WIRELESS SENSOR NETWORKS INTEGRATION INTO INTERNET OF THINGS

Miodrag Živković[1],
Tamara Živković[2]

[1]Faculty of Informatics and Computing,
Singidunum University,
Belgrade, Serbia
[2]Faculty of Electrical Engineering,
University of Belgrade, Serbia

Abstract:

Wireless sensor networks usually consist of a large number of sensor nodes forming a network. Sensor nodes are miniature autonomous devices with very limited resources, capable of collecting and processing data from the surrounding area, and transmitting this data wirelessly over short distances via radio transmitters. The range of wireless sensor networks applications varies from the environment monitoring and detecting forest fires, climate changes monitoring, tele-health monitoring, detecting toxic fumes in factories, to smart sensor systems in the car. With the emerging technology of Internet of Things, the importance and number of applications of wireless sensor networks are increasing every day. Wireless sensor networks are one of the most important parts of the whole Internet of Things concept. The main idea of Internet of Things is to provide smart world, where every device has built-in intelligence, and is connected to other devices in the environment. As such, Internet of Things basically integrates the world of information with real devices, and enables us to have immediate access to this information. Wireless sensor networks provide aspect of surveillance, physical phenomena detection, environment monitoring and remote access to Internet of Things. This paper surveys the current state of the art of wireless sensor networks and Internet of Things, presents challenges of integrating two technologies together, and gives an overview of the new applications of wireless sensor networks in the scope of Internet of Things.

Keywords:

Wireless sensor networks, Internet of Things, sensor nodes.

1. INTRODUCTION

Wireless sensor networks typically consist of large number of sensor nodes. Each node of the network has sensing ability (temperature, pressure, vibration, sound, humidity, etc.). At the same time, each node is router as well. Sensor nodes have very limited resources. They are autonomous devices which collect data from the surrounding area and transmit this data wirelessly over short distances, typically 1-10 meters. Wireless sensor networks use large number of these devices to form a network without any previously established infrastructure.

Sensor nodes forming wireless sensor network are small, so resources for data processing, data storage, communication and energy are very limited. All nodes are usually designed following general architecture based

Correspondence:
Miodrag Živković

e-mail:
mzivkovic@singidunum.ac.rs

DOI: 10.15308/Sinteza-2017-115-120

on the central processing unit, around which different UI components, communication interfaces and power source are placed. Figure 1 shows this general structure of the sensor node, with the microcontroller, communication devices, sensors and actuators, memory and power source.

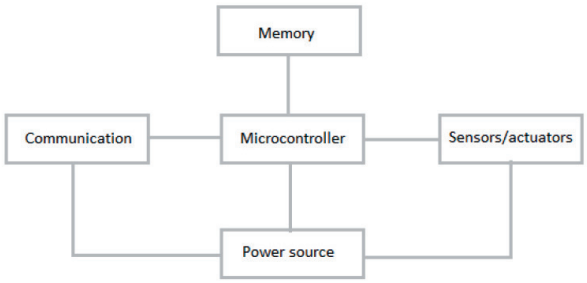

Fig. 1. General structure of the sensor node

The central part of this structure is a microcontroller, general purpose processor optimized for low power consumption. Communication block usually consists of one or more communication devices embedded on the node, such as a radio transmitter, Bluetooth, GSM/UMTS, etc. Each node has physical sensors, which can be passive or active (radar), focused (camera) or multidirectional (temperature, vibration, etc.) with different areas of coverage. Each node has one or more power sources, which need to provide as much energy as possible at lowest possible cost in terms of price, size, weight and recharge time. Charging of the batteries is not always an option in wireless sensor networks. Memory block typically depicts additional flash memory, as in the most cases available RAM memory is negligible. For the given fixed processing power, chip is becoming smaller and cheaper every year due to recent advances in semiconductor technology.

These cheap wireless sensor nodes with low energy consumption can be distributed in the physical area in order to collect data about the physical phenomena under observation. They can process the data, and communicate and coordinate actions with each other. In most cases, large number of distributed sensor nodes is required to overcome obstacles such as walls, optical visibility limitations, ground configuration, etc. The area under observation often does not have any existing infrastructure in terms of communications and energy sources (forests, active volcanoes, etc.). Communications between the nodes is the biggest energy consumer in wireless sensor network. Large number of transmissions over large distances lead to large energy consumption, and consequently failure of the nodes due to empty batteries. It is imperative to keep the number of wireless transmissions minimal, in order to keep network operational over longer periods of time. Typical wireless sensor network architecture is shown in Figure 2. Nodes collect data and send it to the sink node, or base station. Data is then transferred to the end user via Internet network.

