**Autonomous Vehicles:**

**Boons of the IoT Landscape**

**Origins/Development/Adoption:**

The past decade has seen a surging trend of interest and developments in the Internet of Things (IoT). According to a 2014 Forbes article, “The analyst firm Gartner says that by 2020 there will be over 26 billion connected devices [3].” One emerging technology within this context is the autonomous, or driverless, vehicle. They are joining the growing list of objects that can be called cyber-physical systems (CPS), systems which “tightly integrate cyber and physical components and transcend discrete and continuous domains. [11] ” In this sense, driverless cars, like many other IoT devices, exist at the nexus of disparate technologies unified by the ability to transfer data. While automated travel to some extent has been realized within public transit, autonomous cars provide something novel in that true autonomy is achieved by communicating with the surrounding environment.

Autonomous cars represent a host of benefits ranging from the local viewpoint of the end user to large-scale economic and municipal perspectives. Many companies, researchers, and governmental bodies are supporting the transition into the technology because of the potential for saving human lives, increasing consumer convenience and time, lowering insurance premiums, and reducing traffic congestion.

The technology does, however, contain dangers and hidden caveats; most notably, the dangers of vehicle hacking and the consequences of software malfunction may lead to tragic results. Other concerns such as the legislation and regulation involved with the new technology may lead to many legal grey areas in cases of accidents involving driverless vehicles. Also, autonomous vehicles face some of the problems common to other IoT devices such as privacy concerns surrounding the potentially personal data that sensors may process.

The development of the technology centers around data and learning. The degree of connectivity required to actualize autonomous driving is exemplified in the name given to the wireless communication protocol developing in tandem, Vehicle-to- Everything (V2X) communication. V2X is adapted from WLAN (marketed as Wi-Fi) and standardized in the IEEE 802.11p amendment to add wireless access in vehicular environments (WAVE) to the 802.11 networking specifications. V2X technology allows for Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I), Vehicle-to-Pedestrian (V2P) , [Vehicle-to-Device](https://en.wikipedia.org/wiki/V2D) (V2D) and Vehicle-to-Grid (V2G) communication, forming ad-hoc networks based on range [22]. It is standardized both in the United States and Europe, where it forms the basis of the ITS-G5 specification [30].

Furthermore, another helper in the development of driverless cars and to the IoT landscape in general, is an architectural paradigm dubbed Fog Computing, a term coined by the Cisco Corporation and also called fogging or simply fog. Fog is emerging to complement the cloud computing architecture. According to the OpenFogConsortium, “Fog is a system-level horizontal architecture that distributes computing, storage, and networking closer to the user, and anywhere along the cloud-to-things continuum.” Its intent is to leverage more of the network end-nodes and edges between the centralized backbone of the internet cloud and the devices connected to it [26].

Fog computing provides a robust architectural framework well-suited to handle the requirements of autonomous vehicles’ breakthrough into the “internet of cars” amidst the IoT landscape. While the benefits of autonomous cars depend largely on the the reliability and adoption of the technology on large scales, even at small scales the technology is highly data-driven. As Chiang and Zhang indicate, “a connected car, for example, can create tens of megabytes of data per second. An autonomous vehicle will generate even more data, which was estimated to be about one gigabyte per second [17].” This is coupled with the prediction by the IDC research group, that by 2019 nearly 45% of IoT data will reside or otherwise interact at or close to the network edges [31]. Jointly, this emphasizes the importance of a network architecture that is suited for the IoT landscape and in particular for autonomous vehicles whose failures could have fatal consequences.

The explosion of artificial intelligence and data science advancements is another major developmental stepping stone for driverless vehicles which may be the stabilizing counterbalance that drives the technology through uncertain beginnings. In 2005, it was machine learning and probabilistic reasoning techniques that won the DARPA Grand Challenge all-terrain race when Stanley, an AI-controlled vehicle developed at the Stanford AI Laboratory, came in first place [28]. DARPA sponsored the event with the specific purpose of spurring the state of unmanned vehicle technology [2]. Since then areas of research such as computer vision, path finding, deep learning, and probability heuristics have progressed further and are all used in conjunction with autonomous vehicles. Developments in intelligent systems may thus be considered the beating heart of driverless vehicles. [expand on this section]

With the appropriate application of the supporting technologies fueling the cresting wave of vehicle autonomy, The future of the technology is Car manufacturers and tech giants are within years of ushering in the new era in the unfolding of the Internet of Things. Out of twenty major companies and well-funded startups who are working on driverless vehicle models, fourteen -- Nissan, Toyota, Daimler, Tesla, Volvo, BMW, Ford, Baidu, Honda, Faraday Future, LeEco, Bosch, PSA Groupe, and even Apple -- are said to be aiming for public release within the next one to three years [32]. These companies span the globe and are able to manufacture and market autonomous vehicles en masse. Autonomous cars themselves depend on such communication. As stated in an IoTJournal web article, “Driverless cars require an immense amount of data gathering and analysis due to their connection to cloud-based traffic and navigation services, among other outlets for connectivity [15].”

