
Swinburne University of Technology, Australia

Taka Sakurai
University of Melbourne, Australia

ABSTRACT

It is envisaged that supporting vehicle-to-vehicle and vehicle-to-infrastructure communications with a Vehicular Ad-Hoc Network (VANET) can improve road safety and increase transportation efficiency. Among the candidate applications of VANETs, cooperative collision avoidance (CCA) has attracted considerable interest as it can significantly improve road safety. Due to the ad hoc nature of these highly dynamic networks, no central coordination or handshaking protocol can be assumed and safety applications must broadcast information of interest to many surrounding cars by sharing a single channel in a distributed manner. This gives rise to one of the key challenges in vehicle-to-vehicle communication systems, namely, the development of an efficient and reliable medium access control (MAC) protocol for CCA. In this chapter, we provide an overview of proposed MAC protocols for VANETs and describe current standardization activities. We then focus on the performance of the IEEE 802.11 carrier sense multiple access (CSMA) based MAC protocol that is being standardized by the IEEE standards body for VANET applications. In particular, we review prominent existing analytical models and study their advantages, disadvantages and their suitability for performance evaluation of the MAC protocol for VANETs. After a discussion of the shortcomings of these models, we develop a new analytical model in the second half of the chapter. Explicit expressions are derived for the mean and standard deviation of the packet delay, as well as for the packet delivery ratio (PDR) at the MAC layer in an unsaturated network formed by moving vehicles on a highway. We validate the analytical results using extensive

DOI: 10.4018/978-1-61520-913-2.ch006
INTRODUCTION

A Vehicular Ad-Hoc Network (VANET) supports vehicle-to-vehicle and vehicle-to-infrastructure communications and covers a wide range of applications based on smart information use to improve road safety and to increase transportation efficiency. Among the candidate applications, cooperative collision avoidance (CCA) has attracted considerable interest in the research community as it can significantly improve road safety. In CCA, moving cars form a network to wirelessly communicate and warn each other of changing conditions or dangers ahead on the road to avoid accidents.

While the aims of a VANET system are to both enhance road safety and to improve transportation efficiency, in this chapter, we only focus on the safety applications such as CCA. Road safety is supported by the transmission of routine status messages and event-driven emergency messages. Routine status messages are sent periodically to neighbouring vehicles to inform them of the current status of the originating vehicle (e.g., location speed, direction), whereby the receiving vehicles/drivers can then anticipate any potential hazards (e.g., traffic jam ahead) and take necessary action. Event-driven safety messages are triggered by rapid changes in vehicle behaviour such as a hard brake or an airbag explosion. To enable preventative action, it is essential that both types of safety messages are received correctly by surrounding vehicles in a timely fashion.

The likelihood of a rapidly changing VANET topology makes it difficult to rely on centrally coordinated communications. Therefore, decentralized broadcast is the natural choice of communication mode for safety messages in a VANET. The broadcast could use multi-hop transmissions to enhance coverage, but recent studies suggest that a single-hop transmission is sufficient in most situations to reach all neighbouring vehicles in an accident’s vicinity (Hartenstein & Laberteaux, 2008).

Ensuring reliable and timely packet delivery using decentralized broadcast is essential for CCA. For instance, according to (Biswas, Tatchikou, & Dion, 2006) the packet delay must be less than 400 ms in order to avoid chain collisions. Also, the VANET standard developed by the American Society for Testing and Materials (ASTM) (ASTM, 2003), requires that the communication devices should be capable of transferring safety messages with more than 90% reliability. One of the main difficulties to achieve those requirements is the loss of packets due to the presence of hidden terminals (Chen, Refai, & Ma, 2007). This occurs when a node is transmitting to a target node while a third node that is unaware of the transmitting node also starts its transmission and causes interference at the receiver. The hidden terminal problem can afflict all decentralized wireless networks, but is particularly severe in broadcast scenarios. In the broadcast case, there are multiple receivers for each message, scattered in the transmission range of the sender. Any node that is within sensing range of any receiver but outside the transmission range of the sender is a potential hidden terminal. Therefore, the potential hidden terminal region is significantly larger than that for unicast communication.

The distinctive demands of VANET applications, as well as the unique operating environment involving fast moving vehicles, mean that specifically tailored communication protocols are required for VANET systems. Particularly, the simulations and show that good accuracy can be achieved with the proposed model for a range of topologies and traffic load conditions. More importantly, using the model, we show that hidden terminals can have a severe, detrimental impact on the PDR, which may compromise the reliability required for safety applications.
Related Content

Analysis of the US Privacy Model: Implications of the GDPR in the US
Francisco García Martínez (2019). International Journal of Hyperconnectivity and the Internet of Things (pp. 43-52).
www.igi-global.com/article/analysis-of-the-us-privacy-model/234344?camid=4v1a

A Security Framework for Enhancing User Experience
www.igi-global.com/article/a-security-framework-for-enhancing-user-experience/179895?camid=4v1a

Disrupting the U.S. National Security Through Financial Cybercrimes
Calvin Nobles (2019). International Journal of Hyperconnectivity and the Internet of Things (pp. 1-21).
www.igi-global.com/article/disrupting-the-us-national-security-through-financial-cybercrimes/234342?camid=4v1a

A Systematic Exploration on Challenges and Limitations in Middleware Programming for IoT Technology
www.igi-global.com/article/a-systematic-exploration-on-challenges-and-limitations-in-middleware-programming-for-iot-technology/221331?camid=4v1a