Requirements and Challenges Associated with Deployment of Connected Vehicles

Md. Ahsanul Islam
Graduate Research Assistant, Department of Civil, Construction and Environmental Engineering, The University of Alabama at Birmingham

Abstract: Connected vehicles are the latest innovation in the era of road transportation systems. Connected vehicles use a number of different communication technologies like vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I) and sensors to communicate with each other. Such technologies allow information exchange, cooperative localization and map updating, as well as facilitate cooperative maneuvers between vehicles within a short range of each other. The major benefit of vehicle connectivity is that information can be shared in an efficient and reliable manner and can be used to support drivers’ decision-making process. This, in turn, can improve traffic safety, operational efficiency, road utilization, and user satisfaction. Moreover, connected vehicles can increase accessibility and mobility for those less mobile or those unable to use traditional vehicles, such as the elderly or disabled. In addition to the remarkable safety potential of connected vehicles, connected vehicle technology has the potential to transform the transportation industry into the automotive industry. However, several challenges appear when dealing connected vehicles due to the diverse and dynamic features of such system. This paper provides a comprehensive review of the relevant literature and explores requirements and possible challenges associated with the deployment of connected vehicles.

Keywords: Connected vehicles, requirements, challenges

1. Introduction and Motivation

Connected vehicle technology is modernizing current transportation systems and it can play a vital role in modern intelligent transportation systems to provide safety, mobility, and environmental preservation. It is an indispensable part of intelligent transportation systems (ITS). The term “Connected vehicle” refers to the technologies that can ensure communication between contributing stakeholders or agents comprising authorities and vehicles, pedestrians, as well as infrastructure.

Currently, wireless connectivity to vehicles is expected to be the next leading edge of automobile industry due to the rapid development of information and communication technologies (ICT). Connected vehicles are proactive, well cooperative and coordinated and can provide a 360-degree awareness that informs a driver of hazards and situations they cannot see as well as reduce or eliminate crashes through a combination of driver advisories, driver warnings, and vehicle controls. For example, the intersection movement assist application warns drivers when it's unsafe to enter an intersection. The Do Not Pass application warns drivers when it is not safe to pass a slower moving vehicle. The Emergency Electronic Brake Light application notifies the driver when an out of sight vehicle several cars ahead is breaking. In addition, according to a business report, global market of connected vehicles is increasing at a compound annual growth rate (CAGR) of 34.7% from 2013 to 2019 and it is expected to reach USD 131.9 billion by 2019 [1].

There are two main contributing factors of bringing wireless connectivity to vehicles. First and foremost to improve safety and efficiency of the existing road transportation systems. According to the statistics for road accidents in the United States in 2010: 32999 people killed, 3.9 million injured, 24 million vehicles damaged and the consequences in terms of huge economic cost $242 billion [2]. This cost has negative impact on productivity, legal and court costs, workplace losses, property damage, insurance administration costs, congestion burden, emergency service costs, medical costs. However, a downward trend found in the number of crashes in the United states due to the adaption of new technology features such as forward collision warnings, electronic stability control [3] that will be adopted in connected vehicle technology. The second one is the demand of collection of real time data that is transmitted through the basic safety messages (BSM) using Dedicated Short Range Communication (DSRC) technology. The BSM alerts drivers to avoid crashes or back-ups, vehicles equipped with DSRC could broadcast information such as their location, speeds, and direction of travel and infrastructure equipped with DSRC could broadcast data including signal phase and timing (SPaT), speed warnings (drive 35 mph), and the number of available parking spaces. Hence, connected vehicles considered as an emerging technology that has the potential to gather, share, process, compute, and secure release of information to next generation intelligent transportation systems (ITSs). In addition, connected vehicles can even help us to reduce carbon footprint.
and facilitate green transportation choices. However, the development and deployment of fully connected vehicles requires a combination of emerging technologies, and some uncertainty remains of each technology as well as institutional and other deployment issues. This study aims to explore the requirements and potential challenges of the Connected Vehicle technology in real-world settings.

2. Literature review
At present, connected vehicles are a topic of huge interest both internationally and in the US as cities and transportation agencies trying to understand the future of the transportation systems when these vehicles are widely available. Much focus has been on the requirements and challenges associated with the deployment of connected vehicles. In this chapter, an extensive discussion of those findings is presented.

2.1. Requirements for deployment of connected vehicles
Several studies in the past indicated some requirements for deployment of connected vehicles. In this section, an extensive discussion of past findings is presented under the following subsections: infostructure elements, sensors and other in-vehicle technologies, standards, institutional roles and responsibilities and security of network.