This is an important note for the technology since, as mentioned above, several of the benefits of autonomous vehicles are only realizable when a large enough threshold of the population has access to driverless vehicles.

**Benefits/Consequences**

Driverless cars have the potential to significantly reduce traffic congestion. One way autonomous cars can help achieve this is known as “platooning.” Platooning refers to the formation of chains of sensor-assisted vehicles in the single lane. The communication capabilities of the vehicles allows for safely achieving close-proximity even at high speeds, taking advantage of improved aerodynamics and highway space capacity. This ability will increase as more vehicles on the road are either driverless or can otherwise communicate with driverless vehicles.

Unfortunately, in the initial stages of the technology’s consumer-facing release, the user base will be a small proportion of the total vehicles on the road. The initial cost of an autonomous car may be too high for most consumers leading to a slow return on the apparent benefits. Driving conditions for autonomous cars will be more chaotic in the potentially unpredictable situations created by human drivers.

Nevertheless, the Huffington Post reports that "per the Insurance Information Institute (III) even if you don't plan on getting one, all consumers are likely to financially benefit from self-driving cars." Their explanation is that even with low initial consumer adoption rates “autonomous cars will make roads safer through their interconnectivity (via the IoT), meaning fewer accidents and fewer claims filed, meaning consumers are less at risk, meaning insurance companies will need to lower their premiums overall [15].”

However, a severe issue with security will still exist at any level of adoption rate. Demonstrations of car hacking have proven how disastrous the prospective consequences of software vulnerabilities can be. Charlie Miller and Chris Valasek are two names now synonymous with hacking vehicles. These two developed a program for a year in order to hack the controls of vehicles that are connected to the internet. Their program can control just about any aspect of a vehicle including: the air control, the stereo, windshield wipers, and most importantly, the brakes. Although a passenger could attempt to resist the control of Miller and Valasek’s program, the driver would have to be alert and aware of the hack, and have a quick enough reaction time to stop the vehicle from, for example, turning left at 80 miles per hour [33]. If the vehicle is totally autonomous, then the passenger of the vehicle could be placed in the backseat of the vehicle (much like the plans for autonomous taxi services that Uber and others have planned). If this is the case in an autonomous automobile hack, then the passenger would have physically no manual control over the vehicle.

One of the more vulnerable points of a vehicle’s system is the OBD2 port usually found under a dashboard. An OBD2 port is used mainly for on-board diagnostics, but can be used for much more [34]. For instance, in certain cases the OBD2 port may allow hackers to control the brakes of a vehicle [33].

In 2016, researchers found that they were able to deceive Tesla’s autopilot sensors by using “off-the-shelf radio-, sound- and light-emitting tools.” This theory and practice of hacking the Tesla S came from the conclusion of a devastating crash that occurred earlier that year. Apparently, the autopilot sensors in the Tesla S did not properly sense a trailer turning into the vehicle’s path and killed the person inside the vehicle. Through their research, the researchers were able to dube the autopilot sensors of the Tesla S into believing that there either was not an object in the vehicle’s path when in reality there actually was, or that there was an object in the vehicle’s path when in reality there actually was not. Fortunately, for Tesla, the experiments called for rather expensive equipment to be performed successfully. The researchers also claimed that the experiment would prove even more difficult to be executed while the vehicle was in motion. One of the more interesting and cost effective hacks on the Tesla S was the ability to disguise an object with acoustic dampening foam, similar the foam one might find in a sound studio. The acoustic dampening foam hack prevented an object from being seen by the Tesla S ultrasonic sensors. All of the hacks were not seen as entirely realistic, but begin to peel the layers of flaws when relying on current autopilot technologies [35].

One of the reasons behind the difficulties in securing these hardware and software related issues is that the companies that are attempting to deliver autonomous taxi services are not the same companies that are developing and manufacturing the vehicles themselves. In order for autonomous vehicles to become a ubiquitous reality, open communication between companies such as Uber and Didi, and auto manufacturers like Chevy and Toyota is vital.

Difficulties aside, autonomous cars from both an individual user’s perspective as well as a city government offer tantalizing benefits. The ability for a car to self-navigate shifts drivers to passengers. Drunk and distracted driving would be reduced as more driverless cars fill the streets. A single passenger in a driverless vehicle would be able to use the time at his or her discretion, increasing leisure or productivity on daily commutes for instance. Driverless cars would also benefit even when a passenger leaves the vehicle by allowing the occupant to leave the car while it parks itself.

