Category: review paper

Idlbek, Robert [1]
Vučković, Žarko [2]
Prpić, Ivan [3]

Development of Network Agnostic SIM Technologies for M2M Data Transfer

Abstract:

The development of smart devices and their functionality is not possible without adequate network connectivity.

Every two to three years, smart devices increase their processing power, amount of memory and functionality for double. One of the limiting factors in the process of creating new smart devices is the way they connect to the network. Network connectivity must be reliable, inexpensive and financially affordable. Also, the device must be ready for manufacturing without additional costs. Many wireless networking technologies now exist on the market, but LPWAN and UICC are essential for the development of IoT devices in the next few years.

Keywords:
IoT connectivity; machine to machine; UICC; network agnostic SIM

Author´s data:
[1] Polytechnic in Pozega, Vukovarska 17, 34000 Požega, Croatia, ridlbek@vup.hr
[2] Wolf d.o.o., Miroslava Krleže 22, 34000, Požega, Croatia, wolf@po.t-com.hr
[3] student, Polytechnic in Pozega, Vukovarska 17, 34000 Požega, Croatia, iprpic@vup.hr

International Journal - VALLIS AUREA • Volume 5 • Number 1 • Croatia, June 2019
UDK 004.7; DOI 10.2507/IJVA.5.1.6.60

VALLIS AUREA

Introduction

In the last ten years, the available modern and high-tech services have changed considerably and created new ways of consuming them. By networking IP video cameras, mobile phones, various sensors, vehicles and machines, the basis for the provision of new services, that have not been possible or anticipated, has been created. Nowadays, most households have video surveillance and smart-home systems that can quickly and cheaply control the property. Smart mobile phones are powerful enough to enable surveillance of such equipment. The main reason for that transformation is the significant reduction in prices of before-mentioned equipment and the omnipresent availability of WiFi that enable its connections to the network. For 10-50 euros it is possible to acquire remotely operated switches that can be controlled by mobile phones from any location (e.g. Sonoff), and video surveillance can be purchased for 50 euros and receive alarms from motion sensors in a monitored space, and even store a video recording in the „cloud“.

Machines, sensors, actuators and other devices become available through the network from any part of the world. Of course, the device must have access to the Internet. That allows an entirely different use of these devices, and data security is becoming increasingly essential and data more interesting to unauthorized users (for example, hackers).

According to Juniper [1], more than 13 billion devices are already connected to the network, and more than 5 million new devices are connected every single day. About 38 billion connected devices are expected by 2020. Approximately 40% of total Internet traffic is expected to be generated by machine-to-machine communication [2], without any human interaction. Such predictions indeed constitute an exceptional innovation potential and are expected to explore many new possibilities arising from the explosion of network connectivity. That undoubtedly presents good prerequisites for the development of many business ideas. Moreover, it arises many data security related questions as well.

This paper will present the primary ways of connecting IoT devices to the network, as well as technologies that will allow easy management of their network connectivity.

Machine-to-machine and IoT concepts

The term "Internet of Things" (IoT) is the application of intelligent devices interconnected through different forms of network connectivity, intending to collect data from sensors embedded in physical objects [3]. Development of IoT devices accelerated due to the decline in the price of network connectivity, and the advancement of embedded systems technology such as increasingly powerful microprocessors with low energy consumption (Arduino, Raspberry Pi and the like). That creates a cheap and industrially reliable solution to collect data from different digital and analogue data sources (sensors). ARM processors, which are mainly the foundation of such embedded systems, have sufficient processing power to collect and analyze data on a single device. Low power consumption allows the construction of systems that operate on batteries. For machine-to-machine data exchange (which does not require human interaction) it is necessary to provide networking technologies that are acceptable regarding data bandwidth, energy consumption, data security, and device management.

Bandwidth

Most IoT devices require a small amount of data bandwidth. Simple sensors that report measured information once or twice a day, monthly don't require more than a few dozen kB of data traffic. On the other hand, vehicle monitoring needs data transmission at higher frequencies. Data transmitted in addition to the GPS location of the vehicle, contains numerous information. Some of additional data is: the number of GPS satellites to which the device is connected, LBS data from the teleoperator's base stations, current speed, and informations from various additional sensors (e.g. fuel level, current fuel consumption, cargo temperature, number of passengers, G force to detect inappropriate braking and harsh driving). This type of devices requires about 10-20 MB of data per month.

Finally, the extreme bandwidth consumers are video cameras and audio devices that can spend several GB of traffic per month.

Power consumption

The IoT device communication protocols, depending on their purpose, must be optimized for minimum power consumption. The reason is that most of these devices are not intended to connect to a constant power source (as is the case with a GPS tracker for vehicle monitoring). Some simple sensors need to work on an autonomous battery (often non-rechargeable battery) that allows autonomous operation for several years without charge while sending information once or twice a day. The amount of data transmitted can be several bytes per day, and it is essential to transfer them to the destination at a minimal energy cost.

