# Creating a security conscious IoT ecosystem with innovative monitoring and classification solutions

**Márk Tamás Baross[1] and Péter János Varga[2]**

[1] Doctoral School on Safety and Security Sciences, Óbuda University, 1034 Budapest, Bécsi út 96/B, H-1034 Budapest, Hungary; baross.mark@uni-obuda.hu

[2] Óbuda University, Kando Kalman Faculty of Electrical Engineering, Bécsi út 96/b, H-1034 Budapest, Hungary; varga.peter.janos@uni-obuda.hu

*Absztract: The Internet of Things (IoT) is one of the most dynamically developing areas of technology today. In IoT systems, everyday devices—such as smart home appliances, industrial sensors, and medical devices—are connected to a network and collect and exchange data with each other. However, the spread of these technologies also carries a number of security risks. The aim of this doctoral thesis is to provide a comprehensive overview of the security challenges of IoT systems and to show how effective protection and monitoring solutions can be developed. In my research, I examine how different security classes can be created and how they can be adapted to IoT devices with limited resources. In addition, I aim to develop a test sample measurement that helps classify devices into the security classes I have defined. The research also includes the design of a spectrum monitoring environment capable of continuously monitoring and evaluating the communication processes of IoT networks and identifying any anomalies. The developed system enables the automatic detection and classification of disruptive, faulty, or suspicious devices, thereby contributing to the increased reliability and security of IoT infrastructures. The results of the dissertation are expected to contribute to the development of a decision support framework that will enable developers and operators to improve the security level of IoT systems in a measurable and targeted manner. The results of the dissertation contribute to the development of a decision support framework that helps developers and operators improve the security level of IoT systems in a measurable and targeted manner.*

*Keywords: IoT; IIoT; safety; communication; reliability*

# 1 Frequency bands used by Internet of Things systems

The basis for the operation of Internet of Things (IoT) systems is ensured by the efficient and targeted use of various radio frequency bands. IoT devices rely heavily on ISM (Industrial, Scientific and Medical) frequency bands, as these are globally available and allow license-free use. The 433 MHz band is primarily used for communication between simple, low-data-rate sensors and is well suited for indoor applications. In Europe, the 868 MHz band plays a key role in the operation of LPWAN networks preferred by LoRaWAN and Sigfox technologies, while in North America, the 915 MHz range provides similar technical conditions. The 2.4 GHz ISM band, as the primary medium for Wi-Fi, Bluetooth, and Zigbee systems, supports high-speed but shorter-range communication, but is subject to significant interference due to heavy use. [1]

Mobile network-based IoT technologies such as NB-IoT and LTE-M typically use LTE bands around 700 MHz, 900 MHz, and 1800 MHz, which provide excellent coverage and penetration. Thanks to its narrowband mode, NB-IoT enables extremely low energy consumption, making it ideal for long-life, mass-deployed infrastructures. In contrast, LTE-M's higher data capacity makes it the optimal solution for mobile devices and applications requiring real-time data transmission. The latest 5G networks have further expanded the IoT frequency spectrum, offering solutions ranging from low bands at 700 MHz to mid-bands at 3.5 GHz and even the 24 GHz to 60 GHz mmWave ranges. The 3.5 GHz band is particularly important in industrial automation environments, where low latency and high data rates are critical requirements. [2]

The spectrum of frequency bands used in IoT systems is constantly expanding, with one of the latest steps being the opening of the 6 GHz range for Wi-Fi 6E and later generations, which significantly reduces congestion in the 2.4 and 5 GHz bands. In addition, other lesser-known bands are also available in certain regions: the 169 MHz band is primarily used for smart meter communication, while the 315 MHz band can be used by short-range, low-power IoT devices. Frequency selection therefore depends largely on the specific application environment, the expected energy efficiency, the desired data rate, and coverage requirements, the coordinated optimization of which is a fundamental prerequisite for the development of highly reliable and sustainable IoT infrastructures. [3]

Table 1
IoT technologies frequency bands

| Technology | Frequency band | General features |
|---|---|---|
| LoRaWAN | 433 / 868 / 915 MHz | Long range, low energy |
| Sigfox | 868 / 902 MHz | Very low data rate |
| Wi-Fi | 2.4 / 5 GHz | High data rate, energy intensive |
| Bluetooth (BLE) | 2.4 GHz | Short range, low energy |
| Zigbee | 2.4 GHz | Short-medium range, mesh network |
| NB-IoT / LTE-M | 700–900 / 1800 MHz | Mobile network IoT, wide coverage |
| 5G IoT | 700 MHz, 3.5 GHz+ | High data rate, industrial applications |

Overall, IoT system communication is based on the targeted use of different radio frequency bands, which provide the optimal combination of range, data speed, and energy efficiency to meet different technological needs. ISM bands (433 MHz, 868/915 MHz, 2.4 GHz) play a key role in license-free, low-energy, short- to medium-range solutions, while mobile network and 5G technologies offer a wide spectrum for high-coverage, industrial, and real-time applications. Coordinated optimization of frequency selection is a fundamental requirement for the development of reliable and sustainable IoT infrastructures.

