# Internet of Things or Surveillance of Things?

Petr Doucek, Antonin Pavlicek, Ladislav Luc



# Internet of Things or Surveillance of Things?

Petr Doucek, Antonin Pavlicek[0000-0002-1230-5982], Ladislav Luc

University of Economics W. Churchill sq. 4, Prague, Faculty of Informatics and Statistics, Czech Republic
{doucek,antonin.pavlicek,ladislav.luc}@vse.cz

**Abstract.** The paper deals with digital surveillance in the postmodern world. We define a new term 'Surveillance of Things' in the context of the study of the surveillance, and try to determine, whether and how the surveillance of people is connected with surveillance of things. We pay particular attention to the Internet of things and analyze in detail the principles of Sigfox network.
We work on the presumption that information about people obtained through surveillance of things are interpreted incorrectly and can have a direct impact on groups of people and also individuals.

**Keywords:** Internet of Things, Surveillance of Things, Sigfox.

## 1 Introduction

Surveillance studies are not a young scientific discipline, yet they have been enjoying an unprecedented development lately. With the advent of digitization, miniaturization, and the Internet, substantial cultural and social changes have taken place and the surveillance has been adapted, changed its structure and organization.

Surveillance studies in a traditional concept are primarily focused on human resources – including the individuals, the family, the whole social entity, the interest groups, the states, etc. They study causes and consequences of supervision, mutual interaction of individuals and groups, their opinions, feelings, social inclusion, culture and countless other aspects across many disciplines.

Nowadays people are used to the fact that they are being watched from time to time and that they leave their digital footprint on cell phones, computers and computer networks. People are even actively involved in their own monitoring: they voluntarily give up some private information, and surveillance systems count on their cooperation (Facebook, Google etc.). A DIY-style surveillance was born, transferring the burden of monitoring and the associated responsibility for supervising to individuals themselves [1].

Perhaps the biggest novelty is that monitoring of people begins to be achieved through digital monitoring of things.

### 1.1 Internet of Things (IoT)

If we are looking for a platform where we can monitor things en masse, the Internet seems to be a great choice. The Internet itself is a great tool of supervision and, in essence, has made it possible for surveillance to become conspicuous. But the current Internet as we know it is primarily an 'Internet of Users'. For monitoring things, we need a platform that can handle many more orders of entities than the technological limits of the current Internet network allow. It is not practically conceivable for all postal packages, water or gas meters, light switches, or merchandise items in the shops to be Internet-connected. Internet protocols do not allow to connect directly such a great number of devices that can move freely for a long time without fixed wires. But new networks are emerging to bridge the divide between the Internet of Users and Internet of Things [2, 3].

The Internet of Things (IoT) can be defined as a dynamic global network based on standardized protocols where physical and virtual things have their identity, physical attributes, and virtual personalities. It is expected that things integrated into IoT become active participants in trade, information, and social processes, allowing them to communicate with each other and with their surroundings. These integrated things can independently respond to events and trigger processes even without direct human intervention [4].

### 1.2 Surveillance of Things (SoT)

As we mentioned at the beginning of the paper, the surveillance studies in the traditional concept focus mainly on people. For the purposes of this work, we define a new concept that will express the principles of monitoring (in the context of Surveillance Studies), in which surveilled or surveilling subject is a non-human thing. We also include combined cases where a supervisor is a person watching things and vice versa.

*Surveillance of Things (SoT) means a focused, systematic and routine attention to data about things – collected and analyzed in order to influence, manage, protect and monitor them.*

"Things" in the context of supervising things can be understood as physical and virtual entities that exist in space and time and can be identified.

### 1.3 Ownership of Things

Ownership of things has been one of the key aspects of the development of SoT. If things are to be possessed (and keep in mind, that possession is considered to be nine-tenths of the law), it means we have to ensure their inviolability. We must have some power over our things, have them under the sovereign control, we must have the ability to prove and defend our property when disputed or stolen. In order to achieve this, we need to be aware of their whereabouts, keep them under surveillance. Even though the right to own things is guaranteed by the modern state, in practice we still have to deal with security individually. One of the security features is monitoring or surveillance.

We also began to use SoT techniques to track things that do not belong to us, but for some reason, we are interested in them.

