Interdisciplinary Description of Complex Systems 20(3), 277-283, 2022

WI-FI 6 APPLICATION IN IOT ENVIRONMENT

Péter János Varga[1] and Zsolt Illési[2,*]

[1]Óbuda University, Institution Kandó Kálmán Faculty of Electrical Engineering
Budapest, Hungary

[2]Milton Friedman University
Budapest, Hungary

DOI: 10.7906/indecs.20.3.7
Regular article

Received: 5 April 2021.
Accepted: 31 December 2021.

ABSTRACT

When thinking of wireless communication solutions for IoT devices, the 5G networking technology is the first thing that comes to mind. Besides this, one cannot overlook the fact that a new wireless communication solution is also available, built on the 802.11ax standard. Until now, wireless networking solutions allowed to manage the simultaneous connections of 250 devices via a single router. Meanwhile, the new technology is designed to support 1024 concurrent connections with one router. This enables the management of a large number of Internet of Things devices in smart homes.

KEY WORDS

Wi-Fi, IoT, security

CLASSIFICATION

JEL: L63, L92

*Corresponding author, η: zsolt@illesi.hu;
Milton Friedman University, 1039 Budapest, Kelta st. 2.

INTRODUCTION

Today, the concept of the Internet of Things or IoT for short, is becoming increasingly widespread. This is not a coincidence, as numerous companies are now producing such devices wordwide.

In a few words, IoT devices, besides two-way communication, can execute specific tasks. They store information in cloud-based systems, and these are available for the users at any time. Based on statistical data, IoT devices are used most in the following areas: manufacturing / industrial, transportation / mobility, energy, retail, cities, healthcare, supply chain, agriculture, buildings.

In 2020 the number of IoT devices reached 50 billion [1]. This means almost 6 IoT devices per person worldwide. Besides the small gadgets surrounding us, there are groups of interrelated devices that should be treated as complex systems. These are smart houses, smart factories, smart grids – intelligent electricity distribution systems, and other extensive networking infrastructures [2].

The primary function of IoT devices is to provide solutions that save time, energy, and money, simplify life and make it more comfortable. The trend of their usage shows that the developers and manufacturers of these devices have successfully achieved this goal.

One of the reasons for this explosive development of IoT is the rapid evolution of the two-way communication solutions needed. These devices can use the following wireless communication protocols: Bluetooth, NB-IoT, Wi-Fi, ZigBee, NFC, LoRa. These technologies are summarised in the following table.

Table 1. IoT Communication Protocol Comparison [3].

Protocol	Frequency	Range	Data Rate	Power Draw	Topology
Bluetooth	2.4 GHz	~ 92 m	125 kbps to 2 Mbps	Low	Point to point, Mesh
NB-IoT	Below 1 GHz	~ 32 km	100 kbps	Low	Star
Wi-Fi	2.4 GHZ / 5 GHz	~ 45 m - 5 km	9.6 Gbps	High	Star, Point to point
ZigBee	2.4 GHz	~ 270 m	250 kbps	Low	Mesh
NFC	13.56 MHz	~ 4 cm	106 kbps to 424 kbps	Low	Point to point
LoRa	150 MHz - 1 GHz	up to 16 km	50 kbps	Low	Star

The table above shows that the various communication solutions can bridge different distances, using different transmission speeds and frequency brands. Accordingly, it follows that these communication technologies supported the proliferation of IoT devices. In the following sections, the relationship between IoT devices and Wi-Fi will be discussed.

RELATIONSHIP BETWEEN WI-FI AND IOT DEVICES

Wi-Fi 4, 5 AND 6

With the introduction of the 802.11ax Wi-Fi standard, these technologies were renamed, including 3 Wi-Fi standards. In 2009 the 802.11n standard was published, supporting the 2.4 GHz and the 5 GHz solutions, with up to 600Mbps theoretical data transfer. This standard was renamed Wi-Fi 4.

In 2013 the 802.11ac standard was published, which further improved both range and data transfer speed. This standard works in the 5 GHz frequency band, up to 3,5 GHz data transfer. This standard is called Wi-Fi 5.

