THE CONNECTED CAR: A GLIMPSE INTO THE FUTURE OF TRANSPORTATION

Dakota L. D. Nicley, Ball State University, dlnicley@bsu.edu
Edward J. Lazaros, Ball State University, ejlazaros@bsu.edu
Allen D. Truell, Ball State University, atruell@bsu.edu
Jensen J. Zhao, Ball State University, jzhao@bsu.edu
Christopher B. Davison, Ball State University, cbdavison@bsu.edu

ABSTRACT

This manuscript provides a comprehensive look into connected cars, the future of transportation that is accentuating the power and capabilities of the Internet of Things (IoT). The growing interest and demand for connected cars are ascribable to features they offer such as comfort, connectivity, performance, and safety. Connected cars can utilize their native embedded systems to communicate with other vehicles and infrastructure, exchange safety data, receive system updates, and stream infotainment. This utilization is made possible by the IoT, which is a concept that has grown immensely over the years to encompass billions of physical devices that are embedded with a system of Internet-enabled sensors. This sensor use allows the devices to transmit and receive data across various network types. It also enables communication with a whole interconnected intelligent system of other Internet-capable devices. The integration of IoT technologies in business and home environments has transformed the depth of interaction humans can have with IoT devices, changing the modern world in countless ways. The IoT has redefined how the Internet, and data analytics and processing, can be used in conjunction with physical devices. Nearly any physical object, even if it is not a traditional computing device, can be equipped with IoT functionalities.

Keywords: Internet of Things (IoT); connected car; V2I, V2V, wireless technologies; intelligent transportation systems; big data

INTRODUCTION

The automobile has a rich history in shaping American culture, providing millions of people with the convenience of mobility. The car, in and of itself, has become a symbol of independence and personal freedom that has continued to evolve alongside American society since its inception (HVA, 2013). Over the past decade, there has been an increasing effort to produce cars that can wirelessly communicate with one another as well as the user by using the Internet. By 2020, it is projected that 61 million new automobiles will be on the market that is equipped with data connectivity (Forni & Meulen, 2016). IHS Markit forecasts that by 2023, worldwide sales of connected cars will reach 72.5 million (IHS Markit, 2019). This digitally connected environment of wireless networks and physical sensors that can provide connectivity between the user and other Internet applicable devices is part of the Internet of things (IoT), and it has dramatically changed the relationship between cars and their owners (Alam, Saini, & El Saddik, 2014, 2015; Etzion, Fournier, & Arcushin, 2014; Euchner, 2018).

The IoT is the concept that nearly any object can be designed to have Internet connectivity (Alam, Saini, & El Saddik, 2014, 2015; Etzion, Fournier, & Arcushin, 2014; Raemdonck, Cutsem, Esmaili, Cortes, Dobbelaeere, Hoste, Roelands, & Trappeniers, 2017). These objects are capable of wirelessly connecting to the Internet and can come in a variety of different forms including Google Home, Amazon Echo, connected cars, as well as smart devices such as doorbells, locks, thermostats, refrigerators, security systems, and a whole host of other Internet-capable devices that are connected through the IoT (Postscapes, 2019; Rouse, 2016). As projected by Statista (2019), it is expected that the total number of IoT connected devices will be approximately 35 billion worldwide by 2021, and more than double to over 75 billion connected devices worldwide by 2025.

One product that has seen an increase in demand for production is the connected car (Coppola & Morisio, 2016; Forni & Meulen, 2016; Raemdonck et al., 2017). The connected car is a vehicle that is capable of connecting to the Internet, as well as communicating with mobile phones and smart devices by using Wi-Fi, LTE, and Bluetooth technology (Ahmad et al., 2018; Berdigh & El Yassini, 2018; Coppola & Morisio, 2016). Connected cars employ mobile network technology that enables a user to manage primary functions remotely through a Smartphone, tablet, smartwatch, and computer (Svangren, Skov, & Kjeldskov, 2017; Venture Capital, 2019). Coppola and Morisio (2016) postulate that
connected cars use an in-vehicle network of internal and external connections that allow them to communicate with onboard computers, sensors, smartphones, other moving vehicles, and road infrastructure through the use of electronic control units (ECUs) (Berdigh & El Yassini, 2018; Coppola & Morisio, 2016). An ECU is a computer with pre-programmed and programmable chips that control the engine and other vehicle functions. The ECU receives input from a sensor and process this information before producing the necessary output (Coppola and Morisio, 2016). Connected cars also stream infotainment (music, television, movies, and other associated media) straight to the car’s dashboard (Coppola & Morisio, 2016).

DEFINING THE CONNECTED CAR

The connected car is defined by its capability to use Internet access to wirelessly communicate with other vehicles, mobile technologies, and roadside infrastructure on a rapid and continual basis (Swan, 2015; US Department of Transportation, 2019). As reported by Svangren et al. (2017), there is currently a growing interest in the connected car since it reportedly makes connectivity on wheels easier and offers comfort, convenience, performance, safety, and security alongside networking technology (Coppola & Morisio, 2016).