There have recently been new reasons and needs for tracking things through new technical possibilities and social changes within society.

### 1.4 The degree of tracking things

The degree of tracking of things could be seen on two levels. First, quantitatively, the number of things and the number parameters we can monitor. Secondly, in terms of quality, the depth and complexity of the tracking we perform (whether the tracking is done with all relevant aspects).

Since we are dealing with digital surveillance, we also need to take into account the aspects of digitization. Let us first mention the first Manovich's [5] principle of numerical representation, from which we can infer that the digital tracking is discrete. For example, digital video-recording may seem to be continuous, but it is not. In fact, it is just a stream of individual pictures taken at the rate of 25 shots per second. For normal human activities, it is unlikely that a person would do anything significant in a time span shorter than 33 ms.

However, the situation is different for monitoring things. Things can be very fast in both movement and change (for example a fired bullet). With virtual things, the situation is even more difficult. In the virtual environment, we can even reach the physical boundary of Planck's time. (What happens in a shorter time span than Planck's time (tP) is not physically apparent).

$$t_P \equiv \sqrt{\frac{\hbar G}{c^5}} \approx 5.39124(27) \times 10^{-44}\ \mathrm{s} \tag{1}$$

For our needs, however, it is sufficient to conclude that digital surveillance is discrete and, for SoT, the sampling frequency becomes an essential variable.

## 2 Technical aspects of SoT

When compared to humans, things behave highly predictable, since they lack their own intelligent thinking. Things can be easily parameterized, described and identified. A special category is the existence of virtual things; items without their physical representation in the real world. Things are similar to people in having a life cycle. Two technical aspects (problems) are essential for the purposes of this work.

The first technical problem is the fact that there are many times more things than humans. There would be nothing special about that, but the amount of the things being watched is exponentially growing. Buyya and Dastjerdi [6], in their book Internet of Things, in accordance with McKinsey's estimate that around one trillion devices will be connected to the network by 2025. And here comes the trouble - traditional mobile networks, such as 2G, 3G, LTE, are not capable of handling such huge number of connected things.

The second technical problem is that things can move freely. It is quite easy to monitor things in a fixed perimeter, but the problem occurs when they are geographically unstable or they are moving all the time. Mobile networks cover a large part of the mainland, but the terminal devices require a relatively large amount of electricity to operate.

The answer to these technical problems is building communication platforms dedicated to IoT.

### 2.1 IoT Trends

Let's see how IoT is perceived by leading technological companies:

─ Samsung predicts further growth in IoT technologies, with the IoT market volume reaching USD 1.7 trillion by 2020. Samsung provides a solution in IoT and supports NB LTE and LoRa technologies. [7]

─ Computer giant HPE (Hewlett-Packard Enterprise, formerly HP) is developing a product called the "HPE Universal IoT Platform" to connect a variety of different IoT technologies and manage their lifecycle. HPE forecasts that in the year 2020, the amount spent on IoT hardware alone will reach USD 3 trillion.[8]

─ Another world technological leader, IBM predicts the value of the economic potential of IoT at USD 11 trillion in 2025. [9]

─ Microsoft has been working in the IoT area for a long time and provides a full range of IoT products. From software and solutions for end-to-end devices to cloud-based platforms that provide comprehensive IoT operation. [10]

─ From Czech companies, we can name ČD - Telematika, which offers its own concrete solutions in the field of IoT. [11]

─ Similarly, other companies like Google, Amazon, Dell, or Cisco are actively engaged in the world of IoT.

### 2.2 IoT for SoT

The cornerstone of the Internet of Things is secure two-way communication of a large number of things anywhere, anytime. Contrary to that, one-way communication thing ➔ supervisor is sufficient for SoT, provided that the subsequent stimulus from supervisor will be communicated through another channel.

Practical implementation of IoT must, therefore, ensure ubiquitous connectivity. The supervisor's goal is to be able to keep track of the things as continuously as possible – by systematic and continuous monitoring without failures (with respect to the discrete nature of digital surveillance). Any gap in tracking leaves room for speculation and the possibility of questioning the “pedigree” of monitored things. And let us remind, that for complete global coverage, there is a quite substantial space (the world as we know it and commonly use - the land, underground, water areas, and airspace within the reach of conventional commercial aircraft) to be covered.