2.1.1. Infostructure elements
The term “infostructure elements” refers to the physical communications infrastructure or leased communications services, which would facilitate a connected vehicle deployment. Main elements of the infostructure elements of connected vehicle system architecture are as follows: (i) DSRC roadside equipment, (ii) backhaul communications network, (iii) advanced signal controllers, (iv) credential management, (v) data management systems

DSRC roadside equipment
The roadside equipment is a critical element in the connected vehicle network for vehicle-to-infrastructure communications because it is the primary component that sends and receives data from multiple devices within the connected vehicle architecture. The roadside equipment including DSRC is a two-way short- to medium-range wireless communications that permits very high data transmission critical in communications based active safety applications [4]. DSRC functions at 5.9 GHz in a spectrum band to support vehicle-to-vehicle and vehicle-to-infrastructure services. It is uniquely suited to safety applications that require a fast (low latency) and secure wireless connection. Data is transmitted 10 times a second, up to 300 meters in the line of sight [5]. Privacy is protected, and the vehicle will never be recorded or tracked. The full set of vehicle data available through the basic safety message (BSM) includes brake status, turn signal status, vehicle length, vehicle width, and bumper height, as well as time, heading angle, lateral acceleration, longitudinal acceleration, yaw rate, throttle position, steering angle, headlight status, wiper status, external temperature, and vehicle mass. DSRC is the only viable option and the only wireless communication technology that meets the requirements for safety-critical applications. Multiple vendors are developing interoperable infrastructure equipment; however, there are just five vendors of connected vehicle roadside equipment currently on the list. The devices on the RQPL are based on Roadside Equipment (RSE) Specification v3.0. Roadside Unit (RSU) Specification v4.0 is now available.

Backhaul Communications Network
To deploy connected vehicles in the real world settings, various types of backhaul communications network such as fiber optics, wireless communications, and leased communications are required that are discussed below:

Fiber optics
Fiber optic is a preferred communication method in the deployment of connected vehicles program because it can carry strong signal over a long distance with great quality transmission. Moreover, compare to copper and coaxial cable, fiber cable is susceptible to breaking and it provides a higher data throughput [4].

Wireless communications
Fast, secure, and reliable wireless communications are required to maximize the benefits of connected vehicles. Different types of wireless technology are available. For instance, bluetooth is a short-range wireless communication technology based on the IEEE 802.15.1 standard, which allows communicating between portable devices at a data-transferring rate up to 3Mb/s [6]. Additionally, microwave radio technology is the backbone of a wireless communication technology, which transmits digital signals between locations to location. The basic components required for operating a radio link are the transmitter, towers/poles, antennas, and receiver and these components should be installed at every DSRC equipment location for transmission of the vehicle data to the back-end system. In addition to it, wireless connectivity based on infrastructure is inherently low cost, and offers more flexibility.

Leased communications
Leased communication technology such as cellular, cable, or dedicated communications link, which is required to help connected vehicle technology
deployment at every DSRC equipment location. This backbone technology provides a high degree of flexibility for locations that are not accessible by fiber optics and licensed or unlicensed wireless radios [4]. At present, current cellular technology like 3rd Generation (3G) and 4th Generation (4G) can provide medium to high network reliability and adequate speeds for connected vehicle applications. Instead of it, cable services also provide reliable connection on to the internet for backhaul communications network.

**Advanced Signal Controllers**

Advanced signal controllers are another critical element in the connected vehicle network by transmitting signal phase and timing (SPaT) data to vehicles for safety and mobility applications. Signal phase and timing (SPaT) information includes the signal phase i.e. green, amber, or red which can be used in applications to help increase safety, mobility, and fuel efficiency for all road users. In addition, the use of advanced vehicle technology will enable future integration of a connected vehicle system. Moreover, the implementation of National Transportation Communications for ITS Protocol (NTCIP) based communications at the traffic signal controller achieves greater ability for interoperability of the traffic signal data to be integrated with back-end systems and Advanced Traffic Management System (ATMS) software suites [4].

**Credential management**

Credential management is required to provide a secure exchange of trusted data between users and applications without a pre-existing relationship and without entering into a permanent relationship. This approach provides assurance of privacy between users and from third parties, and more efficient data collection from various sources and distribution to many users. For this reason, connected vehicles system must have a security and credential management system to communicate successfully with a Security Certificate Management System (SCMS) or by using the SCMS emulator. This ensures that the system can obtain properly formatted certificates.