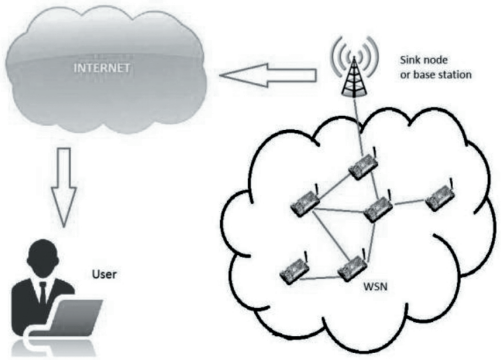

Fig. 2. Architecture of wireless sensor networks

Sensor nodes have simple microcontrollers, and miniaturization allows operation on 10 MHz with energy consumption of 1mW. Most of the components of the node can be switched off if needed, and in standby mode energy consumption is around 1 microwatt. If device is active approximately 1% of time, the average consumption is only several microwatts. These simple microcontrollers, however, have very limited storage capacity, typically less than 10 KB RAM memory for data and less than 100 KB ROM for programs, which is one million times less than average PC [1].

Wireless sensor network formed of these low power sensor nodes, coupled with Big Data analytics and cloud computing led to a great interest and expansion of Internet of Things. With this combination of technologies, we can place multiple sensor nodes anywhere where there is valuable information which needs to be collected, even in places without proper communications and power infrastructure.

Recently, there is an increasing number of researches targeting integration of wireless sensor networks in Internet of Things, with possible applications including medicine, remote patient tracking, environment monitoring, operation in hazardous environments such as active volcanoes, radioactive areas and industrial sites with toxic vapors. Most of the research papers focus on security issues that arise from integration, such as [2], [3]. Other papers focus on possible applications, most notably tele-health care and medical applications, such as [4].

2. INTERNET OF THINGS

The Internet of Things (IoT) has been defined in Recommendation ITU-T Y.2060 as a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies [5]. The basic concept of IoT is simple – connecting various devices over the Internet, and thus, making them "smart". The future Internet, based on IoT, is predicted to be "a world-wide network of interconnected objects uniquely addressable, based on standard communication protocols" [6]. Any "thing", identified by a unique address, will be able to join the network dynamically, and cooperate with other "things" to achieve different tasks. These "things" can be any object, including computers, mobile phones, sensors, home appliances, vehicles, wearable devices including health and fitness monitoring, watches and so on. The growth of the number and variety of devices which can collect data is incredibly rapid. The number of connected devices surpassed the human population in 2010, and some studies estimate that the number of Internet connected devices will be 50 billion by the year 2020 [7]. In other words, there will be 6.5 connected devices per each person in the world. IPv6 is going beyond IPv4 limitations (4 billion addresses only) and it will provide more address space to enable level of scalability required for IoT and Cloud Computing.

The devices connected to IoT can effectively be separated in three classes:

- The smallest devices (including sensor nodes), which have embedded 8-bit microcontrollers. Open source hardware platform Arduino Uno is one example.
- System based on Atheros and ARM chips, with limited 32-bit architecture, such as Arduino Zero
- Full 32-bit or 64-bit computing platforms. These are most capable IoT platforms, including mobile phones or Raspberry Pi. Such devices may also be gateways for smaller devices, for example wearable sensors which connect via Bluetooth Low Energy to mobile phone, which acts as a gateway to the Internet.

There are many different types of communication between devices and the gateway/Internet. Most typical models are:

- Direct Wi-Fi connectivity (TCP or UDP)
- Near Field Communication (NFC)
- Bluetooth Low Energy (BLE)
- ZigBee
- Point-to-point radio links
- UART

Devices can have direct Wi-Fi connection (TCP or UDP) to the Internet and server side cloud. This is the case with more capable devices, such as mobile phones and Raspberry Pi. These devices can interact with cloud services directly. Smaller devices, including most of the common sensor platforms do not have direct access to the Internet. They communicate with gateways on short distances via BLE, ZigBee or similar. As mentioned above, gateways themselves can be IoT devices, i.e. Raspberry Pi.