However, standardisation did not stop because wireless devices are responsible for a significant amount of internet traffic. The table above also shows that bandwidth-hungry IoT solutions are among those [4].

Therefore, in 2019 IEEE introduced the 801.11ax standard, a new and innovative version of wireless communication. This standard is called Wi-Fi 6. The following table shows the summary of the three technologies.

Table 2. Comparison of Wi-Fi generations [3].

Feature	IEEE 802.11n	IEEE 802.11ac	IEEE 802.11ax
New name	Wi-Fi 4	Wi-Fi 5	Wi-Fi 6
Channel bandwidth	20, 40	20, 40, 80, 80+80, 160	20, 40, 80, 80+80, 160
Frequency bands	2,4 GHZ / 5 GHz	5 GHz	2,4 GHZ / 5 GHz
Maximum data rate	600 Mbps	3.5 Gbps	9.6 Gbps
Modulation	64QAM	256QAM	1024QAM
Antennas	4x4	8x8	8x8

Wi-Fi SURVEY

The penetration of wireless and IoT technologies is unstoppable. These areas, however, are developing hand in hand. Therefore, we would like to assess some of the impacts and relations of IoT systems from a series of wireless network surveys [5].

Since 2012, we have surveyed the wireless systems on a 29 km route in Budapest. This route was selected to represent all vital urban settings, such as high-rise apartment buildings, suburbs, industrial units, and offices [6]. The following figure shows the survey route:

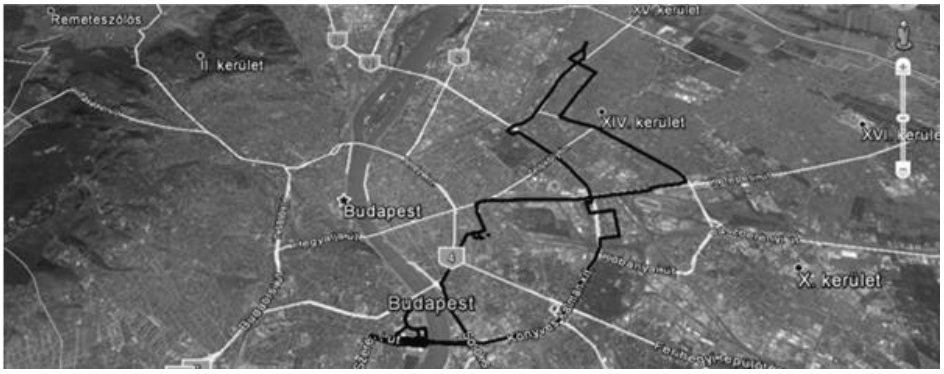

Figure 1. Budapest survey route.

During measurement, up-to-date hardware and software tools were used every time. The hardware environment was a USB connected Wi-Fi device and a GPS receiver unit [7]. The software environment kept changing, depending on the actual operating system and hardware support.

The collected data was compared to the Wireless Geographic Logging Engine (WIGLE) figures to get the overall picture and verify the measured numbers' rationality. WIGLE is an open international database, which shares data about Wi-Fi devices.

The following figure shows the measured and WIGLE data between 2012 and 2020.

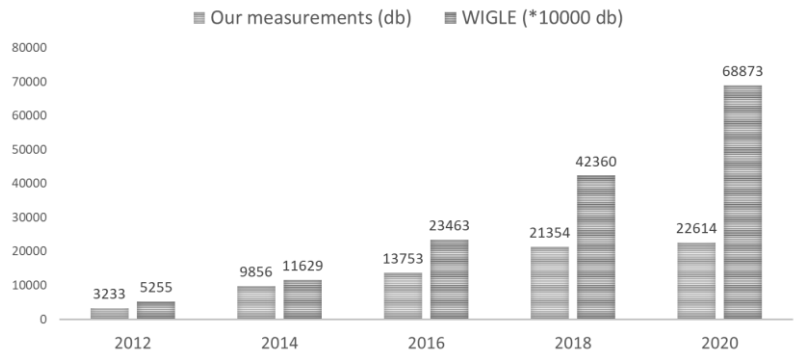

Figure 2. Measured and WIGLE data.