These vehicles come equipped with a whole host of promising technologies such as radar, lidar, cameras, and other sensors (US Department of Transportation, 2019). Even if a potential hazard is out of the driver’s line of sight, connected vehicle technologies can allow the user to receive alerts of hazardous situations much sooner than cars without the added technologies (Lu et al., 2014). This system provides the driver more time to react and may prevent an accident (US Department of Transportation, 2019). According to a study conducted by the National Highway Traffic Safety Administration (2016), vehicle-to-vehicle communication has the potential to reduce up to 80 percent of crashes when drivers are not impaired, which has the potential to save several lives and prevent millions of crash-related injuries a year.

NETWORK CONNECTIVITY IN THE CONNECTED CAR

Wireless networking technologies have a crucial role in delivering Internet services to connected car users. Many connected car models already come equipped with a wireless local area network so that the vehicle may provide wireless Internet access and communicate with other devices both inside and outside the vehicle (Berdigh & El Yassini, 2018; Coppola & Morisio, 2016; Ismail, 2018). Some of the most powerful wireless communication systems used by connected cars include Bluetooth, 4G LTE, ZigBee, Wi-Fi, radio-frequency identification, ultra-wideband, and millimeter-wave (Berdigh & El Yassini, 2018; Lu et al., 2014). Connected cars, like many other vehicles, contain ECUs that provide connectivity to different systems in the vehicle (Berdigh & El Yassini, 2018; Coppola & Morisio, 2016). Each ECU has its own function such as providing connectivity to infotainment systems, power trains, GPS, airbags, ABS, traction controls, engines, and many other systems and sensors in the car (Berdigh & El Yassini, 2018; Coppola & Morisio, 2016; Hamid et al., 2017; Kwon, Park, & Ryu, 2017; Lu et al., 2014).

The in-vehicular network in connected cars provide a wide variety of ECUs that perform different tasks depending on the system for which they are responsible (Berdigh & El Yassini, 2018; Coppola & Morisio, 2016). In newer models, ECUs can use built-in network communication lines to transmit data between one another (Berdigh & El Yassini, 2018). Through the control area network bus (CAN bus), a connected car can use ECUs to relay data along the in-vehicular network. This allows communication to be facilitated among the various ECUs connected to the CAN bus network, as we all as monitoring the various sensors inside of the car. Connected cars can also exchange data with technologies that are outside of the vehicle in the external environment by using vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), vehicle-to-cloud (V2C), and vehicle-to-pedestrian (V2P) (Berdigh & El Yassini, 2018; Lu et al., 2014; Kwon et al., 2017; Smale, 2019). As suggested by Berdigh and El Yassini (2018), these methods of communication between the connected car and the environment allow it to provide an array of security, services, and networking features to the owner. For example, V2I systems can notify the driver of transportation issues, such as heavy traffic, congestion, and vehicle safety (Berdigh & El Yassini, 2018).

Additionally, research using the CAN bus to collect data from onboard ECUs has found car diagnostic data can be extracted wirelessly from ECUs and the OBD-II and sent to the cloud in order to diagnose engine performance issues (Hamid et al., 2017). The OBD-II port is an industry-standard connector that monitors the status of various subsystems...
within a vehicle, such as the chassis, body, accessory devices, and other diagnostics (B&B Electronics, 2011). It allows external electronics to access a car’s computer system to obtain diagnostic reports on malfunctions and other errors. Extracting the data from the ODB-II wirelessly may further provide opportunities to explore the integration of wireless and cloud-enabled automotive testing devices such as the MD8475A signaling tester and the MT8870A universal wireless test, among others. That being said, systems such as V2V have challenges that can interfere with inter-vehicular communication. As reported by Lu et al. (2014), factors such as buildings in the environment, high vehicle mobility, and other vehicles can interfere with inter-vehicle communication. This can lead to issues such as latency in inter-vehicular communication and losing packets of data during transferal (Lu et al., 2014).

There is an increasing demand for V2I technology being integrated with modern vehicles (Lu et al., 2014). V2I technologies deliver Internet services to the user and allow them to tether devices, such as cell phones, tablets, and other mobile devices, to the vehicle (Berdigh & El Yassini, 2018; Lu et al., 2014). This network system can allow users to interact with their car on a deeper, different level because it provides additional services and applications to the user (Berdigh & El Yassini, 2018; Lu et al., 2014). Another feature prominent across many connected car models is how they allow owners remote access to a “smart ecosystem” that is comprised of their own smart home technologies. This can include but is not limited to IoT enabled products such as appliances, heating ventilation, and air conditioning systems, Amazon Echo, Google Assistant, smart thermostats, smart lighting, and security systems in their home. The benefit of this is that the owner can access their functions remotely from the vehicle why they are away (Copolla & Morisio, 2016).

