Vehicular Communications 2 (2015) 223–237

Contents lists available at ScienceDirect

Vehicular Communications

www.elsevier.com/locate/vehcom

Medium access control protocols for safety applications in Vehicular Ad-Hoc Network: A classification and comprehensive survey

Nishu Gupta *, Arun Prakash, Rajeev Tripathi

Department of Electronics and Communication Engineering, Motilal Nehru National Institute of Technology Allahabad, India

ARTICLE INFO

Article history:
Received 20 May 2015
Received in revised form 11 October 2015
Accepted 13 October 2015
Available online 19 October 2015

Keywords:
DSRC
MAC
IEEE 802.11p
Safety
VANET

ABSTRACT

Vehicular Ad-Hoc Network (VANET) is seen as an emerging solution to improve road safety, highway assistance and traveler comfort accounting to vivid applications including safety, non-safety and infotainment applications. Over the past few years, research paradigm has shifted towards areas such as multi-hop broadcasting, information security, clustering, etc. covering intra-vehicular and vehicle-to-infrastructure communication modes. Whereas these scenarios provide diversified information dissemination techniques through various applications of Intelligent Transportation Systems (ITS), data dissemination in VANET environment is still a challenging task, mainly due to rapid changes in network topology and frequent disruptions in connectivity. A distinguished area that still lacks significant research contributions is towards designing reliable and efficient Medium Access Control (MAC) protocols for vehicular communication in order to enhance travel safety. The main motivation behind such a survey is to integrate a wide range of research contributions that have been recently proposed to envisage the inherent characteristics of vehicular communication. Such a study serves as a reference for an in-depth research towards enhancements in the PHY/MAC layers. In this paper, we present state-of-the-art survey of the MAC protocols available for vehicular safety. We classify these protocols based on different applications and the techniques they adopt. We also review the performance metrics used for evaluating these protocols. In later sections, we qualitatively analyze the protocols based on different parameters along with related issues and the challenges they generate. We highlight the mechanisms involved, conceptual features, optimization techniques, strength and drawbacks of the available protocols as well as their applicability in future deployment. Finally, we discuss the open issues and future research directions.

1. Introduction

Vehicular Ad-Hoc Network (VANET) is a sub-class of Mobile Ad-Hoc Network (MANET) and a component of Intelligent Transportation Systems (ITS) that provides communication among nearby vehicles and roadside infrastructure. This type of network uses vehicles as mobile nodes that belong to a self-organizing network without prior screening or knowledge of each other's presence [1]. The network turns every participating vehicle into a wireless router or node, allowing vehicles in a distance of approximately 100 to 300 m from each other in urban scenario to connect and create a network with a wide range. This range extends to around 1000 m in highway scenario. Nodes may intermittently fall out of the signal range and can join in, thereby dynamically establishing connections between the vehicles such that an internetwork is created.

Some of its unique characteristics like geographically constrained topology, predictable mobility and vehicle density, varying channel capacity, etc. constitute VANET as a distinct research field in MANET [2]. These characteristics pose several challenges with respect to medium access, physical communication, coding, routing, congestion control, fault tolerance, multi-modal interactions, end-to-end data transport, security, privacy, simulation and implementation platforms, safety and non-safety information management, Quality of Service (QoS) assurance, infotainment applications, etc. [3].

As a requisite while developing safety-aware Medium Access Control (MAC) protocols, a justified balance need to be assured between protocol complexities, supported metrics, relative node mobility, channel reservation methods, available traffic classes, signaling overheads, fairness, efficient channel utilization, consumed energy and many more attributes. In this context, the present survey explores that there has been limited discussion on the urge to

* Corresponding author.
E-mail addresses: rel0513@mnnit.ac.in (N. Gupta), arun@mnnit.ac.in (A. Prakash), rt@mnnit.ac.in (R. Tripathi).

http://dx.doi.org/10.1016/j.vehcom.2015.10.001
2214-2096/

have real-time requirements and to what extent is the MAC protocol able to meet these requirements. If the MAC protocol does not provide an upper bound on the maximum delay before providing access to the channel, it would not be possible to disseminate real-time data with optimum reliability.

To the best of our knowledge, the present survey is the first to explore MAC protocols for safety applications, applicable to both, IEEE 1609.4 and IEEE 802.11p, standards in an integrated fashion. In this paper, we present a comprehensive analysis of the MAC protocols designed for safety applications in vehicular ad-hoc network.

The rest of the paper is organized as follows. Section 2 provides the background of the MAC architecture employed in the underlying standard. It also discusses the IEEE 802.11p MAC architecture and safety applications of VANET. Section 3 highlights the challenges and role of MAC protocols in VANET. Section 4 constitutes the related works and comparative analysis of existing safety applications based MAC protocols. Section 5 presents review of performance metrics used for evaluating MAC protocols for safety applications along with a detailed qualitative analysis of safety based MAC protocols. Section 6 discusses the open issues and future research directions. Finally, Section 7 summarizes the paper with concluding remarks.

