World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:16, No:5, 2022

Experimental Testbed to Compare 4G and 5G Industrial IoT Connections in Simulated Based Control System

Andrea Gelmini

***Abstract*—**This paper considers the advent of 5G and the use of it in a Based Control System (BCS), posing as a basic concept the question of what the real differences and practical improvements are compared to 4G. To this purpose, a testbed hardware simulator has been designed and built where identical machines with the same sensors and management systems will communicate with different radio access network connections. This allows an objective statistical comparison of performance on the real functioning and improvement of the infrastructure with the Industrial Internet of Things (IIoT) connected to it.

***Keywords*—**4G, 5G, BCS, eSIM, IIoT, SCADA, Testbed.

I. Introduction

MOBILE telecommunications technology is advancing relentlessly and we have now arrived at what has been called the fifth generation of mobile technology. This new technology involves the use of frequencies, devices and mobile communications management cores that are different and innovative from those known and used so far. However, despite the great marketing effect of this new technological step, the infrastructure is only at the beginning of its implementation; moreover, excluding some high-end mobile phones, there are very few devices equipped with 5G chips on the market. Currently, most mobile communication systems remain within the scope of previous generations although there may be a spike in the sale of very expensive mobile devices with the new hardware and software protocols.

In order to switch to the use of 5G technology soon, it is necessary (beyond the theoretical specifications declared in the devices) to carry out tests to obtain comparative values that can help to obtain greater clarity in the advantages and the disadvantages for the use of this new technology. In this regard, this work describes the implementation of an experimental testbed, a hardware simulator capable of connecting both in 4G and 5G modes, transferring simulated IIoT data. That is to say, to test the connections the focus will be on: maintaining carrier band, integrity of the transmitted data and the performance claims of the 5G system. So, the actual values obtained from the tests will be compared with the theoretical declared operating values parameters such as power consumption and checking the capability to maintain the carrier band signal despite potential environmental disturbances, always considering 4G as the referring sample system.

II. Definition of 5G

5G is the fifth generation of mobile communication technologies in cellular networks [1]-[3]. The use and communication of this infrastructure requires devices with antennas compatible with the established frequencies. This network technology does not strictly concern mobile phones, but any electronic device equipped with radio and SIM or electronic SIM (eSIM) equipment regardless of its size or use. 5G is also considered for the first time in the history of mobile communications, the first generation of mobile networks whose prototyping will be able to respond to a vast amount of use by very different services in a vertical vision of industries themselves, potentially covering every conceivable sector [4].

The 5G technology is characterized by the following key concepts underlying its complete implementation and operation [5]:

- *Millimetre Waves* are very high-frequency radio waves, between 30 and 300 GHz, these waves with these frequency values are characterized by lengths ranging from 1 to 10 mm from which they take their name.
- *Small Cell* is a new concept of antenna directly derived and connected to the *mmWAVE*. Basically, they are small low-power antennas, for which installation in a large number of antennas has been foreseen and planned to overcome the problem of the high frequency of the *mmWAVE* which cannot pass through buildings and vegetation, but also cannot arrive in long distance.
- *Massive MIMO* stands for "Massive Multiple – Input Multiple – Output", where any single antenna can receive and transmit a massive quantity of signals and connections at the same time.
- *Beamforming* is a technology that allows directing and concentrating the radio signal in one direction rather than another. It can be seen as a wave processing technique that allows directional transmission and reception of the signal. It is of fundamental importance and uses with *mmWAVE* and massive *MIMO* to avoid interference, so as to arrive only at the user's destination without broadcasting everything.
- *Full Duplex* has always been known, implementable and usable only with different frequencies. However, for 5G, the

Andrea Gelmini is with Cyber Security Department, University of South Wales, Pontypridd, UK (e-mail: andrea.gelmini@southwales.ac.uk).

technology allows with the use of new high-efficiency chips a routing circuit to be able to exploit full-duplex on the same frequency.

A detail to consider on the 5G radio spectrum is the wide range of frequencies that will be used. For the *mmWAVE* the designers have established limits that start from 30 up to 300 GHz; however, it is believed that in practice the frequencies will fluctuate from 24 to 100 GHz.