In order to monitor things, a considerable degree of autonomy of the monitored things must be ensured. Having things constantly connected to the network (both electricity and data) is impractical and expensive, making it impossible for them to move

easily. A properly dimensioned wireless power supply and data connectivity need to be solved.

However, in addition to the above, the viability of SoT depends also on the following criteria: economic aspects, miniaturization, restrictive legislation, increasing complexity - increasing number of connected elements in the network.

## 3 Sigfox – IoT solution for SoT

One possible solution for IoT is the French project Sigfox. Sigfox builds a brand new network dedicated to the Internet of things. As of May 30, 2016, the Sigfox network was available in 18 European countries and covered an area of 1.2 million km$^2$ [12]. In the Czech Republic, Sigfox has established a partnership with SimpleCell Networks, which has contracted T-Mobile Czech Republic (TMCZ). TMCZ is actually building the Sigfox Network for the Internet of Things [13]. By the end of 2016, more than 350 base stations were connected to the network, covering roughly 3 × 95% of the Czech Republic's territory, and further expansion is planned to increase reliability. The situation illustrate the coverage maps of the Czech Republic and Europe of May 2017, see Figure 1.

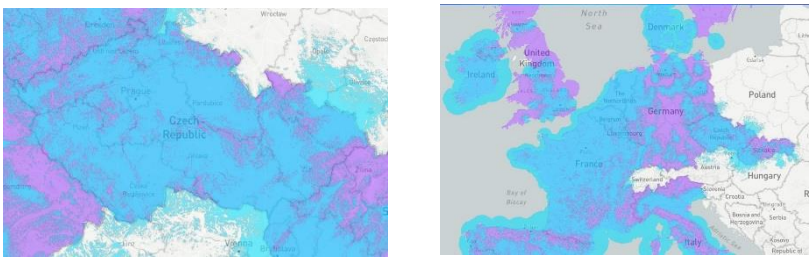


**Fig. 1.** A coverage of Sigfox network in the Czech Republic and Europe – as of May 2017. (http://www.sigfox.com/en/coverage)

### 3.1 Sigfox connectivity

In this chapter, we will get closer look how Sigfox works to meet the requirements for SoT. The aim is not to describe the technical details, but to introduce this specific IoT solution.

The Sigfox wireless network operates at 868 MHz, an unlicensed but regulated frequency. Thanks to that no licensing neither authorization is needed, but the country-specific arrangements must be respected. The Decree R/10/05.2014 enforces the limits within the Czech Republic. The Decree states inter alia that the maximum transmitting power should be only 25 mW [14]. This is the same bandwidth and power we commonly use in remote controllers to open garage doors. However, the Sigfox transmission signal is directed to a very narrow beam, providing connection within a direct visibility of up to 200 km (a practical test performed by TMCZ repeatedly succeeded in

connection between the highest mountain of the Czech Republic, Snezka and Prague – which are 120 km apart), declared reach in the populated area is 5-30 km.

A maximum of 140 messages per day can be sent from the Sigfox device (in other words - the device can send a message every ten minutes). The device can receive up to 4 messages per day. These parameters are strictly legislatively enforced, see the CTU Decree, technology itself allows to broadcast almost continuously.

However, the size of one message is quite tiny - only 12 bytes of user data plus some technological information (for example device battery status, etc.) as well as headers with message identifiers. The entire message is encrypted with an AES-128 certificate before sending.

The device sends the message repeatedly three times in a row and does not monitor, whether a base station received it. After a broadcast, the device powers off to wake up just before the next message is ready to be broadcasted. When the device is in the sleep mode, it is not possible to contact it remotely.

The sent message is received by the base stations. Sigfox assumes that each geographic location should be covered at least three times in order to increase the likelihood of receiving the message.

The mobile operator places Sigfox base units at standard locations (masts) next to the traditional mobile phone technology. From mobile operator's point of view, the system is complete "black box" - the device works completely autonomously, sending data through encrypted VPN tunnels to the Sigfox headquarters in France. The Sigfox network headquarters is a cloud platform. Data is preprocessed and ready to be sent to users (from the IT architecture point of view it is a back end). Users can connect to the cloud platform via either a web interface or they can use third party applications that connect to the Cloud Sigfox through the API.