More powerful IoT devices designed to transmit and analyze video and audio content, such as surveillance cameras, usually require a constant current source. The reason is that they consume much more energy considering video and image compression algorithms and object recognition (for example, detection movement or human recognition). More powerful processors require even more energy.

Security

Having in mind a large number of currently connected devices (with the expected substantial future growth), a significant challenge for network experts, hardware manufacturers and software developers is security. It is not about the security of the device itself (unauthorized access to the device), but also the tapping or intercepting and changing the data that comes from the device.

There is growing concern about the sabotage of IoT devices that can sabotage business activities, such as a production facility. That is an entirely new security issue and needs to be addressed on multiple levels: hardware level, software level, network level, and organisational level.

Device and software manufacturers are forced to raise the level of security.

So, first security management frameworks in the IoT world are emerging, such as the IoT Security Foundation [4]. Security becomes one of the major topics when it comes to the application of smart sensors in healthcare, smart home appliances, transport and energy management.

Device management

Managing a larger number of IoT devices is a problem. There is a growing need for a central application that is used to monitor the operation of the device, to diagnose the failure, and to change the configuration parameters. The important functions of such management platforms also provide software updates (firmware), which is important in the case of security vulnerabilities that can be solved by software patches.

In short lines, this can be defined as mangement IoT devices:

IoT device management is the process of authenticating, provisioning, configuring, monitoring and maintaining the device firmware and software that provides its functional capabilities. Effective device management is critical to establishing and maintaining the health, connectivity, and security of IoT devices [6]

3. Machine to machine communication

From the previous text, it is apparent that IoT devices for their work must achieve communication connection to send collected/processed data. More technologies can be used to accomplish this network connectivity, and its choice is primarily based on the specific application of the device. In the past decade, we have seen an intense penetration of internet and network technologies in the so-called "consumer technology" arena.

The connection to the Internet today have home alarm systems, heating and cooling systems, and even toasters and washing machines. The reason for this lies in the fact that the network electronics that is convenient for connecting the devices to the Internet has become incredibly inexpensive (1 EUR per piece for wired Ethernet port and 3-4 EUR for a wireless antenna connection). Moreover, a marketing presentation of a device that can connect to the Internet is always more vibrant, and to the average customer more attractive, although the applicability of such devices is questionable.

Initially, connection to the Internet was solely based on the ethernet UTP network connection, and after that, a growing number of devices supported wireless technologies (802.11a / b / g / n / ac). Such devices are connected to a local wired network or a short-range WiFi wireless network - typically up to 10-50 feet from a network router.

IoT devises today use one of the following network technologies for Internet access and consuming network services.

Bluetooth

Bluetooth represents a network data exchange protocol between two or more network devices. Typically, and in real terms, it works at a distance of 10 m. Bluetooth protocol is part of most of today's modern devices, from computers and cameras to cell phones where it has been an inevitable part for years. As the Bluetooth network connection consumes little electrical energy (especially for the latest generation of BT protocols like 4.2 BLE), the peak load is about 15mA, which is excellent for battery-powered devices [8].

The short distance from one device to another for sending and receiving data ensures a high level of security and prevents the eavesdropping and altering of data from a malicious attacker.

WLAN

A wireless network based on radio frequency is the standard for transferring data to small distances, mostly within a home or small business space.

Communication standards are based on the IEEE 802.11 set of protocols, and the latest 802.11ax standard supports speeds from 600 up to 9608 Mbit/s. Today, 802.11n and 802.11ac are base protocols, and widely used in most of the new mobile devices and multimedia audio-video devices that require faster data transfer.

WLAN network connectivity is used primarily by two types of devices:

1) Those who require a large amount of data transmitted for their work (for example video cameras), and

2) those devices require low power consumption for their work and are close to the wireless access point (for example, measuring devices that are put on livestock and recorded life activities).

A wireless network is a right choice for IoT devices that are connected to the local area and do not need to change its location. Given the small distance on which they work (in realistic conditions up to 30m, outdoors and up to 300m), the number of devices that use them is limited.

Cellular network

Lately, there has been an increasing number of devices that need to send and receive data from geographic locations that do not have a wired or WiFi connection. Among the first such devices are the GPS tracking devices already mentioned. Their network connection is based on a communication module with a SIM card that can connect to GPRS, 2G, 3G, or 4G networks.