Finally, to consider what has already been implemented and considered like 5G first step, there are very close standard wave frequencies used, very similar to the 4G system defined as sub 6, which means up to 6 Ghz [6], [7]. In this sub 6 family range we have 5 possible windows of frequencies bands (depends on the country plan infrastructure implementation) [8], [9]:

- *617 MHz to 960 MHz Rural Long Distance*
- *1427 MHz to 2200 MHz Urban for mMTC*
- *2496 MHz to 2690 MHz Urban*
- *3300 MHz to 4200 MHz Dense Urban*
- *4400 MHz to 5000 MHz Urban High Speed*

This first group of frequencies (FR1) uses some frequencies that were already in the pre 5G standard. In contrast, from the FR2 group (over 6 GHz), they result in an analysis of no little difficulty due to the complex and very expensive finding of highly professional instrumentation, which is often behind a standard academic budget. For this specific reason, it is possible to analyze and test the connection and functions of the simulator with a software-defined radio instrument.

Differences with 4G

The descriptions of 5G first of all declare the great speed available that the devices will be equipped with, to prepare futuristic services. However, when dealing with small amounts of data, the focus on speed fades into the background, focusing on the security of the connection itself.

From the frequencies aspect, always remaining below 6 GHz, the 4G system already uses many of the frequencies planned for 5G, with the exceptions of 1.7 GHz, 3.4 GHz and 5 GHz.

The *Orthogonal Frequency Division Multiple Access* OFDMA modulation system, had already been implemented in 4G, now it will have to be verified how this modulation will improve or maintain the performance with different frequencies available. Another aspect to consider is the advanced ability to aggregate radio bands, that is the ability of a device to connect to several frequencies at the same time, increasing connection stability and performance, but perhaps presenting a higher energy consumption [8]-[11], [6].

III. Definition of BCS

A Based Control System is a control system better known as Industrial Control System or Distributed Control System, it is an automatic control system equipped with various subsets in different levels, including that of data acquisition and management better known as SCADA (Supervisory Control and Data acquisition), capable of automatically exchanging information from the process side for the entire architecture distribution, without therefore being centralized.

Many industrial computers called controllers form the system suitably segmented and separate each for each process plant. A failure or incident in the control of a process is not capable of affecting the operation of the distributed control system [12].

IV. Definition of IIoT

IIoT are an industrial category of IoT, that is, structures of the manufacturing production sector. In this regard, IIoT are and will be very important in industry 4.0 (considered in full application with 5G), where new intelligent technologies, for data, connections and automation are emphasized at the highest possible level. These devices can be seen both as sensors (temperature, air pressure, humidity, light, presence) with minimum energy consumption, great reliability in the detection of environmental values and long-time capacity for maintaining connection and operation, but also as sensor networks. intelligent, capable of intercommunication, energy management, predictive maintenance and intelligent production. Given their reliability in performance as well as apparent functional simplicity, a Lite Linux system was chosen for the simulation as a simple simulator to recreate its reality and operation; it is not possible to have excessively expensive industrial control and communication systems available. In 5G we can easily classify IIoT in two groups "*ultra-reliable low latency communication*" and "*massive machine type communication*"; "*enhanced mobile broadband*" are not considered as such as they are IoT devices with enormous payloads and IIoT could use years to generate the same payload that the latter could generate in a few hours such as virtual reality and high definition video streaming.

V. Testbed Model

This experimental testbed model is based on the concept of comparing the performance connections of two identical machines with the same sensors, therefore the same data to be transmitted, but remotely connected via two different connections: one in 4G and one in 5G. The relative comparison that will be highlighted through the analysis of the data emerging in the tests will give an answer or at least verify the actual differences and improvements that 5G claims to introduce. The simulator has been assembled considering the use of Raspberry Pi 4 B micro PC which is similar to an industrial PC, as they can represent in their reliability of operation with Lite embedded software compared to other operating systems. Exactly the behavior of an IIoT where it is essential to have simplicity and functioning as a device within any OT environment. The logic diagram of the testbed is shown in Fig. 1.