The other aspect of the IoT, apart from devices themselves, is the server side architecture that supports them. The servers are usually based on Cloud Computing. According to the American National Institute of Standards and Technology (NIST), "Cloud Computing is a model that allows convenient access to the configurable network resources on demand". By providing computing, network and data resources, cloud offers large number of services, applications, data and infrastructures to the users. Cloud components can be configured, secured, implemented, scaled up or down, or completely removed quickly [8]. Cloud Computing is different from traditional Internet services as it has dynamic and flexible architecture. Today, it is not needed to pay attention to the background infrastructure when accessing content on the Internet, and Cloud Computing is offering such model for providing computing services. The most popular Cloud Computing providers include Amazon and Elastic Compute Cloud (EC2), Microsoft Azure platform and Google Cloud Platform. Open source community has also been very active in Cloud Computing, with numerous solutions in fields such as system and network virtualization. One of the most important features of Cloud technologies is scalability, in terms of ability of the Cloud to adapt to smaller or larger scale of the required amount of processing. Complete implementation is hidden behind the Cloud, and users get exactly what they require. Additionally, Cloud systems are very reliable.

3. WIRELESS SENSOR NETWORK INTEGRATION

Wireless sensor networks play a major role in Internet of Things, by collecting data from surrounding environment. New challenges arise when wireless sensor networks are configured to access the Internet, and will

be discussed later. Integration and connection of wireless sensor network into the Internet can be done in one of the three main approaches, described in [9].

First approach, currently used by the most wireless sensor networks implementations, is based of connecting Internet and WSN through a single gateway (base station), as shown in Figure 3. Since sensor nodes do not have direct access to the Internet, WSN is independent, thus more secure. However, downside is that in this approach there is single point of failure. If gateway is down, complete WSN becomes disconnected from the Internet.

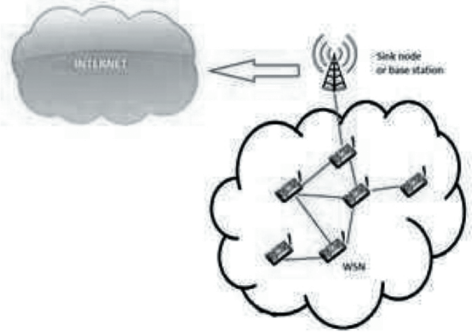

Fig. 3. Single gateway connection

The second approach is based on multiple gateways, forming a hybrid network with increased integration level, as shown in Figure 4. Sensor nodes still do not have direct access to the Internet, but risk of gateway failure and WSN disconnection from the Internet is greatly reduced, making the network more robust.

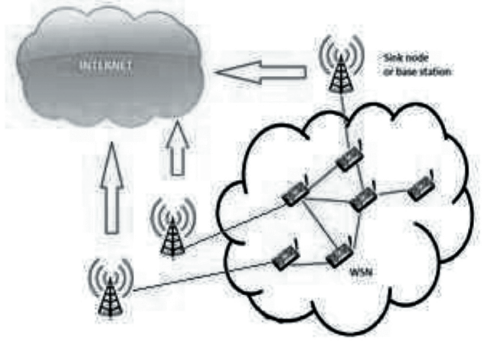

Fig. 4. Hybrid network with multiple gateways

The third approach is based on the idea that sensor nodes can join the Internet in one hop, as shown in Figure 5. It is based on the WLAN structure and forms access point network. This approach is particularly useful in applications requiring direct connectivity to the Internet and low latency.

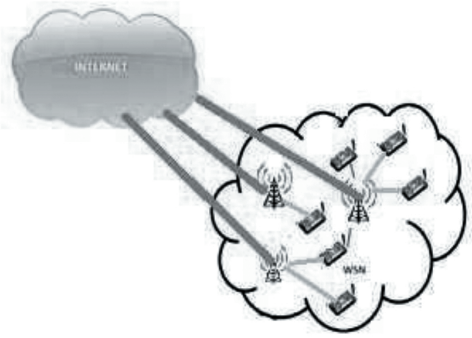

Fig. 5. Nodes can join internet in one hop

There is large number of different technologies available for sensor networks, including network support, operating systems, etc. However, support usually ends on the network gateway, leaving open space for implementation of ad hoc solutions for modelling and analysis of data collected by sensor nodes. Implementation of back-end resources could be particularly problematic in case of application of sensor networks in specific environments. For example, sensor network for detection of forest fires uses sensor data in real time. In standard mode of operation, incoming data from sensors is not time critical (no fire detected). However, in case of forest fire, alarming first responders is time critical [10]. In case of traditional data processing technologies, manual allocating of additional processing capacity is required. On the other hand, by using elastic system as IoT and Cloud computing, it is possible to incrementally allocate additional processing power to provide better granularity of the results.

IoT integrates large scale sensor networks with Cloud Computing infrastructure. It allows sharing of large scale data between users and applications on the Cloud. Cloud provides options for easy data access, processing, visualization, archiving and searching large amounts of sensor data.