In most countries, GSM coverage is excellent. In Croatia, there are three mobile operators: A1, T-Mobile and Tele2. In the early 1990s, the first GPS standard for 2G devices was adopted [7], which allowed the connection of a large number of IoT devices that now function precisely on the 2G communication standard. Although this way of communication is slow for today's modern mobile phones and user needs, it is fast and energy efficient enough for IoT devices. That is why it represents underlying technology even today, almost 30 years later.

2G technology is in use so much that some countries plan to shut down the 3G network and leave 2G up and running for the next few years. This shutdown free additional frequency bandwidth for upcoming technologies and networks [8].

The reason for this is the M2M market and the connection of a large number of IoT devices that now operate on 2G.

To accomplish the transfer, the device in the cellular network requires a Subscriber Identity Module (SIM) card purchased from a teleoperator providing a data transmission service. Services may be associated with a voice transmission, sending and receiving SMS messages and data transfer. When purchasing a SIM card, the terms and conditions in which the card works and the prices for individual services are subject to negotiate with the teleoperator.

For example, If the card leaves the local network, the device connects to the network of another operator and the roaming service is charged. From 15 June 2017 in the European Union, the new roaming regulation is called Roam Like At Home and provides the same prices for network services (voice, data, SMS) like they are on the local network [9]. Such a rule significantly reduced the cost of using mobile telephony for those persons or devices travelling within the EU, Norway, Iceland and Liechtenstein. However, devices that use SIM cards recognize the new network as roaming and accordingly can disable certain services if they are potentially expensive for the user. Also, a device with SIM card of the local operator cannot be out of the local mobile network all the time, so this is a constraint in using local providers for IoT devices outside the county.

Low-power wide-area network (LPWAN)

LPWAN or low-power wide-area (LPWA) network or low-power network (LPN) as an idea represents wireless networking technologies designed for IoT devices that exchange small amounts of data over long distances and use low data bandwidth. Because of these characteristics, LWPAN is designed for various sensors, actuators and devices intended for the IoT ecosystem. The transfer rate is up to 50 kbit/s per channel, which is insufficient for computer connections, mobile phones or other large bandwidth applications.

In addition to long-distance transmission (up to 10-40 km) and low power consumption, an essential feature of LPWAN is the low transmission cost.

Within the LPWAN concept, there are currently three different wireless technologies, and new ones are developing rapidly: DASH7, Sigfox and LoRa.

Network agnostic SIM - UICC

The technology for access to the cellular network, as mentioned, exists for 30 years and is based on a communication module and the SIM card of a particular mobile provider. The mobile operator is the one that offers the user of a card a specific service price (voice, SMS, data) and the change of the mobile operator requires the change of the SIM card in the device (phone or IoT device).

Changing the SIM card is accessible in mobile devices that users always have nearby. However, changing the same card in IoT devices is often problematic considering their number and possible physical inaccessibility. Besides, to physically change the card, it is necessary to change the configuration parameters of the IoT device so that it can access the network. In data traffic, a parameter that requires a change is called Access Point Name (APN), and each mobile operator has a different APN name. For example, the Croatian operator T-Mobile APN is "internet.hr.hr", while for A1 it is "internet". Therefore, once selected mobile operator service provider is not changed without a good reason, although other providers might offer better terms and conditions for using their services.

The new technology, called Universal Integrated Circuit Card (UICC) solves this problem. Simplified, UICC is a solution for easy changing prefered mobile network operator, without changing the SIM card itself. The companies which sell UICC card are not classic mobile operators. These companies do not have their network infrastructure, and their services and products are based on the SIM cards that can connect to a different mobile operator with whom the company has a signed contract.

For example, if the company has a signed contract with T-Mobile and A1 in Croatia, then the device using the specified UICC SIM can change the service provider on the fly, almost instantly. The device does not need to change the APN configuration for A1 or T-Mobile operator and can use the cheapest service, or service with better signal. The device itself does not see the difference between the two operators, nor does the operator change play a role in the functioning of the device.

As examples of such companies, we can list names like Things Mobile, PodM2M, DolphinM2M and EMnify. The new name for this type of enterprise is the Mobile Virtual Network Operator (MVNO), Virtual Network Operator (VNO), or Mobile Other Licensed Operator (MOLO). So, MVNO is a wireless communications services provider that does not own the wireless network infrastructure over which it provides services to its customers. An MVNO enters into a business agreement with a mobile network operator to obtain bulk access to network services at wholesale rates, then sets retail prices independently. An MVNO may use its customer service, billing support systems, marketing, and sales personnel, or it could employ the services of a mobile virtual network enabler (MVNE)[11]

Two fundamental characteristics of UICC cards are: [10]:

- Provisioning:

Classic SIM cards come with installed data/application for one mobile service provider (MNO); its change requires a physical change of the card. In contrast, UICC cards allow MNO change as needed, on the fly. The device with this type of card always connects to the network with the most reliable coverage and the cheapest service for the user.