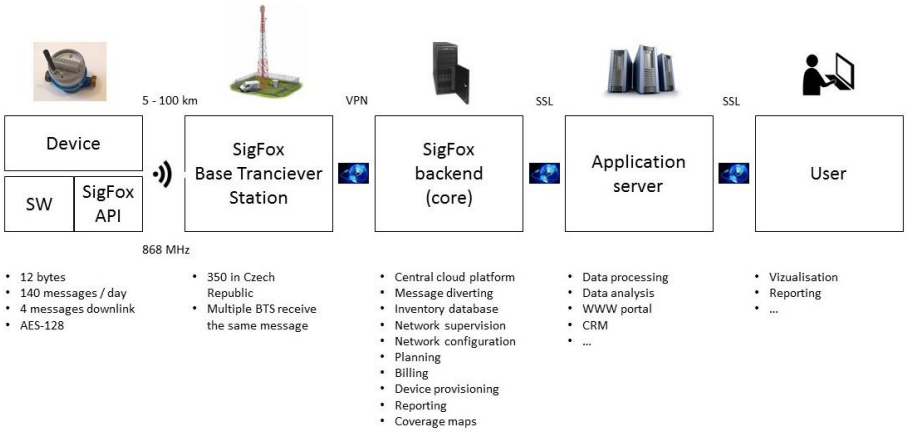


**Fig. 2.** Message transmission over Sigfox network

### 3.2 Sigfox devices

Sigfox terminal devices consist of three main parts. The first part is Sigfox modem with the antenna. This module (usually a printed circuit or a chip of several square centimeters in size, with a unique ID - similar to a SIM card) is responsible for sending and receiving messages. In the second part are the sensors – can be practically any digital detector – e.g. sensors of temperature, humidity, air pressure, sound and vibration, flowmeter, sensor of chemical states and gas states, pressure gauge and weight sensor, fluid detection and fluid level measurement, magnetic sensor, acceleration sensor, light and optical sensor, GPS, motion sensors, position change sensor, … The third major part is the battery.

The Sigfox modem is designed to have extremely low power consumption. The whole device is designed to last for a long time without a battery replacement. For example, to measure daily the temperature around the device, ie send one message a day with the user's temperature information, the device can last for more than fifteen years. But energy-intensive user device (such as a GPS module) or high message frequency decrease the battery life.

The Sigfox is a half-open concept. The chip is available to any regular user to make amateur devices with just the right equipment. Professional modules can be made by any company without need of Sigfox license.

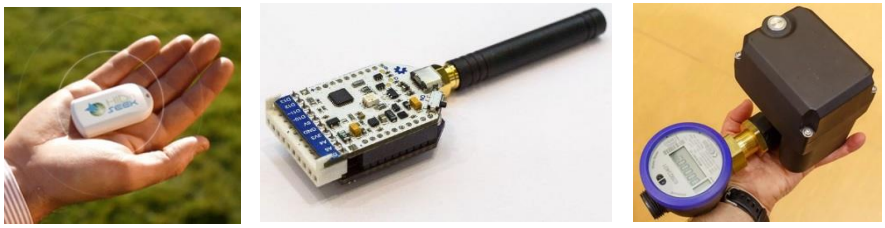

**Fig. 3.** Sigfox devices (https://www.cnet.com/devices-for-sigfoxs-super-cheap-network)

### 3.3 Examples of using Sigfox technology

Sigfox is best suited for use in situations where we need a long-running, autonomous system that provides regular or event generated information of low data volume. The technology has an excellent reach and can be deployed both in natural and urban agglomerations. Moreover, Sigfox's cloud concept is not limited by state borders. Devices purchased and paid in the Czech Republic will work equally well in France or the UK. There are no extra roaming fees. The system is quite robust, it has been designed to handle up to hundreds of millions of devices.

Sigfox solution does not provide information in real time – there is slight delay within one minute, so the system is "near online". The system is not designed as highly reliable. In practice, some messages are not received and there is no feedback (with the device). Sigfox does not suit even fast movement due to Doppler effect. However, the practice has shown that movement in motorway speeds will not affect functionality, a flying plane is problematic.