During the survey, not only the number of devices were recorded, but the following transmitted data was also collected [8]: SSID (Service Set Identifier), MAC Address, RSSI (Received signal strength indication), Channel, Channel Width, 802.11 standard,Security and authentication mechanisms, GPS coordinates.

Based on these pieces of information, some trends and wireless network and IoT relations can be concluded. One of the possible benchmarks is the operational frequency based on the measured data. This is important because 2,4 GHz and 5GHz devices can operate with different transfer rates. 2,4 GHz has higher coverage but supports lower, several hundreds of Mbps transfer speed; meanwhile, 5 GHz supports several Gbps transfer speed at a lesser range. The following figure shows the volume trend of 2,4 GHz and 5GHz devices.

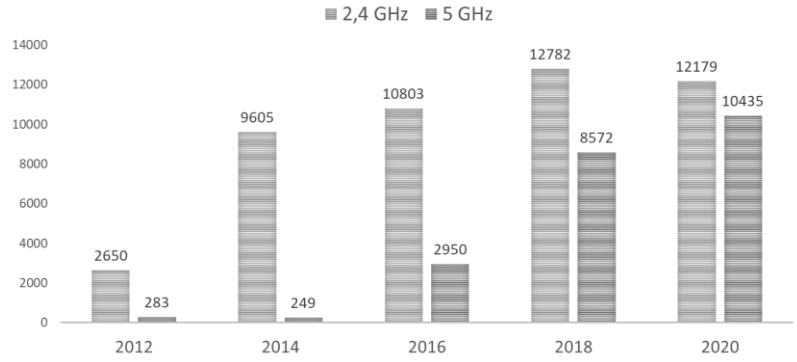

Figure 3. Number of 2,4 GHz and 5 GHz devices.

The survey results indicate that the number of 5 GHz devices increased fivefold in the last four years. This tendency is demonstrated in the following figure, showing the changes in the number of Wi-Fi 4, Wi-Fi 5, and Wi-Fi 6 devices.

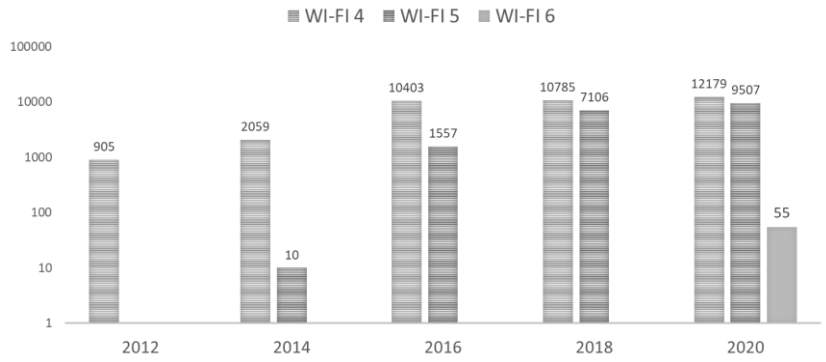

Figure 4. Wi-Fi 4, Wi-Fi 5 and Wi-Fi 6 trends.

The y-axis, on the logarithmic scale, shows the number of devices to highlight the low number of devices when a new technology is introduced to the market. By grouping the data from this perspective, the 2013 introduction and rising of Wi-Fi 5 devices are similar to the Wi-Fi 4 launching tendency, which started in 2012. In our view, Wi-Fi 6 has followed this tendency since its appearance in 2019. After one year of introducing Wi-Fi 5, only 10 of such devices were identified on the survey route. In 2020, one year after introducing Wi-Fi 6, 55 of such technology devices were found. Projecting this trend to IoT devices, it can be concluded that at the increase of the Wi-Fi 6 devices, the number of IoT devices per person can reach 9-10 in the following years.