- Device management:

Classic SIM cards need activation before use. The activation procedure follows placing the card in the mobile device, activating the PIN password, and then returning the card to the target device. Once activated, it has a certain monthly fee and cannot be easily deactivated or paused if the user doesn't need the service anymore. Often, to activate and deactivate the card, it is necessary to contact MNO (for example T-Mobile) and sign a contract or authenticate some of the documents. Managing UICCs is easy because the user can activate and deactivate the cards without paperwork, and without an additional mobile device for activation. In addition, it can change the card's workflow parameters and know whether or not it is active, how much data traffic is consumed over the specified card or network, which cards are card is connected to what MNO and when, and to activate and deactivate additional services such as voice or SMS on the fly.

Furthermore, it is possible to lock the SIM card to a particular device International Mobile Equipment Identity (IMEI number) so that it can not move to another device. Also, the user can configure various spending limits and network connections like VPN and fixed IP address. Another exciting option is to track the location where the card is used (on the map) regarding the LBS information obtained from the currently active mobile operator.

Conclusion

This paper presents the problems of connecting the IoT devices to the network, which is a critical component in their operation. Having in mind a large number of IoT devices, it is necessary to adopt a technology that provides a cost-effective, comfortable, long-lasting, cheap and stable network connection.

The current SIM cards are limited to only one teleoperator (MNO), but by the appearance of UICC cards and the change of legal regulation that enables businesses to provide network services using the infrastructure of another operator, more and more companies are competing in the M2M arena in providing services that could not be imagined a few years ago. There is a significant departure from the classic signing of contracts for each SIM card in the direction of the use of services according to their own needs, activation and deactivation of all required parameters independently and without the need to contact teleoperator.

Transition to UICC technology is expected in the next few years. That is particularly applicable to current devices, and older generation devices would have the most benefits from it. However, the development of network technology is emerging in the direction of eUICC; that is, the installation of the UICC smart chip in the microprocessor of the device itself. In this way, all devices will be able to connect wirelessly to the network without the need for a SIM card.

References

[1] Juniper Research. (2015). Internet of Things connected devices to almost triple to over 38 billion units by 2020 [Press release]. Retrieved from http://www.juniperresearch.com/press/press-releases/iot-connected-devices-to-triple-to-38-bn-by-2020. [Accessed 17 Feb 2019].

[2] Capgemini (2015). The impact of Internet of things on Financial services. [online] Available at: ww.capgemini.com/resource-file-access/resource/pdf/the_impact_of_the_internet_of_things.pdf [Accessed 17 Feb 2019].

[3] GSM Association (2014). Understanding the Internet of Things (IOT). Available at: http://www.gsma.com/connectedliving/wp-content/uploads/2014/08/cl_iot_wp_07_14.pdf [Accessed 17 Feb 2019].

[4] IoT Security Foundation (2019). [online] Available at: https://www.iotsecurityfoundation.org [Accessed 17 Feb 2019].

[5] i-scoop (2017). IoT device management: challenges, solutions, platforms, choices, market and future [online] Available at: https://www.i-scoop.eu/internet-of-things-guide/iot-device-management [Accessed 20 May 2019].

[6] Hamilton, D. (2018). The future of IoT device management [online] Available at: https://www.networkworld.com/article/3258812/the-future-of-iot-device-management.html [Accessed 20 May 2019].

[7] BrightHun (2011). History of Cellular Technology: The Evolution of 1G, 2G, 3G, and 4G Phone Networks [online] Available at: https://www.brighthub.com/mobile/emerging-platforms/articles/30965.aspx [Accessed 20 May 2019].

[8] https://www.mobileworldlive.com/featured-content/top-three/telenor-norway-shut-3g-network-2020-five-years-2g/

[8] Everything RF (2017). [online] Available at: https://www.everythingrf.com/community/what-is-the-difference-between-bluetooth-5-0-bluetooth-low-energy-bluetooth-v4-2-and-classic-bluetooth [Accessed 18 Oct. 2018].

[9] T-Portal (2017). [online] Available at: https://www.tportal.hr/tehno/clanak/veliki-vodic-kroz-ukidanje-roaminga-evo-sto-nas-ceka-od-15-lipnja-20170516 [Accessed 8 Feb. 2019].

[10] EMnify eUICC: what it is and why it matters (2016). [online] Available at: https://www.emnify.com/blog/2016/01/29/euicc-what-it-is-and-why-it-matters [Accessed 13 Feb. 2019].

[11] Berec.europa.eu. (2016). [online] Available at: https://berec.europa.eu/files/document_register_store/2016/8/NN%20Factsheet.pdf [Accessed 18 Jul. 2018].