Results from Svangren et al. (2017) on connected car users found that many times, drivers would use smartphones to interact with the car. From their smartphone, users could obtain data or information, such as battery level, mileage, the car’s physical location, and charging status, about their connected car. Additionally, some connected cars can receive system updates that are as easy to install as clicking a button. Research from Svangren et al. (2017) found that software updates could be installed either wirelessly or manually. These two methods for updating were correlated to car make and model. Wirelessly updating the system software, as seen with Tesla models, involves receiving updates through the Internet, which may be initiated through a phone app or the car itself; the manual methods for updating system software involve taking the car to a mechanic who has the right equipment to successfully install a software update (Svangren et al., 2017).

ENHANCED APPLICATIONS AND FEATURES IN CONNECTED CARS

Connected cars have a wide range of features and mobile applications available to the consumer. Manufacturers may integrate unique features into a connected car model that is exclusive to their brand. BMW offers a unique system called ConnectedDrive which combines various elements from online applications, Wi-Fi hotspots, driver assistance, eCall center services, concierge services, stolen vehicle recovery, on-street parking assistance, real-time traffic information, parking assist, remote 3D viewing, and various solutions to provide Internet connection for intravehicular mobile devices (BMW, 2019). NissanConnect and AudiConnect are some other examples of brand-specific applications and features that manufacturers may only put exclusively in their cars (Audi, 2019; Nissan, 2019).

As reported by Swan (2015), connected car models made after 2010 may come equipped with infotainment media centers built into the dashboard that can be navigated through touch or voice command. These infotainment centers convert the car into a multimedia environment where the user can interact with the car using video, music, Internet browsing, and an array of services at the touch of a button. Some typical features of infotainment devices can include music streaming, navigation, smartphone-to-vehicle integration, navigation, parking assistance, and car diagnostics (Copolla & Morisio, 2016; Lu et al., 2014; Svangren et al., 2017). Two of the more popular infotainment technologies available to connected car owners that researchers have found include Apple Carplay and Android Auto (Svangren et al., 2017). These systems utilize mirroring technology to connect a car and smartphone to one another. Apps such as Carplay, MirrorLink, and Android Auto operate from a smartphone and integrate functions that are native to the smartphone into the dashboard display of the car (Android, 2019; Apple 2019; Rosamond, 2017; Svangren et al., 2017). This provides the driver with enhanced smartphone functionalities that are specifically designed for driving, so distractions from the road are severely minimized (Apple, 2019; Lu et al., 2014; Rosamond, 2017).
Many car manufacturers and third-party software developers have apps available for owners to download. These apps work alongside the sensors inside the connected vehicle to give owners up-to-date notifications on their vehicle, and may also offer additional features, such as remotely checking gas mileage, emissions, battery charge, tire pressure, and much more (Smale, 2019; Svangren et al., 2017). Depending on the brand, there will be different features and personalization options available. Nonetheless, these features provide users with an abundance of personalization features and settings. One company ahead of the curve is Tesla, which provides free system updates for the software on seemingly each Tesla model (Svangren et al., 2017). Owners are sent a notification through the Tesla app when a new update is available, which can be applied manually in the car or remotely through the Tesla app. Some owners report noticing differences in the responsiveness and performance of the car after some updates (Svangren et al., 2017). For an additional fee, the company offers Autopilot packages that install an advanced driver-assistance system into the car that features autosteer, auto park, and driver assistance visualization, among other features and services (Kwon et al., 2017; Svangren et al., 2017).

INSURANCE

Driving data generated by connected vehicles has had an impact on the car insurance industry (IMS, 2019). Factors such as predictive modeling, machine learning, and AI technologies, as well as real-time data streaming and many others, have caused a shift in how insurance companies do business (IMS, 2019; Smale, 2019). Some major insurance companies have begun to modify their policy offerings in conjunction with new developments happening in the automotive industry, which has instigated these insurance companies to transition from being a pure insurance provider to providing other insurance alternatives such as usage-based insurance (IMS, 2019). For example, Progressive offers a usage-based insurance program, Snapshot, which factors in driving habits, such as driving times, speed, braking, and driving ability, in order to provide the user with a personalized rate based on how and how much the car is driven (Progressive, 2019).

The data are typically gathered by insurance companies through a dongle connected to the vehicle’s OBD-II port, or an onboard telematics diagnostics device that allows the company to perform further personal and regional risk assessments (Dataman, 2018; IMS 2019). These companies may also offer mobile apps for users to download to their smartphones from the app marketplace to receive detailed updates and notifications on how they are driving. Aside from Progressive, other insurance companies with usage-based insurance options include Metromile, Nationwide, Allstate, and Esurance, among others (Hunt, 2019).

