ІСТ-2023

28 листопада - 01 грудня
Харків 2023

12ª Міжнародна науково-технічна конференція
«Інформаційні системи та технології»
(ІСТ-2023)

Матеріали доповідей

Частина 1

Харків 2024

Міністерство освіти та науки України
Національна академія наук України
Люблінський відділ Польської Академії Наук
Представництво „Польська академія наук” у Києві
Харківський національний університет радіоелектроніки
AGH науково-технологічний університет ім. Ст. Сташіца в Кракові
Прикарпатський національний університет ім. В. Стефаника
Національний університет кораблебудування ім. адмірала Макарова
Одеський державний екологічний університет
Національний університет Запорізька політехніка
Академія Наук Прикладної Радіоелектроніки
Українська нафтогазова академія
Українська Федерація Інформатики

Інформаційні системи та технології ІСТ-2023

МАТЕРІАЛИ

12-ї Міжнародної науково-технічної конференції

Частина 1

29 листопада – 01 грудня 2023 р.
Харків, Україна

Харків 2024

Improvement in Wireless Sensor Networks: From Technology Integration to Network Management

Volodimir Karnaushenko[a], Evhen Gorbenko[a], Mariia Piataikina[a] , and Yuriy Vasilyev[a]

[a] *Kharkiv National University of Radio Electronics, Nauky Ave. 14, Kharkiv, 61166, Ukraine*

Abstract

This paper provides insights into the utilization of electronic components, specifically microcontrollers, in the construction of wireless sensor networks. The discussion covers their role in facilitating system design, maintenance, and efficient data transfer, highlighting the crucial impact of electronic components on the successful deployment of wireless sensor technologies.

Keywords [23]

Information and Communication Technologies, Wireless Sensor Networks, ZigBee Technology, IEEE 802.15.4 Standard, Bluetooth Low Energy.

1. Introduction

In recent years, the development of information and communication technologies is proceeding at a rapid pace. This is connected with the demand for exchange and processing services of various types of information. A number of interrelated and mutually determined processes, such as identification, selection, formation of information, input into technical systems, analysis, processing, storage and transmission from a set of information are part of a network based on the complex use of computer equipment and technology connection.

Natural processes, such as sudden climate changes, earthquakes, environmental pollution, radiation hazards, etc., force a person to manage natural processes, not limited to managing only social processes.

The essence of this is to collect the necessary information and carefully analyze it. Regular monitoring ensures timely detection of errors and their correction as soon as possible.

However, it often happens that you need to consider the state of the system without local access. The lack of such access may be related to both the regional remoteness of the system and physical security limitations, which is why there was a need to create remote monitoring tools.

Wireless sensor networks have great potential for solving such tasks as one of the modern trends in the development of data transmission networks.

It was the expansion of information services that led to the development of wireless sensor networks.

When designing security, communications and notification systems in residential, industrial or office buildings, the question of building local networks arises and, first of all, developers face a dilemma - wired or wireless type of network.

For economic reasons, the decision often remains in favor of wired networks.

Such a choice does not require highly qualified staff and there is no need to solve the problem of choosing components.

With the increase in the number of sensors, the location area of the automated system increases, the efficiency of control algorithms increases, and the use of distributed systems becomes more efficient.

Proccedings *Information Systems and Technology (IST-2023), November 28-December 01, 2023, Kharkiv, Ukraine*
EMAIL: vladimir.karnaushenko@nure.ua (A. 1); yevhen.horbenko@nure.ua (A. 2); mariia.piataikina@nure.ua (A. 3); yurii.vasyliev@nure.ua (A. 4)
ORCID: 0000-0001-7744-2569 (A. 1); 0000-0003-1993-6717 (A. 2); 0000-0003-2448-4436 (A. 3); 0000-0002-9385-7411 (A. 4)

The maximum benefit from a distributed system is achieved when the controllers work independently, and the exchange of information between them is minimal.