# 2 Implementation of the Internet of Things in terms of critical infrastructure and public use

The integration of IoT technologies is playing an increasingly important role in both critical infrastructure and various areas of civil use, as they enable real-time data collection, intelligent decision support, and autonomous operation. In the field of critical infrastructure, IoT is particularly important in maintaining the stability and reliability of energy and public utility services. Modern smart grid systems are capable of continuously monitoring and optimizing the load on the electricity grid in real time, while automatically detecting faults and anomalies affecting the grid. In water supply and wastewater treatment systems, IoT-based

sensors are key to accurately measuring water quality, water pressure, and infrastructure load, thereby increasing system safety and efficiency. [4]

The digitization of transport and logistics infrastructures is also fundamentally shaped by IoT technologies. Intelligent transport systems, for example, use adaptive traffic lights that can respond to traffic conditions in real time, thereby reducing congestion and fuel consumption. In addition, bridge and road monitoring systems rely on sensor networks to measure structural loads, changes in condition, and signs of potential damage, thereby preventing accidents and infrastructure deterioration. In the healthcare sector, IoT plays a key role in improving the efficiency of patient care, as remote patient monitoring systems enable continuous monitoring of vital functions, while automated medication tracking systems ensure the availability of critical supplies.

The application of IoT in military and defense infrastructures is of strategic importance, as modern warfare relies heavily on real-time information gathering and precise decision-making. Battlefield sensor networks are capable of detecting movements, continuously monitoring the environment, and supporting situational awareness using a wide range of communication technologies. The frequency bands used include 433 MHz, 868 MHz, 915 MHz, and UHF/VHF bands reserved for military purposes. Autonomous vehicles and drone platforms rely on IoT-based communication to perform reconnaissance, logistics, and support tasks, and target tracking and status monitoring are also featured in integrated weapon systems. Encrypted IoT communication increases the reliability of the chain of command, while cybersecurity IoT systems are capable of quickly detecting intrusions, network anomalies, or hostile activities. However, military IoT also carries significant risks, with cyber warfare threats, GPS spoofing and jamming techniques, and supply chain vulnerabilities all posing serious threats to system integrity and operability. [5], [6]

In general civilian use, IoT technologies primarily increase the convenience and efficiency of everyday life. Smart home systems, including networked lighting, smart thermostats, and security cameras, operate on globally available 2.4 GHz and 5 GHz Wi-Fi and Bluetooth Low Energy communication bands. Wearable devices, such as smart watches and health monitors, continuously collect data to maintain human health and improve users' quality of life. Parking sensors, air pollution monitoring stations, and traffic information systems play an important role in smart city infrastructure, typically using 868 MHz, 915 MHz, or LTE-M and NB-IoT mobile network frequencies. Industrial IIoT solutions provide significant economic and efficiency benefits in predictive maintenance, process optimization, and automated manufacturing chain operations, often using bands below 6 GHz and around 3.5 GHz for low-latency communication. [7], [9]

Table 2
Areas of IoT application

| Area | Examples | Risks |
|---|---|---|
| Critical infrastructures | Smart Grid, Water network sensors, Smart transportation systems, Health monitoring | Cybersecurity threats, Data protection issues, System failure with serious consequences |
| Military applications | Battlefield sensor networks, Drones, Autonomous vehicles, IoT integration of weapon systems | Cyber warfare and hacker attacks, GPS spoofing/jamming, Supply chain vulnerability |
| Public use | Smart homes (thermostats, lighting), Wearable devices, Smart cities, Industrial IoT | Data leaks, Device vulnerabilities, Privacy violations |

Overall, the implementation of IoT results in an extremely heterogeneous, complex, and rapidly evolving ecosystem for both critical infrastructure and civilian applications, the operation of which can be ensured and secured by a coordinated system of appropriate communication protocols, frequency bands, and security solutions.

# 3 Implementation of a system suitable for testing and its potential uses

IoT systems have become a defining feature of our everyday lives and work environments, providing intelligent and networked operation in a wide range of areas, from home automation to industrial process optimization. Parallel to this phenomenon, assessing the security of IoT devices and classifying them into security categories has become an extremely complex task, as the heterogeneous technological background, diverse communication protocols, and large number of devices pose significant challenges in terms of maintaining cybersecurity and network integrity. My research goal is to make IoT security measurable and uniformly classifiable, which can provide a methodological basis for objectively determining risk levels and comparing different IoT systems. [8]

In our work, we place particular emphasis on developing innovative monitoring and decision support solutions that are capable of detecting and evaluating the communication environment of IoT systems in real time. The goal is to create a complex measurement system that continuously monitors the radio frequency spectrum and is able to detect network anomalies, interfering or malfunctioning devices, and potentially suspicious or hostile activity in a timely manner. The spectrum analysis-based approach enables the recognition of various IoT communication patterns, the identification of traffic anomalies, and the detection of new or unauthorized devices appearing in the environment.

