bizcommunity

How will 5G impact automotive IoT and its security?

The internet of things (IoT) has taken the world by storm, from smart toasters to pet feeders, it seems that each of our everyday appliances is getting upgraded with an embedded computer a an internet connection.

By Nicolò Boatto 2 Mar 2021

© Karsten Neglia – 123RF.com

The advent of 5G will only help in accelerating this trend by adding much-needed bandwidth, enabling massive deployments of low power and low-cost devices and, more importantly for critical applications, providing cellular devices with internet connections capable of ultra-low latencies (down to 1ms) and high reliability (up to 99.9999%). These improvements in cellular technology won't have much of an impact on your smart kettle, which most likely relies on a Wi-Fi connection to operate, but they will have an enormous impact on the automotive industry through C-V2X and autonomous vehicles.

LOGISTICS & TRANSPORT

Self-driving cars will not fix our transportation woes

6 Jan 2020

What is C-V2X?

C-V2X (which is short for cellular vehicle-to-anything) is a standard designed to allow vehicles to communicate with other vehicles and with urban infrastructure via cellular connections. Its purpose is to enable not only modern comforts such as connected infotainment systems, but also better safety and efficiency and to support the development of increased autonomy by providing vehicles with cooperative awareness from a plethora of sensors, both stationary and on other vehicles.

Some examples of the features that could be implemented thanks to C-V2X are: cooperative collision avoidance and hazard warnings enabled by the knowledge shared between vehicles and roadside sensors congestion prevention through real-time traffic management, and platooning, which is the formation of autonomously driven vehicle convoys, which provide better efficiency through improved aerodynamics and avoidance of excessive braking.

AUTOTECH

Are we ready for self-driving vehicles?

28 Nov 2019

Trusting autonomous vehicles

One key enabler of these features is the increased autonomy that these vehicles will possess, allowing the to make decisions based on all the data that they collect through their sensors and the network. For these vehicles to be able to act autonomously and for users to feel at ease riding in them, manufacturers need to make sure that both the decision-making software and the data on which these decisions are based have not been tampered with, which brings us to the topic of security.

Securing the automotive industry

With each car becoming a node in a network of moving things, there is an exponentially increased risk of cyber-criminals remotely performing malicious activities which previously required physical access to the vehicle. These attacks could range from ransomware, where the victim could be forced to pay a ransom to regain the ability to use their car or even an entire fleet of vehicles, to spying on the car's users, or to even more grim ones that could cause vehicles to crash. All these attacks could be performed by tampering with vehicle's software. This could be achieved directly by exploiting existing vulnerabilities in the software, or by attacking the systems that are tasked with providing vehicles with software updates.

AUTOTECH

Connected cars and the revolutionary road of the future

Christophe Lepoivre 24 Jun 2019

Another aspect that needs to be considered when discussing the security of connected things is the protection of devices against attacks that involve physical access. This is a key issue especially because vehicles are often parked in public spaces where attackers could easily access them. Moreover, issues in hardware security are generally difficult to remediate and might require measures as extreme as recalling vehicles to be upgraded with new and more secure hardware.

These scenarios are not only possible, but could become plausible unless manufacturers approach the security of vehicles and infrastructure proactively, which could end up being not only more responsible towards consumers, but also more cost-effective in the long run.

ABOUT THE AUTHOR

Nicolò Boatto, security tester at Aon