Specific use cases are still being devised. For some solutions, there is already a pilot study in operation. A feasibility study is being developed. Of the existing ones, let us mention at least some of them:

- Remote readings of water meters, gas meters, heat sensors on radiators and the like (smart metering);
- Electronic seals;
- Flood sensors;
- Environmental measurements (temperature, pressure, humidity, air quality, river level);
- Waste management (dustbin alerts the collection agency being full);
- Sensors of parked cars (placed directly under the asphalt);
- Shock sensors on bridge structures;
- Availability of meeting rooms ("digital company" concept);
- Soil quality (can be buried in soil and monitor soil moisture, composition, pH, etc.);
- Tracking of consignments, containers or livestock and the like (GPS tracking technology);
- Remote health monitoring.

## 4 Case studies: IoT in the Czech Republic

IoT is not a newcomer with the arrival of Sigfox in TMCZ. Previously, there were also systems called M2M (machine to machine) built on 2G, 3G, LTE, and the like. They serve primarily for corporate clients and were usually built as tailor-made customer solutions. We can include, for example, connection of ATMs and payment terminals, MeR (measurement and control) systems, or corporate fleet management systems. With Sigfox, however, it is a dedicated network for IoT, and TMCZ will have to form another strategy, invent new products and run traffic.

IoT still does not have a defined world standard. There are other technologies (ie LoRa) on which IoT can be built. From this perspective, Sigfox can be considered as an uncertain project.

### 4.1 Alternatives to the Sigfox network

As mentioned, the global IoT standard does not yet exist and Sigfox is not the only platform for the Internet of Things. In the Czech Republic, CRA (České Radiokomunikace a.s.) is also trying to build a network for the Internet of Things.

LoRa technology is technically and strategically different from Sig-Fox technology. The LoRa operator can be anyone. The city may decide to build its IoT on its territory fully under its management. With LoRa it is possible. But there is only one specific company, which can produce a proprietary chip. LoRa has its pros and cons, but the intention and purpose are the same. The ability to connect millions of devices to a network of things. Identical are therefore cases of use.

Another system, which can be used for IoT, is a system based on LTE technology - LTE M.

### 4.2 Case studies - Sigfox technology from the SoT perspective

Sigfox meets the basic definition of surveillance because many uses (such as Sigfox in combination with GPS) are concentrated, systematic and routine attention to data about things to influence, manage, protect and route them. By providing supervision, we also provide factual power over things and consolidate the principle of ownership.

Sigfox is a highly centralized database on a pan-European scale that associates information from all connected devices in one place under the supervision of a single organization. Sigfox allows you to convey information about a particular thing and to make whole pedigree of things, for example in agriculture [15] or energy industry [16].

Imagine an apple orchard. The farmer has installed sensors of humidity, Ph level, sunshine, and the like. The nearby apiculture company has honeybee sensors installed in its hives. Growing fruits have been monitored since birth, and even though the farmer cannot see the beekeeping company's data (and vice versa); this information may come together at the Sigfox headquarters. After harvest, a logistics company is using the GPS tracking device, the apple is once again monitored – as it goes to the vendor's warehouse – where its environment is again monitored. When someone orders the delivery of apples on the internet, Sigfox logistics company can transport them again. None of these companies see each other in the data but in Sigfox they know that the apple has grown under the specific conditions when it was harvested, knowing how much it weighted, where it went, how long and under what conditions it was stored and eventually where it was taken by the consumer - including address). Such pedigree of things of unprecedented proportions is feasible today.

The practical applicability of Sigfox tracking technology is evidenced, for example, by the pilot operation in the TMCZ implementation demanded by Václav Havel Airports in Prague. The airport considered Sigfox tracking of luggage trolleys – passengers leave carriages in car parks and do not return them to the marked places. Because of the vastness of the airport, carriages pose even a security threat. Sigfox can provide both indoor and outdoor protection and solve the problem.

## 5 Conclusion

The Sigfox network bypasses the need for a large number of IP addresses, thus avoiding IPv6 issues. Terminal devices are not connected directly to the Internet and do not have an IP address. Sigfox has its "last mile", or the connection to the last section between the network and the end device by a separate network. It is only from the base station that the data is moving over the IP network. Terminal devices are not available for IPv4 or IPv6.