The measurement environment is designed specifically to perform monitoring and testing functions on a continuous and long-term basis, as well as in ad hoc locations for shorter periods of time.

Meanwhile, the evaluation modules are capable of analyzing temporal changes in spectral data and drawing reliable conclusions based on them. My ultimate goal is to create an integrated hardware and software environment that is suitable for the continuous, automated testing of IoT systems, the mapping of system-level security risks, and the operation of early warning mechanisms that support network security. This approach can contribute to the reliability, resilience, and sustainable operation of future IoT infrastructures.

The systems shown in the image below were developed using SDR (Software Defined Radio) based devices. A special consideration was given to selecting SDR equipment capable of monitoring the frequency bands mentioned above. Thus, the systems were designed using the Ettus B210 USRP device, which is capable of performing this task from 70 MHz to 6 GHz, which is suitable for the frequency bands used by IoT technologies.

Figure 1

Rack unit inspection environment

Figure 2

Portable inspection environmentSummary

The measurement and monitoring system developed during the research contributes significantly to increasing the security and reliability of IoT networks, as it enables the detection of individual devices exhibiting undesirable, abnormal behavior or posing a potential threat through real-time spectrum analysis. The technological solution created can also provide the basis for the development of a decision support framework that helps operators respond quickly and appropriately. Thanks to its flexible design, the system can be used effectively in industrial environments, healthcare infrastructures, and smart home systems, giving it a wide range of applications.

The research results confirm the hypothesis that it is possible to develop an installable and portable complex ecosystem that is suitable for in-depth examination of IoT systems and can be used to identify unwanted devices and communication sources that may pose a critical security risk. The system's capabilities enable early detection of potential threats, subsequent tracking of compromised devices, and identification of processes that compromise network integrity. All of these factors contribute to reducing security risks alongside the spread of IoT technologies and enable the implementation of reliable, data-driven protection mechanisms that can be used in the future.

## References

**[1]** A. S. Malik, M. A. Khan and M. S. Farooqi, “Internet of Things: Challenges, Advances, and Applications,” *IEEE Access*, vol. 9, pp. 61785–61803, 2021, doi: 10.1109/ACCESS.2021.3074035.

**[2]** E. Sisinni, A. Saifullah, S. Han, U. Jennehag and M. Gidlund, “Industrial Internet of Things: Challenges, Opportunities, and Directions,” *IEEE*

*Transactions on Industrial Informatics*, vol. 14, no. 11, pp. 4724–4734, Nov. 2018, doi: 10.1109/TII.2018.2852491.

**[3]** S. Sicari, A. Rizzardi, L. A. Grieco and A. Coen-Porisini, "Security, Privacy and Trust in Internet of Things: The Road Ahead," *Computer Networks*, vol. 76, pp. 146–164, 2015, doi: 10.1016/j.comnet.2014.11.008.

**[4]** P. Porambage, A. Braeken, M. Liyanage and M. Ylianttila, "Security and Privacy in Distributed IoT Systems," *Future Generation Computer Systems*, vol. 123, pp. 230–249, 2021, doi: 10.1016/j.future.2021.04.009.

**[5]** R. Anderson and S. Fuloria, "Security Economics and Critical National Infrastructure," *IEEE Security & Privacy*, vol. 8, no. 1, pp. 12–23, Jan.–Feb. 2010, doi: 10.1109/MSP.2010.11.

**[6]** NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), *Internet of Things in the Context of Military Operations*, 2020. [Online]. Available: https://ccdcoe.org/library/publications. [Accessed: Sept. 13, 2023].

**[7]** D. Evans, *The Internet of Things – How the Next Evolution of the Internet Is Changing Everything*, CISCO White Paper, 2011. [Online]. Available: https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf. [Accessed: Sept. 13, 2023].

**[8]** J. Gubbi, R. Buyya, S. Marusic and M. Palaniswami, "Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions," *Future Generation Computer Systems*, vol. 29, no. 7, pp. 1645–1660, 2013, doi: 10.1016/j.future.2013.01.010.

**[9]** M. Z. A. Bhuiyan, G. Wang, M. F. Zolkipli, J. Cao, H. Li and T. Chen, "Energy-Efficient Security for Wireless Sensor Networks in Critical Infrastructures," *IEEE Communications Magazine*, vol. 53, no. 1, pp. 48–55, Jan. 2015, doi: 10.1109/MCOM.2015.7010518.