**Data management systems**

The goal of data management systems is to collect real-time multimodal data from multiple sources for transportation management and performance measurement [7]. Moreover, there is an opportunity to comprise the data either centralized or regional due to application requirements and availability of connection between regions, data management systems must be included with the consideration of equipment, architecture and applications [4]. For example, one set of data can have many applications. Probe data (data generated by vehicles about their current position, motion, and time stamp) has several applications that can provide support for many aspects of travel including transportation operations, traveler information, transportation planning, and asset management.

### 2.1.2. Sensors and other in-vehicle technologies

Sensors are also important components of connected vehicle technologies. It is used to detect drowsiness of driver, identify tire pressure and water temperature in the cooling system. Moreover, due to stationary characteristic of sensors, network topology does not change over time.

Other in-vehicle technologies like Ultra-wideband (UWB) refers to radio technology that can provide short-range communications within high bandwidth (3.1-10.6 GHz frequency band) at a very low energy level. UWB system has many advantages, such as low cost, high time domain resolution suitable for localization and tracking applications, low processing complexity, and resistance to severe wireless channel fading and shadowing [23]. In addition, Radio-Frequency Identification (RFID), ZigBee and 60 GHz Millimeter Wave are also required in connected vehicle deployment program.

### 2.1.3. Standards

Standards such as communications standards for DSRC and other media, such as 4G LTE and/or HD radio is also another important factor in connected vehicle deployment program. Interface standards are essential. Interfaces must be standardized to provide interoperability in four different areas i.e. between vehicles; between vehicles, roadside, and handheld devices; between roadside equipment; and between roadside equipment and management centers. For example, IEEE 802.11 [11] [Thomas Gruber] standards for wireless vehicular communications and ISO 27000 [12] standards for information security management that have been proposed over the years, need to follow in the deployment of connected vehicles.

### 2.1.4. Institutional roles and responsibilities

Institutional roles and responsibilities are classified into different categories that are mentioned below:

**US Department of Transportation (USDOT)**

The Department of Transportation must take a leadership role in establishing requirements and standards for roadside equipment, evaluating effectiveness of driver action to connected vehicle (CV) technologies. In addition, in case of a national deployment scenario, the Department of Transportation has some responsibilities like establishing safety guidelines for in-vehicle alerts and guidelines or requirements for state and local agencies to develop secure roadside infrastructure including DSRC radios and advanced signal...
controllers, and developing a national security system which enables credentialing of both vehicles and roadside devices [4].

Local transportation and transit agencies
Local agencies must consider their role in leading connected vehicle (CV) technology development from an operational perspective to take the right technical and strategic view across their organization [8]. Moreover, it is expected that the main task of local agencies are deploying, operating and maintaining of roadside equipment and communications under their jurisdiction [4]. In addition, transit agencies should try to maximize the potential use of connected vehicle (CV) technology at an early stage. They have roles in a connected vehicle deployment such as adding vehicle-to-vehicle (V2V) and vehicle to infrastructure communications to replace existing systems, and initially retrofitting of their fleets with On Board Equipment (OBE) during deployment [4].

Application developers
Several roles can be done by application developers in a connected vehicle deployment program such as development of data processing and management applications for both public agencies and OEMs, and also safety and commercialized applications for mobility, entertainment for connected vehicle network.

2.1.5. Security of network
Security of network is a high-visibility issue, as connected vehicle systems such as DSRC based system requires a separate security network. The role of the security network is to create a “trusted environment” where vehicles from one manufacturer can trust DSRC messages received from another manufacturer’s vehicle. Moreover, a system of verifying the legitimacy of messages is necessary to prevent many false warnings to a driver because bad messages can come from not only malfunctioning devices but also from malicious attacks.

2.2. Challenges for deployment of connected vehicles
While the benefits of the connected vehicle are influential and obvious to consumers and to forward-looking transportation agencies and automakers, the path toward deployment of connected vehicle does pose significant challenges.

2.2.1. Cyber security
This is the most vital challenge in the connected vehicle deployment. Due to dramatic advances in cybercrime technology and techniques, data may be breached from connected vehicle infrastructure [9]. In connected vehicle technology, another major threat is the inoculation of false messages that could cause inappropriate reactions to drivers. Hence, the detection of malfunctioning systems requires not only a software update of the on-board unit (OBU) but also a key change in the current standardized security architecture like European Telecommunications Standards Institute (ETSI) or the American National Standards Institute’s (ANSI) reference architecture [10]. For instance, according to Schoitsch et al. [11] “ISO 26262 Road Vehicles-Functional safety” can be integrated for combined security and safety standard [12].

2.2.2. Privacy
An arising challenge in the connected vehicle deployment program is to ensure privacy. Connected and cooperative transportation systems generate and exchange huge amount of data. Handling this big data, may cause breach a user’s privacy due to eavesdropping on the communication or unauthorized access to stored data [14]. For this reason, anonymous communication is an ideal solution for privacy. In addition, position and movement data ought to be transformed at minimum to limit location following and identification.