The distributed system has the following characteristics:

- greater speed, this is achieved due to the use of parallel distribution of tasks between processors;
- system uses a simplified modernization algorithm;
- resistance to failures;
- increased reliability;
- simpler expansion of reconfigured systems;
- it has great simplicity of designing, layout, configuration, diagnostics and maintenance of the system.

2. Types of Wireless Communication Protocols in IOT

Networks, as you know, are a means of data transmission. However, networks differ depending on the amount of data transferred [1]. Industrial networks are networks that deal with large-scale data transmission. This means that they allow you to connect different devices over large areas and provide communication between them, ensuring the transfer of huge amounts of data between them.

Traditional networks may seem very efficient, but in reality they are limited to a very small number of systems. Industrial networks are designed to meet real-time and multi-system needs.

An industrial network is connected to its components (devices, network nodes) through an interface.

A network interface is a logical and/or physical boundary between a device and a communication environment. This limitation is usually a combination of electronic components and related software. With significant changes in the internal structure of the device or software, the interface remains unchanged, which allows you to distinguish the interface as part of the hardware. One of the most important parameters of the interface is the bandwidth and the maximum length of the data bus.

To organize information exchange, interacting devices must have the same data exchange protocol.

A protocol is a set of rules that govern data exchange. A protocol can be implemented in hardware and software.

A network typically uses multiple protocols to form a protocol stack, which is a set of interrelated communication protocols that work together [2].

A wireless sensor network is an infrastructure-less wireless network that is specifically deployed in a large number of wireless sensors used to monitor systems, physical conditions, or environmental conditions.

Sensor nodes are used in a wireless sensor network with an embedded processor that controls the system in a specific area. They are connected to the base station, which acts as a processing unit in the wireless sensor network system.

The base station of the wireless sensor network system is connected to exchange data via the Internet.

The space covered by the sensor network is called the sensor field.

Wireless sensor nodes are tiny devices with limited resources: battery charge, memory capacity, computing power, etc.

The parameters of the network nodes may change depending on the purpose of the network. When designing a network of a specific type, it is necessary to take into account the capabilities of nodes: energy efficiency, computing power, the possibility of autonomous operation, etc.

A self-organizing wireless network, in particular a wireless sensor network, can be formed by a certain set of nodes, each of which is within the range of at least one node from this set, and each has the ability to send data to a destination node, which can be a gateway or any other network node.

In general, in a heterogeneous network, all or part of the network nodes can be mobile, have different speed characteristics, physical and channel communication standards.

The IEEE 802.15.4 standard was developed to organize communication between nodes in wireless sensor networks. This standard includes ZigBee technology, which allows the creation of self-

organizing and self-healing wireless networks with automatic message forwarding and support for battery-powered and mobile nodes.

ZigBee networks with relatively low data rates offer guaranteed packet delivery and protection of transmitted information.

The ZigBee standard provides frequency channels in the 868 MHz, 915 MHz and 2.4 GHz ranges.

High data transfer rates and noise protection are available in the 2.4 GHz band. The data transfer rate is 250 Kbit/s. Depending on the network load and the number of retransmissions, the average data transfer speed of a node user can vary from 5 to 40 Kbit/s.

The distance between network nodes is tens of meters when working indoors and hundreds of meters outdoors. Rebroadcast can significantly increase network coverage.

The ZigBee network is based on a mesh topology. In such a network, each device can communicate with any other device directly and through indirect network nodes.

The network topology provides alternative routing between nodes. Messages travel from node to node until they reach the final recipient. There are several ways to forward messages, which increases network availability in the event of a connection failure.

An exception to the standard can be considered Bluetooth technology, which is described by the IEEE 802.15.1 standard.

A Bluetooth wireless network in the classical sense is a dynamic peer-to-peer wireless network with a variable number of mobile nodes with decentralized control, which can be deployed in a limited space (up to 80 nodes). Bluetooth radio communication takes place in the license-free ISM band (2.4 ... 2.4835 GHz) at a speed of 1 Mbit/s (version 1.2); 3 Mbit/s (version 2.0); 24 Mbps (version 3.0).