[Discuss smart cities and relations to IoT]

[Conclusion]

\*\*\*\*

Autonomous cars themselves depend on such communication.“Driverless cars require an immense amount of data gathering and analysis due to their connection to cloud-based traffic and navigation services, among other outlets for connectivity”

Potentially less road accidents in the long run

Savings in insurance and healthcare due to less accidents

“a primary benefit of fog computing is its ability reduce latency,” [https://www.openfogconsortium.org/top-10-myths-of-fog-computing/Computing]

* Privacy/Security issue: personal data collected may be breached or misused
* Economy issue: Transportation jobs at risk of elimination
* Computers rely on information like GPS and traffic signals, which could be a problem if these fail (edge cases, power failure, inaccuracy, etc.)

[ttps://blog.caranddriver.com/researchers-find-a-malicious-way-to-meddle-with-autonomous-cars/](https://blog.caranddriver.com/researchers-find-a-malicious-way-to-meddle-with-autonomous-cars/)

[1] J. Boeglin, “- The Costs of Self-Driving Cars: Reconciling Freedom and Privacy with Tort Liability in Autonomous Vehicle Regulation,” *- Yale J. Law Technol.*, p. 171, 2015.

[2] “A Brief History of Autonomous Vehicle Technology,” *WIRED*. [Online]. Available: https://www.wired.com/brandlab/2016/03/a-brief-history-of-autonomous-vehicle-technology/. [Accessed: 20-Nov-2017].

[3] J. Morgan, “A Simple Explanation Of ‘The Internet Of Things,’” *Forbes*. [Online]. Available: https://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/. [Accessed: 20-Nov-2017].

[4] C. M. Silva, B. M. Masini, G. Ferrari, and I. Thibault, “A Survey on Infrastructure-Based Vehicular Networks,” *Mob. Inf. Syst.*, vol. 2017, pp. 1–28, 2017.

[5] D. Wu, Q. Liu, Y. Li, J. A. McCann, A. C. Regan, and N. Venkatasubramanian, “Adaptive Lookup of Open WiFi Using Crowdsensing,” *IEEEACM Trans. Netw.*, vol. 24, no. 6, pp. 3634–3647, Dec. 2016.

[6] J. Jung, R. Chen, W. Jin, R. Jayakrishnan, and A. C. Regan, “An Empirical Study of Inter-Vehicle Communication Performance Using NS-2,” *Univ. Calif. Transp. Cent.*, 2010.

[7] “Atlanta plans ‘smart corridor’ in Midtown to help test self-driving cars and technologies,” *Atlanta Business Chronicle*. [Online]. Available: https://www.bizjournals.com/atlanta/news/2016/10/24/atlanta-plans-smart-corridor-in-midtown-to-help.html. [Accessed: 20-Nov-2017].

[8] “Autonomous Vehicles and the Internet of Things,” *LeClairRyan - Law & Technology*, 10-Nov-2016. .

[9] R. Chen, W. L. Jin, and A. Regan, “Broadcasting safety information in vehicular networks: issues and approaches,” *IEEE Netw.*, vol. 24, no. 1, pp. 20–25, Jan. 2010.

[10] D. Wu, Q. Liu, Y. Zhang, J. McCann, A. Regan, and N. Venkatasubramanian, “CrowdWiFi: efficient crowdsensing of roadside WiFi networks,” 2014, pp. 229–240.

[11] R. Baheti and H. Gill, “Cyber-physical systems,” *Impact Control Technol.*, vol. 12, pp. 161–166, 2011.

[12] G. Yang and X. Zhou, *Cyber-Physical Systems*. 2013.

[13] Y. Zhang, F. Xie, Y. Dong, X. Zhou, and C. Ma, “Cyber/Physical Co-verification for Developing Reliable Cyber-physical Systems,” in *2013 IEEE 37th Annual Computer Software and Applications Conference*, 2013, pp. 539–548.

[14] L. Zhenyu, P. Lin, Z. Konglin, and Z. Lin, “Design and evaluation of V2X communication system for vehicle and pedestrian safety,” *J. China Univ. Posts Telecommun.*, vol. 22, no. 6, pp. 18–26, Dec. 2015.

[15] “Driverless Cars and Their Relation to the IoT - IOT Journal.” [Online]. Available: http://www.iotjournal.com/articles/view?15352. [Accessed: 20-Nov-2017].

[16] “FACT SHEET: Administration Announces New ‘Smart Cities’ Initiative to Help Communities Tackle Local Challenges and Improve City Services,” *whitehouse.gov*, 14-Sep-2015. [Online]. Available: https://obamawhitehouse.archives.gov/the-press-office/2015/09/14/fact-sheet-administration-announces-new-smart-cities-initiative-help. [Accessed: 20-Nov-2017].