The survey data also supports defining the number of secure and insecure networks for the overall test population. The following figure shows this trend:

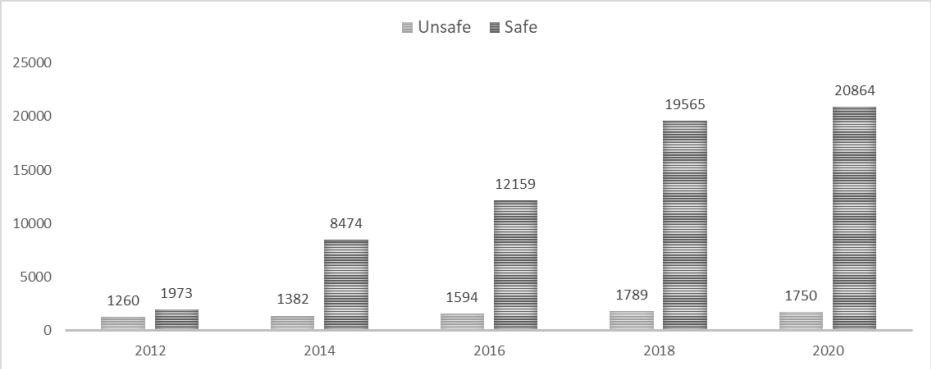

Figure 5. Secure and insecure devices.

Results show that the number of secured-closed-networks has been continually rising since 2012. However, there is another point to remember: in 2020, the number of not secured networks was still 1750. The following figure shows in percentages the changes in the number of secure and insecure networks.

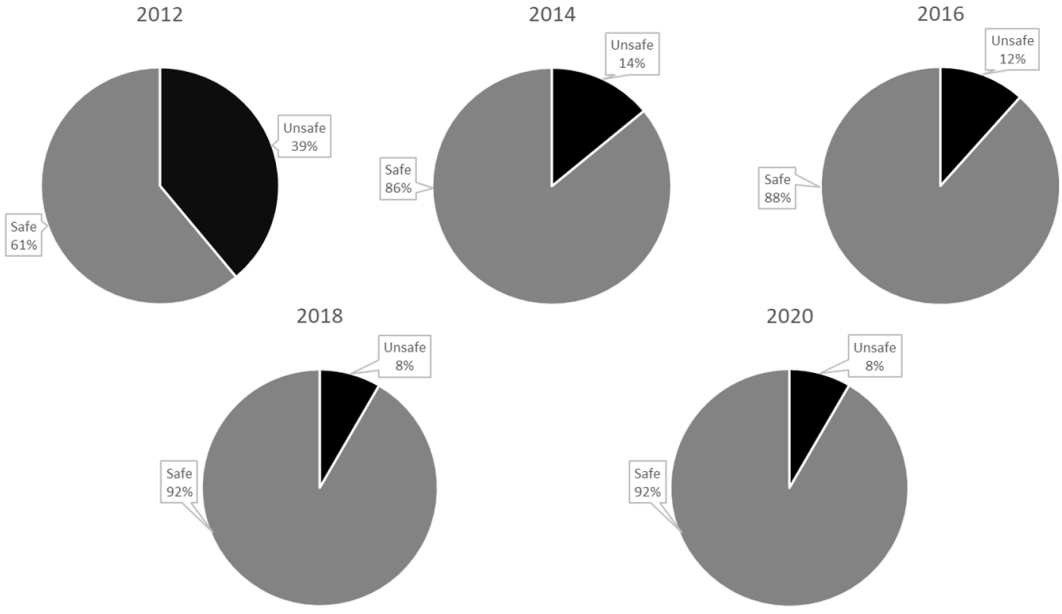

Figure 6. Secure and insecure device percentage.

The above pie charts clearly describe the trend of secure/insecure network proportions from 2012. This figure also shows that in 2020 insecure network had a rate of 8 % in the overall test population. We believe that inadequate configuration and negligence is behind this poor security [9].

Projecting this tendency to the IoT devices, the security of 8 % (4 billion) of the total number of 50 billion devices is managed poorly and can serve as a potential attack point.

OPTIONS TO INCREASE PROTECTION

The spread of insecure Wi-Fi networks and IoT devices increases the potential for attackers to find endpoints, which can be used to launch an attack against critical infrastructures. Based on the technology trends, we can estimate a significant increase in weaponised gadgets in the cyberspace. Mitigation strategies should focus on the end-users, internet service providers (ISPs) and enterprises that employ Wi-Fi networks and IoT devices.