Sigfox's top authority is Sigfox, which has access to all transferred data. Due to the fact that only 12 bytes are sent from a single device, user encryption is impracticable;

the data are open and readable for Sigfox. The message is signed with a digital certificate, to forge a system of fake law is difficult. Sigfox can thus act as a guardian over the entire global network. In theory, however, it is possible that regional Internet sovereignty (for example, the state) could order its internet service providers to disallow data streams to Sigfox servers. In that case, the Sigfox would cease to function in that country.

Geographical boundaries are significant in the Sigfox network so far, but in general, it should not be a problem. Although the network is still covered only by part of Europe, the coverage is planned to be complete. Additionally, in the Sigfox network, automatic roaming works across borders. The communication protocol is the same everywhere. Perhaps the Internet of Things is going to be the Internet without borders, as Internet creators introduced it because things do not have their own language, culture or thinking. For the time being, however, it would seem that if Sigfox copied the geographic Internet scenario, it would be a restriction from the top (meaning state regulations) rather than from users.

In conclusion, the Sigfox standard meets the surveillance studies theory and, at least in Europe, has the best prospects of becoming state-of-the-art Surveillance of Things tool.

## References


1. Li, B., Yu, J.: Research and application on the smart home based on component technologies and Internet of Things. In: Ran, C. and Yang, G. (eds.) Ceis 2011. Elsevier Science Bv, Amsterdam (2011).
2. Haiyan, S., Xiaobin, L.: Research on practical teaching system of the Internet of things technologies and application. In: Zhang, H.M. (ed.) Proceedings of the 2014 International Conference on Education, Management and Computing Technology. pp. 536–538 Atlantis Press, Paris (2014).
3. Sun, E. et al.: The internet of things (IOT) and cloud computing (CC) based tailings dam monitoring and pre-alarm system in mines. Saf. Sci, vol. 50, no. 4, pp. 811–815. Elsevier Publishing (2012).
4. Sundmaeker, H. et al.: Vision and Challenges for Realising the Internet of Things. Publications Office of the European Union, Luxembourg (2010).
5. Manovich, L.: The Language of New Media. The MIT Press, Cambridge, Mass. (2002).
6. Buyya, R., Dastjerdi, A.V. eds: Internet of Things: Principles and Paradigms. Morgan Kaufmann, Amsterdam Boston Heidelberg (2016).
7. SAMSUNG: IoT Solution Samsung Business, http://www.samsung.com/global/business/networks/solutions/solutions/iot-solution, last accessed 2017/12/21.
8. Hewlett Packard Enterprise: Delivering on the IoT customer experience The HPE Universal IoT Platform 1.4, http://h20195.www2.hpe.com/V2/getpdf.aspx/4AA6-5353ENW.pdf?ver=3.0, last accessed 2017/12/21.
9. IBM: IBM Watson Internet of Things (IoT), https://www.ibm.com/internet-of-things/, last accessed 2017/12/21.
10. Microsoft: Internet of Things (IoT) Microsoft, https://www.microsoft.com/en-us/internet-of-things/, last accessed 2017/15/21.
11. ČDT: Internet věcí ČD-Telematika a.s., http://www.cdt.cz/cz/internet-veci-1272/, last accessed 2017/12/21.

12. Sigfox: Sigfox - The Global Communications Service Provider for the Internet of Things (IoT), https://www.sigfox.com/en, last accessed 2017/12/18.
13. SimpleCell: simplecell.eu – Connecting Things, https://simplecell.eu/, (2017).
14. CTU: Všeobecné oprávnění č. VO-R/10/05.2014-3 k využívání rádiových kmitočtů a k provozování zařízení krátkého dosahu. (2014).
15. Ma, J. et al.: Connecting agriculture to the internet of things through sensor networks. Presented at the Proceedings - 2011 IEEE International Conferences on Internet of Things and Cyber, Physical and Social Computing, iThings/CPSCom (2011).
16. Sladek, P., Maryska, M.: Internet of things in energy industry. In: IDIMT 2017 - Digitalization in Management, Society and Economy, pp. 411-418. Linz: Trauner Verlag Universitet, Poděbrady, Czech Republic (2017).