[17] M. Chiang and T. Zhang, “Fog and IoT: An Overview of Research Opportunities,” *IEEE Internet Things J.*, vol. 3, no. 6, pp. 854–864, Dec. 2016.

[18] “Forget the Internet of Things: Here Comes the ‘Internet of Cars,’” *WIRED*. [Online]. Available: https://www.wired.com/2013/01/forget-the-internet-of-things-here-comes-the-internet-of-cars/. [Accessed: 20-Nov-2017].

[19] D. Wu, J. Luo, R. Li, and A. Regan, “Geographic load balancing routing in hybrid Vehicular Ad Hoc Networks,” in *2011 14th International IEEE Conference on Intelligent Transportation Systems (ITSC)*, 2011, pp. 2057–2062.

[20] W. D. Jones, “Hard drive - robotic cars impress in rough road race,” *IEEE Spectr.*, vol. 42, no. 12, p. 13-, Dec. 2005.

[21] “HP News - HP Study Reveals 70 Percent of Internet of Things Devices Vulnerable to Attack.” [Online]. Available: http://www8.hp.com/us/en/hp-news/press-release.html?id=1744676#.WEgZLPkrJPZ. [Accessed: 20-Nov-2017].

[22] Z. Liu, Z. Liu, Z. Meng, X. Yang, L. Pu, and L. Zhang, “Implementation and performance measurement of a V2X communication system for vehicle and pedestrian safety,” *Int. J. Distrib. Sens. Netw.*, vol. 12, no. 9, p. 1550147716671267, Sep. 2016.

[23] D. Wu, L. Bao, A. C. Regan, and C. L. Talcott, “Large-scale access scheduling in wireless mesh networks using social centrality,” *J. Parallel Distrib. Comput.*, vol. 73, no. 8, pp. 1049–1065, Aug. 2013.

[24] D. Wu, Y. Zhang, L. Bao, and A. C. Regan, “Location-Based Crowdsourcing for Vehicular Communication in Hybrid Networks,” *IEEE Trans. Intell. Transp. Syst.*, vol. 14, no. 2, pp. 837–846, Jun. 2013.

[25] R. Chen, W. Jin, and A. Regan, “Multi-Hop Broadcasting in Vehicular Ad Hoc Networks with Shockwave Traffic,” in *2010 7th IEEE Consumer Communications and Networking Conference*, 2010, pp. 1–5.

[26] “Resources | OpenFog Consortium.” [Online]. Available: https://www.openfogconsortium.org/resources/#definition-of-fog-computing. [Accessed: 20-Nov-2017].

[27] “Self-Driving Cars of the Future: Reliable IoT Components Promote Vehicle Safety.” [Online]. Available: https://www.sierrawireless.com/iot-blog/iot-blog/2017/05/self\_driving\_cars\_of\_the\_future\_reliable\_iot\_components\_promote\_vehicle\_safety/. [Accessed: 20-Nov-2017].

[28] S. Thrun *et al.*, “Stanley: The robot that won the DARPA Grand Challenge,” *J. Field Robot.*, vol. 23, no. 9, pp. 661–692, Sep. 2006.

[29] “Top 10 myths of fog computing | OpenFog Consortium.” .

[30] “Intelligent Transport Systems (ITS); Access layer specification for Intelligent Transport Systems operating in the 5 GHz frequency band.” European Telecommunications Standards Institute, Nov-2012.

[31] "IDC FutureScape: Worldwide Internet of Things 2017 Predictions", *www.idc.com*, 2017. [Online]. Available: <https://www.idc.com/research/viewtoc.jsp?containerId=US40755816>.

[32] D. Muoio, “These 20 companies are racing to build self-driving cars in the next 5 years,” *Business Insider*. [Online]. Available: <http://www.businessinsider.com/companies-making-driverless-cars-by-2020-2016-11>.

[33] A. Greenberg, “Securing Driverless Cars From Hackers Is Hard. Ask the Ex-Uber Guy Who Protects Them,” *WIRED*, 12-Apr-2017. [Online]. Available: https://www.wired.com/2017/04/ubers-former-top-hacker-securing-autonomous-cars-really-hard-problem/.

[34] S. Edelstein, “From dongles to diagnostics, here’s all you need to know about OBD/OBD II,” *Digital Trends*, 07-Apr-2017. [Online]. Available: <https://www.digitaltrends.com/cars/everything-you-need-to-know-about-obd-obdii/>.

[35] A. Greenberg, “Hackers Fool Tesla S’s Autopilot to Hide and Spoof Obstacles,” *WIRED*. [Online]. Available: https://www.wired.com/2016/08/hackers-fool-tesla-ss-autopilot-hide-spoof-obstacles/.