SAFETY AND SECURITY

One of the primary goals of the connected vehicle is driver safety. Manufacturers aim to reduce the number of injuries and fatalities caused by crashes and other road incidents. Connected cars achieve this through the use of in-vehicular radars, lasers, and other sensory devices equipped on the connected car that can notify the user of crashes about to occur through detection. In order to protect the driver, the car can attempt to prevent the crash through automated decision-making (Coppola & Morisio, 2016). It can perform actions such as applying the brakes and steering to avoid a collision (Coppola & Morisio, 2016). Many models of cars being produced also include lane keep assist and lane departure warning systems to keep drivers from drifting into another lane or merging too close to another vehicle (Coppola & Morisio, 2016; Lu et al., 2014).

In Europe, many new car models are required to come equipped with eCall, a system that sends out an automatic call to emergency personnel if a crash or other vehicular hazard occurs. OnStar, found in many vehicles in the United States, shares similar functions to the European system. Coppola and Morisio (2016) report that the eCall system attempts to minimize the period of time between the crash and the victim receiving aid for their injuries. This emergency system is estimated to save over 2,500 lives a year (European Commission, 2019).

There is a notable concern for the security of connected cars. In a review of the dangers of Internet connectivity in non-self-driving cars, Consumer Watchdog (2019) partnered with car industry technologists and engineers and found that a number of new 2020 models have open communication networking ports that leave their systems vulnerable to an array of different cyberattacks. Consumer Watchdog (2019) found that most connected vehicles share this same vulnerability due to V2I connectivity to the infotainment system, and connectivity provided by the vehicle’s CAN
buses. Among the list includes top-selling carmakers GM, Toyota, Ford, Fiat-Chrysler, Renault-Nissan-Mitsubishi, Honda, Hyundai/Kia, Subaru, Volkswagen, and Daimler (Consumer Watchdog, 2019). The report found that some of these manufacturers use open source software written by third parties in their vehicle software, and that can provide a “backdoor” for hackers to enter the system through.

Additionally, this brings into consideration the security of certain functions of some connected cars, such as wireless updates to the vehicle’s software. Because of this, it is critical that manufacturers are aware of consumer safety. It is imperative to ensure that hackers cannot compromise the security of connected vehicles. Research conducted by Svangren et al. (2017) on connected cars reported that many connected-car owners did not even consider their car as something that could be compromised or hacked. This security issue may be startling to some individuals, but the danger is genuine.

DATA COLLECTION AND PRIVACY

It is no secret that connected cars, along with many other devices a part of the IoT, actively collect data for companies to provide better assistance to their customers. Devices connected to the Internet will generate useful data that is collected, analyzed, and in some cases, even sold by a company; this is a concept known as big data (Kwon et al., 2017; Marr, 2017; Verma, 2018). Big data is a rich collection of data that is generated through usage by a user. This amalgamation of data can include an array of information from driving behavior, shopping habits, and online searches, too many other activities that generate data for a company (Liedtke, 2018; Quay Consulting, 2019). Research has reported that some connected car owners have a concern as to what data is being sent to the manufacturer (Svangren et al., 2017).

According to findings by Svangren et al. (2017), the data collected may include non-personal data such as information about the car battery or other types of data such as geographic location though it can be challenging to assess the exact data being supplied to the manufacturer. This has made privacy, the purpose of data usage, and knowledge of data being collected a real issue for consumers (Svangren et al., 2017). For this reason, individuals should be mindful of what data is being collected and supplied to car manufacturers. Even interacting with a connected car remotely with a computer or smartphone app is enough to leave behind a digital footprint of data that can be collected and supplied to the car manufacturer.

SUMMARY

This manuscript presented an overview of the IoT and connected cars. This includes information pertaining to connected cars, safety and security, wireless networking capabilities, intra-vehicular systems, Internet accessibility, data collection, privacy, and both applications and features available to connected car users. It also identifies changes in automotive insurance caused by connected cars, along with some of the benefits and drawbacks of connected cars in their current state. One of the biggest challenges for manufacturers to overcome will be strengthening the security of their software, as well as improving the wireless networking efficiency of connected cars so that external and internal interferences do not slow down data transferal speed. In the coming years, millions of connected cars will be on the road, equipped with a whole host of specifications and features to meet consumer needs. Some manufacturers are already ahead of the competition and are finding new ways to integrate IoT technologies with the connected car in an effort to improve user experience.

REFERENCES


National Highway Traffic Administration. (2016). *Proposed rule would mandate vehicle-to-vehicle (v2v) communication on light vehicles, allowing cars to ‘talk’ to each other to avoid crashes.* Retrieved from https://one.nhtsa.gov/About-NHTSA/Press-Releases/ci.nhtsa_v2v_proposed_rule_12132016.print/