4. INTEGRATION CHALLENGES

Integration of wireless sensor networks in IoT brings new technical challenges, including complex event processing, large scale systems, real time data processing, and privacy. WSN specific challenges, such as network deployment, automatic configuration, operation without

supervision and energy constraints are out of the scope of this paper.

Complex event processing

Incoming data from sensor networks can trigger certain events and services in real time. Applications can use this data to determine the context, location and environment of the data source and decide which other services can be relevant to the current data set to make right decisions.

Large scale systems and real time data processing

Integration in case of large sensor networks is a challenge due to large amount of data, which is collected and processed in real time. Challenge is even bigger if data include multimedia, such as video streaming or images. Sometimes multiple sets of sensor data used for decision making are geographically distributed, meaning they are coming from different locations. In that case, allocation of the resources for data processing and data storage is critical.

Privacy

Cloud is the least transparent way of providing service, as complete implementation, data storage and data processing is hidden behind the cloud. Data privacy is of the critical importance [11]. When data leave sensor network and arrive to the cloud, adversaries can try to gain access to it. Data collected by the sensor network is often sensitive, and great attention needs to be payed to security and data protection. In case of common sensor networks without Internet connectivity, adversary would need to be physically present near the targeted network to attack it (by jamming, introducing malicious node, physically destroying nodes, etc.). However, in case of IoT, wireless sensor network is open to the Internet, and adversary can attack from anywhere around the world. Security mechanisms need to be selected carefully, keeping in mind that most of the common sensor node platforms have very limited computing power, energy and storage.

5. CONCLUSION

This paper aimed to give introductory overview about the wireless sensor networks, Internet of Things, and how the two technologies can be integrated. Integration challenges were also mentioned, the most important one being the privacy issue that needs to be addressed carefully. Internet of Things is not technology of the future – it is already happening. With the number of connected devices expected to be around 50 billion by the year 2020, the whole world is becoming one big connected thing. Integration of the wireless sensor networks with Internet of Things will bring many traditional applications of WSN to the higher lever, including tele-health care, first responders and environment monitoring. It will also enable new types of WSN applications in the future. Data is collected from the different sensor networks in the real time. Data processing is also performed in real time to make time critical decisions. Cloud services are responsible for complex tasks processing and fast response to the users.

REFERENCES

[1] M. Živković, R. Popović, T. Tanasković, "Pregled komercijalno raspoloživih senzorskih platformi sa aspekta potrošnje energije", 20. Telekomunikacioni forum TELFOR 2012, Beograd, 2012

[2] M. A. Iqbal, M. Bayoumi, "Wireless Sensors Integration into Internet of Things and the Security Primitives", Computer Science & Information Technology, ICCSEA, SPPR, UBIC, pp. 59–67, 2016

[3] H. S. Gol, "Integration of Wireless Sensor Network (WSN) and Internet of Things (IOT), Investigation of Its Security Challenges and Risks", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 6, Issue 1, pp. 37-40, January 2016

[4] N.Alharbe, A. S. Atkins, J. Champion, "Use of Cloud Computing with Wireless Sensor Networks in an Internet of Things Environment for a Smart Hospital Network", The Seventh International Conference on eHealth, Telemedicine, and Social Medicine, eTELEMED 2015, pp. 52- 58, 2015

[5] Recommendation ITU-T Y.2060 (06/2012), available online: http://handle.itu.int/11.1002/1000/11559

[6] "Internet of Things in 2020: Roadmap for the Future," 2008, online, http://www.smart-systems-integration.org/public/internet-of-things.

[7] D. Evans, "The Internet of Things – How the Next Evolution of the Internet Is Changing Everything", Cisco White Paper, April 2011, online: http://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0 411FINAL.pdf

[8] P. Mell and T. Grance, "The NIST Definition of Cloud Computing - Recommendations of the National Institute of Standards and Technology. NIST," NIST Spec. Publ., 2011.

[9] R. Roman and J. Lopez, "Integrating Wireless Sensor Networks and the Internet: a Security Analysis," Internet Research: Electronic Networking Applications and Policy, vol. 19, no. 2, 2009

10] N.G. Nair, P.J. Morrow, G.P. Parr, "Design Considerations for a Self- Managed Wireless Sensor Cloud for Emergency Response Scenario," The 12th Annual PostGraduate Symposium on the Convergence of Telecommunications, networking and Broadcasting, PGNET2011, June 2011.

[11] O. Popovic. Z. Jovanovic, N. Jovanovic, R. Popovic, "A Comparison and Security Analysis of the Cloud Computing Software Platforms,"Telecommunication in Modern Satellite Cable and Broadcasting Services (TELSIKS), 10th International Conference, Vol. 2, pp. 632-634, October, 2011