2.2.3. Connected system of systems
Vehicles in the past were stand-alone units, occasionally interacting with other road users in their direct vicinities. The connectivity transforms transportation into a system of systems, in which vehicles are connected internally (e.g. steering, sensor, actuator, and communications) and with other road users and the infrastructure systems. Connected vehicles rely on seamless data exchange and information flow. The implication of connectivity is beyond vehicles themselves. The increased connectivity and interaction gives rise to new hazards. Hazards and their causes, faults and vulnerabilities are no longer restricted within a single vehicle. Due to connectivity, vulnerabilities and faults from a single vehicle can propagate further, leading to hazards affecting multiple vehicles at once. An attacker might exploit vulnerabilities or tamper data, causing hazards on a multi-vehicle level. The goals of the attacks encompass Bluetooth connection for consumer devices, long variety connection over cellular networks for Telematics, and in-vehicle WiFi access point [14].
Experimental analysis [15], [16] and [17] proven that open car structures have expanded assault floor, allowing misuse and manipulation of in-car systems. Additionally, due to the excessive dynamics of network topology and limited variety of V2V communication, more common network partitioning can occur, resulting in data flow disconnections. The change of the infrastructure from a passive system to an active system makes it susceptible to security threats which leads to safety hazards. Security is
critical to defend the in-vehicle network and protect system from malicious attacks [18].

The intra-automobile communication surroundings are harsh due to extreme scattering in a totally restrained area and regularly none-line-of-sight that is the predominant reason for substantial effort to characterize the intra-automobile wireless channels [19], [20]. In city situations, the line-of-sight (LOS) route of V2V communication is often blocked with the aid of buildings at intersections. While on a highway, the trucks on a communication track may additionally introduce remarkable signal attenuation and packet loss [21]. Assessments of field in [22] show that multipath fading, shadowing, and Doppler effects because of excessive car mobility and the complex city surroundings will result in extreme WiFi loss, and with a massive scale of motors transmitting concurrently, the mutual interference plays vital role as well. Moreover, data transmissions require low latency and excessive reliability to satisfy the stringent requirement of real-time intra-vehicle manage system. Since connected vehicles form a connected system of systems, safety and security must be ensured at the sub-system level as well as the systems combined.

2.2.4. Uncertainty of cost effectiveness

Cellular-based access technologies play an important role in providing trustworthy web access to vehicles. However, cellular networks can be congested by the production of huge amount of mobile data traffic. For that reason, cellular infrastructures are not capable to support a huge number of connected vehicles [23]. According to AASHTO, “site development costs for Dedicated Short Range Communication (DSRC) and Road Site Equipment (RSE) - $17 – 18K, backhaul costs - $4 – 40K, operation and maintenance costs - $2 – 3K per year”. Hence, there remains great ambiguity to the cost effectiveness in deploying these technologies in the real-world settings.

3. Conclusion

Connected vehicles provide a way for travelers to engage the transportation experience in new ways and offer significant improvements to roadway operations, and prefer safety. Connected vehicles, whether cell or DSRC-based, are also a powerful tool for public agencies because they can generate new data and large quantities of data. They can enable information flow between vehicles and infrastructure and with travelers. The National Highway Traffic Safety Administration estimates that the widespread use of connected or autonomous vehicles could “eliminate 90% of all auto accidents in the United States, prevent up to US$190 billion in damages and health-costs annually and save thousands of lives”. So, connected vehicle technology has the potential to address major problems impacting the US transportation system and revolutionize mobility in the future. Moreover, numerous analysis and development efforts are needed to deal with the subsequent problems.

a. A unique solution of wireless technology is required to provide vehicle-to-vehicle and vehicle to infrastructure with cost effective vehicular networks.

b. According to [7], most past studies have focused on vehicle-to-vehicle safety applications and less on mobility and environmental improvements. Therefore, more attention is required to develop the traffic system impacts as a whole.

c. Connected vehicles provide a lot of information to the drivers that increase the load on driver. A study on driver workload limit [24] showed that driver could not control vehicle safely due to excessive information. Therefore, appropriate design of vehicle information systems are needed to overcome this problem.

d. Strong concerns about privacy and clear guidelines about institutional issues are also required to support connected vehicle deployment program.

References:


[7] Zeng, X., K.N. Balke, and P. Songchitruksa, Potential connected vehicle applications to enhance mobility, safety, and environmental security. 2012, Southwest Region University Transportation Center, Texas Transportation Institute, Texas A & M University System.