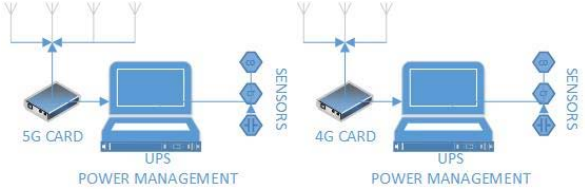

Fig. 1 Testbed Logic Scheme

The testbed model is designed to compare transmitted data and operating values; this can be done both with a single analysis on both devices, with the same uninterruptible power supply (UPS) power management system and the same sensors group. As previously mentioned in the definition of 5G about to frequency families, this model has been equipped at the 5G device side, with a radio access network 5G Sub-6 module. In addition to the difficulty of supplying a mmWAVE module on the market, almost all IIoT will work in industrial and rural areas of poor coverage and not in the city Centre, where there will probably be only the availability of 5G low frequencies belonging to the Sub-6 family. The assembled testbed is shown in Fig. 2, it is possible to view in details the same components for both sides, respectively for the 4G (Fig. 4) and 5G (Fig. 3) radio cards units.

Fig. 2 Testbed

VI. Tests' Description

The tests are designed to be as detailed and functional as possible in verifying the real differences between advantages and hypothetical disadvantages between the two communication technologies. To this purpose, it was thought to carry out statistical analyses and continuous surveys in the following operating situations:

- An essential factor is the ability of a device to consume as little energy as possible or be green resulting in the most negligible environmental impact. An analysis of how many *Watts* the device absorbs will be performed, both in full use and on standby. Theoretically, these devices should be designed to consume less energy. So considering the large use of IIoT, it will be very important to understand whether the sensors networks very sensitive to battery power consumption will demonstrate a more efficient absorption with the 5G network compared to 4G. In this regard, an energy management system which works in UPS mode will be used with times and absorption values.
- To obtain a comparison of the actual connection quality a latency check will be performed both in the transmission of data packets and in the speed of losing the connection with the radio cell and reconnecting. For these devices, it is not of fundamental importance the large bandwidth that 5G promises, but rather the ability to respond with almost zero latencies as URLLC and mMTC require. Here we are considering variations of a few milliseconds; however, it will be verified whether the 5G network can provide and guarantee this by improving 4G with refinement specifics.
- It will then be important to have a clear assessment of how the device connected in 5G will be able to constantly maintain the connection, whether it will be better than 4G or whether it will show problems due to environmental disturbances or not.
- In order to verify and compare latency and connection quality, a streaming flow control will be implemented. This stream will be related to the data transfer of individual files and the streaming of webcams for environmental monitoring. In both situations, it is planned to use payloads with a low amount of data (no more than a few hundred MB) not to saturate the timing of the tests.

These tests are performing a comparison just with the compatibility 4G infrastructure frequencies coverage at the moment. In particular, the 5G card is working in a compatibility mode like an NSA system without 5G frequencies [13]. This is because the presence of 5G coverage on the infrastructural side is very low as it has slowed down significantly in the last year [11].

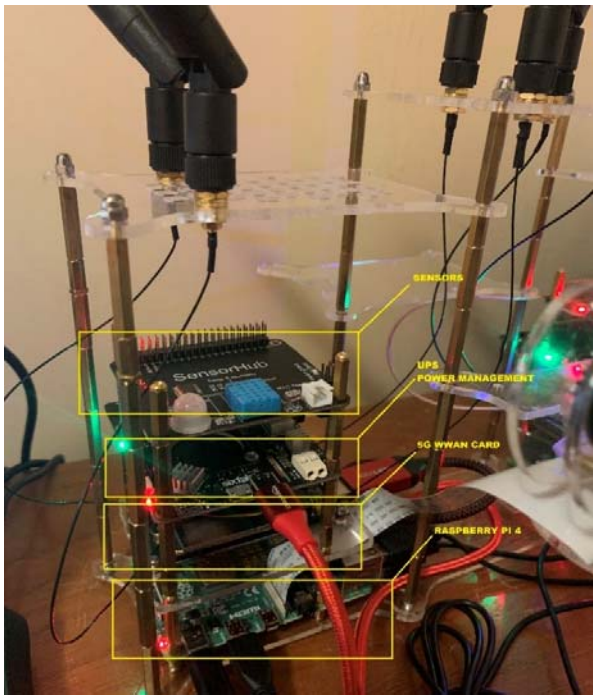

Fig. 3 Testbed 5G side

VII. Conclusion

This simulation study is going to be able to have these data and comparisons that were previously described in the kinds of tests potentially during 2022. It will be possible to have tests carried out under 4G and 5G coverage frequencies. From that point, it will be possible to understand how the testbed will behave with both a non-standalone (NSA) and a pure stand-