As for end-user protection, there are two main options to nudge people towards a more security-conscious attitude. Firstly, negligence needs to be addressed. Users need to be more aware of the consequences of poorly secured networks and IoT devices by increasing the liability of misconfigured or unprotected devices. However, enforcing legal liability is difficult, especially when most of the users are not technically trained.

There is another option to increase security awareness for IT products by implementing a cybersecurity labelling scheme (CLS). The Cybersecurity Agency of Singapore launched a labelling scheme for smart devices, which identifies four tiers of security assessment [10]:

- tier 1: Security Baseline Requirements,
- tier 2: Lifecycle Requirements,
- tier 3: Software Binary Analysis,
- tier 4: Penetration Testing.

The tier sequence corresponds to the increasing level of assurance and improved cyber resilience. This model informs the public about the security resistance of devices and increases manufacturers' competition to develop more secure appliances.

CONCLUSIONS

The evolution of smart devices increased network utilisation in both households and enterprises. We have been collecting data about Wi-Fi systems in Budapest since 2012, by scanning devices connected to them, in order to be able to assess the used technologies. In this article, we presented some utilisation trends. Based on the strongly coupled development of Wi-Fi networks and IoT devices, we showed how Wi-Fi 4, Wi-Fi 5 and Wi-Fi 6 transition happens, and what are the tendencies in change of the secure/insecure proportions of these devices. We pointed out that future IoT consumption will increase the number of misconfigured or poorly configured devices, which will increase the potential to use these against critical infrastructure. We also pointed out that some action was needed to raise the security awareness of end-users and manufacturers to reduce operational negligence.

REFERENCES

[1] Knud, L.L.: *State of the IoT 2020: 12 billion IoT connections, surpassing non-IoT for the first time.* http://iot-analytics.com/state-of-the-iot-2020-12-billion-iot-connections-surpassing-non-iot-for-the-first-time, accessed 25th November 2020,

[2] Pető, R. and Tokody D.: *Building and operating a smart city*. Interdisciplinary Description of Complex Systems **17**(3-A), 476-484, 2019, http://dx.doi.org/10.7906/indecs.17.3.6,

[3] Wisilica: *Top 6 IoT Communication Protocols.* Wireless Communication Protocols, 2020, http://wisilica.com/company/top-6-iot-communication-protocols , accessed 25th November 2020,

[4] Haig, Zs.: *Cyber information.* In Hungarian. Dialóg Campus Kiadó, Budapest, 2018,

[5] Farkas, T. and Parada, I.: *Reporting and analysis and penetration testing - 1. Information technology.* In Hungarian.
Hadmérnök **15**(1), 159-182, 2020,
http://dx.doi.org/10.32567/hm.2020.1.11,

[6] Pokorádi, L.K.; Boucetta, S.I. and Johanyák, Z.C.: *Survey on software defined VANETs*.
Gradus **4**, 272-283, 2017,

[7] Sostaric, D.; Mester, G. and Dorner, S.: *Mobile ECG and SPO2 Chest Pain Subjective Indicators of Patient with GPS Location in Smart Cities*.
Interdisciplinary Description of Complex Systems **17**(3-B), 629-639, 2019,
http://dx.doi.org/10.7906/indecs.17.3.17,

[8] Rajnai, Z. and Albininé Budavári, E.: *The role of additional information in obtaining information*.
Interdisciplinary Description of Complex Systems **17**(3-B), 438-443, 2019,
http://dx.doi.org/10.7906/indecs.17.3.2,

[9] Albini, A.; Tokody, D. and Papp, J.: *IT Infrastructure Informatics Security Aspects.* In Hungarian.
Bánki Közlemények **1**(1), 11-16, 2018,
http://dx.doi.org/10.21825/agora.v16i2.9646,

[10] Cybersecurity Labelling Scheme (CLS) For Manufacturers: *Cybersecurity Levels & Assessment Tiers.*
http://www.csa.gov.sg/programmes/cybersecurity-labelling/for-manufacturers.