2. Background

The IEEE 1609 working group has collectively defined the stack of IEEE 802.11p/1609.x protocol families as Wireless Access in Vehicular Environment (WAVE). WAVE has its origins in the standardization of Dedicated Short Range Communications (DSRC) as a radio technology. It is a part of a group of standards related to all the layers of protocols designed for DSRC-based operations. The IEEE 1609.4 standard [4] is a MAC extension of the IEEE 802.11p to support multichannel operations. It describes wireless multichannel radio operations which use the IEEE 802.11p protocol (MAC and PHY) for WAVE architecture. It specifies priority access categories (ACs), Synchronization Interval (SI), Control Channel (CCH) and Service Channel (SCH) operations. Moreover, it defines management services, channel routing and switching parameters as well. The IEEE 802.11p is the currently proposed standard for MAC in VANET. Draft 3.3 is the most recent version of this standard [5]. However, the standard is not known to provide an efficient one-hop broadcast service. The IEEE 802.11p MAC does not adequately address the requirements imposed by VANET applications, since it uses a standard contention-based MAC approach. QoS cannot be guaranteed for safety critical messages and other real-time transmissions [6]. Moreover, it is known that the medium access technique employed in IEEE 802.11p, Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA), is unsuitable for critical communication scenarios. There are a lot of challenges ahead which need to be addressed by existing protocols and by proposing new solutions that would optimize the performance of vehicular communication in terms of several classical metrics. Notably, DSRC, WAVE and IEEE 802.11p are used interchangeably to delegate the entire protocol stack of standards dealing with VANET.

2.1. IEEE 802.11p MAC architecture

MAC layer is considered as the key layer in the communication protocol stack of any networking environment. It is this layer that determines which node is to be given access to the medium. MAC mechanisms can be categorized as contention-based and contention-free. Contention-based approaches rely on carrier sensing, back-offs and retry schemes, whereas contention-free approaches rely on time division multiple access and synchronization schemes [6]. The IEEE 802.11p standard defines the PHY and MAC layers based on earlier standards for wireless LAN with some modifications. The MAC protocol in IEEE 802.11p is CSMA/CA where each node starts by listening to the wireless channel and transmits only if the channel is sensed free. However, CSMA/CA is known to have problems with predictability and fairness, especially when periodic positioning messages are used. For a distributed network scenario, this protocol can be easily deployed but suffers from one disadvantage; the nodes experience unbounded delays due to constantly sensing a busy channel during high utilization periods. This is nearly unacceptable in real-time scenarios such as safety applications. Real-time systems urge for a proactive MAC protocol in which the upper bound of the channel access delay is deterministic. Unlike its preceding standard, IEEE 802.11p does not incorporate authentication and association schemes in the MAC and PHY layers. The normal modes of authentication and association would not be able to meet the stringent timing requirements set by the VANET environment. To list a few, limited transmission power, limited bandwidth, attenuations, high mobility, frequent disconnections and anonymity of the infrastructural support are some of these requirements.

VANET presents a challenging environment for protocol and application design due to their low latency and high throughput requirements in a high mobility environment. It employs the mechanism originally provided for IEEE 802.11a to operate in the DSRC band to support Inter-Vehicular Communication (IVC) and ITS applications. DSRC is considered to provide communication architecture for nodes. It can be in Vehicle to Vehicle (V2V) mode to communicate with each other and in Vehicle to Infrastructure (V2I) mode to communicate with the Road Side Units (RSU) [7]. Whereas the use of DSRC band is not subject to any license, but certain channelization mechanisms have been predefined towards its strict and effective utilization. The 75 MHz DSRC band (5850 to 5925 MHz) is divided into seven channels of 10 MHz numbered as 172, 174, 176, 178, 180, 182 and 184 as depicted in Fig. 1. Channel number 178 is the CCH. It is this channel that look after the overall coordination between all the channels along with providing access to critical safety applications. The other six channels are SCH. SCH number 172 is reserved for High Availability and Low Latency (HALL). Channel 184 is reserved for public safety intersections. Both of these channels (172 and 184) are specifically dedicated to public safety. Channels 174 and 176 provide medium range service applications for shared public safety/private usage. SCH 180 and 182 render short range services for shared public safety/private usage.

IEEE 802.11p employs contention-based channel access as MAC method, known as Enhanced Distributed Channel Access (EDCA) MAC sub-layer protocol design based on IEEE 802.11e standard with some modifications, which is an enhanced version of the basic Distributed Coordination Function (DCF) from IEEE 802.11. The working mechanism behind this protocol is that a node willing to transmit will sense the medium first, and if it is free for Arbitration Inter-frame Space (AIFS) duration, the node shall defer the transmission by selecting a random backoff time. Lower is the backoff time, higher is the priority assigned to the node. In order to ensure more chance to safety messages so they can be transmitted within a reasonable time even when operating in a dense scenario, EDCA introduces the management of QoS concept through the notion of (ACs). There are four ACs with different priorities defined by IEEE 802.11p. They are Background traffic (BK or AC0), Best Effort traffic (BE or AC1), Video traffic (VI or AC2) and Voice traffic (VO or AC3). Voice traffic is given the highest priority. Different Arbitration Inter-Frame Space Number (AIFSN) and Contention Window (CW) values are selected for different types of ACs in the CCH and SCH interval. Table 1 shows different contention parameters used on the CCH and SCH intervals of IEEE 802.11p for different ACs