alone SA infrastructure designed for 5G [11], [13]. The novelty of this study concerns the possibility of studying and comparing two identical systems equipped with environmental sensor data transmitted on the network through a new radio connection evolution which requires new hardware and new infrastructure, obtaining a direct comparison with the infrastructure used so far. In addition to this fundamental first simulation step, it will be important as a subsequent job to carry out the same types of tests with different situations, for example with simulated cyber-attacks, for example, jamming electromagnetic signal disturbances on the same frequencies used.

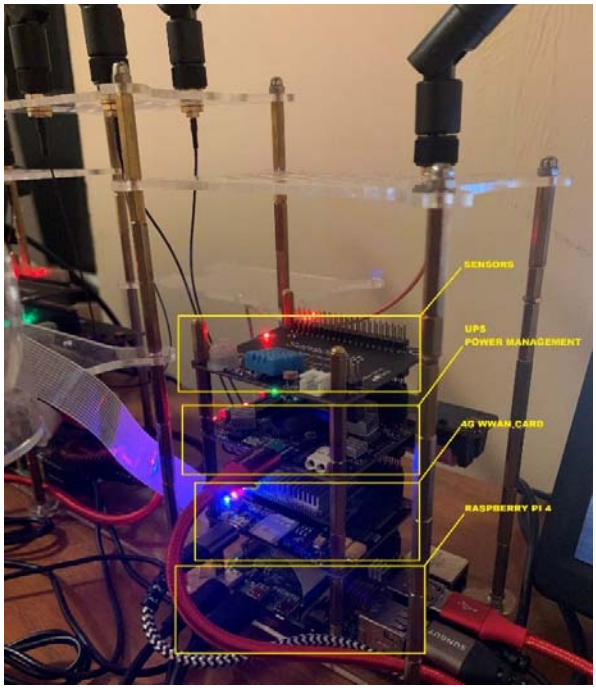

Fig. 4 Testbed 4G side

REFERENCES

[1] Symmetry Electronics, "From Digi: What is 5G? Part 1--Evolution and the Next Generation," 2019. (Online). Available: https://www.semiconductorstore.com/blog/2019/From-Digi-What-is-5G-Part-1-Evolution-and-the-Next-Generation/4179/. (Accessed: 16-Apr-2020).
[2] P. M. et al. (eds.), *5G System Design: Architectural and Functional Considerations and Long Term Research*. Hoboken, NJ: Wiley, 2018.
[3] B. NGMN Alliance, R. El Hattachi, and J. Erfanian, "NGMN Alliance 5G White Paper," 2015.
[4] 5G PPP Architecture Working Group, "View on 5G Architecture," 2019.
[5] IEEE, "Everything You Need to Know About 5G - IEEE Spectrum," 2018. (Online). Available: https://spectrum.ieee.org/video/telecom/wireless/everything-you-need-to-know-about-5g. (Accessed: 16-Apr-2020).
[6] MathWorks, "Testing 5G NR Devices with Standard Waveforms," 2019.
[7] N. R. Testbed *et al.*, "5G NR Testbed 3.5 GHz Coverage Results," pp. 2–6, 2019.
[8] Rohde & Schwarz, "Be ahead in 5G. Demystifying 5G NR," no. 6, pp. 5–6, 2020.
[9] MathWorks, "5G Explained: Introduction to 5G NR PHY - MATLAB," 2018. (Online). Available: https://uk.mathworks.com/videos/5g-explained-introduction-to-5g-nr-phy-1558595604785.html. (Accessed: 16-Apr-2020).
[10] R. Bhatia, "Introduction & Features of 4G: A Review," IJERT-International Journal of Engineering Research & Technology, Apr. 2018.
[11] Spirent, "5G: What to expect in 2020," 2020.
[12] R. R. R. Barbosa, R. Sadre, and A. Pras, "A first look into SCADA network traffic," in *Proceedings of the 2012 IEEE Network Operations and Management Symposium, NOMS 2012*, 2012, pp. 518–521.
[13] Cradlepoint, "The Pathway to 5G," 2019.