Bluetooth is characterized by the spontaneous creation of a mass user mobile network, when almost anyone who owns such a radio interface can easily connect to it, unless, of course, security policies against unauthorized access are not resolved. This becomes a major problem when using Bluetooth technology for a wireless sensor network.

If we talk about ZigBee, software and hardware tools in the form of AES - crypto protection are already provided for this technology. Unlike Bluetooth, the ZigBee network is a distributed, self-organizing wireless structure that can span many kilometers and consist of a large number of nodes.

Currently, the ZigBee technology, developed directly for wireless sensor networks, is essentially the only technology that can be used to solve any monitoring and control tasks, including critical response time from sensors.

Wi-Fi technology allows you to build self-organizing infrastructure-type wireless networks, that is, to create a multi-point topology with a wireless access point for connecting mobile subscribers. However, such a topology is rather one of the disadvantages, if we consider it as a variant of a self-organizing network - the failure of the base station (access point) leads to the collapse of the entire mobile network.

Wi-Fi networks use several modifications of the 802.11 standard. The 802.11a standard provides data transmission at a frequency of 5 GHz at a speed of up to 54 Mbps.

The main advantage of the technology is the simplicity of the principles of building and configuring a mobile subscriber to a wireless network, but at the same time Wi-Fi ZigBee significantly "loses" in terms of mobility and power consumption.

The properties of the network depend on many factors, such as the characteristics of the service area (area), the number and distribution of nodes on an area or space, their parameters and others.

To date, quite a few algorithms have been developed for selecting the main node of a cluster in a wireless sensor network. It should be noted that it is unlikely that an optimal master node selection algorithm for any sensor network will ever be developed due to the extremely large number of sensor network applications, as well as the diversity of node locations of these networks in n-dimensional space.

However, the analysis of the main node selection algorithms allows for their classification.

First of all, algorithms for selecting the main node in a wireless sensor network are divided into centralized and decentralized as shown in Figure 1.

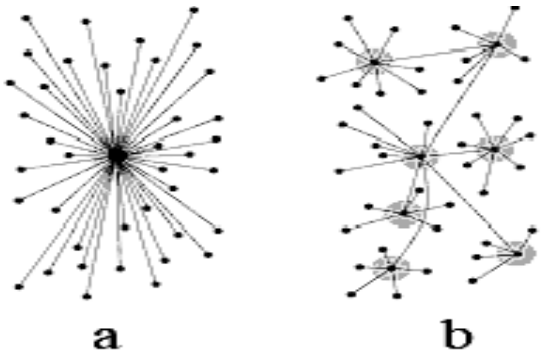

Figure 1: Types of master node in a wireless sensor network: a) centralized network; b) decentralized network

Algorithms for the selection of centralized main nodes assume the presence of computing power in a given network control element, which is not associated with strict restrictions on electricity consumption. Decentralized master node selection algorithms assume that the master node appointment procedure takes place in the sensor field itself without centralized intervention. At the same time, very strict requirements are put forward to the complexity of the process itself, which should not consume more or less noticeable costs of the limited energy resources of the increasingly permeable sensor network.

3. Ready-Made Wireless Sensor Network Solutions

The first step in the design process is choosing a wireless microcontroller, which means choosing both the microcontroller platform and the transceivers, as well as choosing one of the many communication protocols. Let's consider possible solutions for a wireless communication system for buildings.

As requirements evolve or the number of end products increases, it becomes difficult to update devices and software to keep up with the wireless network. Therefore, it is best to choose a wireless microcontroller that will work for both the first and future generations of the product.

Future-proof design provides the flexibility to update or extend products, leveraging investments, minimizing development cycle time, and optimizing product costs. New technological capabilities such as reduced power consumption, smaller size, integration, and new protocol features are increasing the number of wireless applications.

Wireless connectivity designs require seamless communication between different types of end devices. For example, in the security system of a large apartment building, several wireless devices work together to protect the residents.

The first level of security of an apartment building can start with an intelligent electronic lock at each apartment entrance. The electronic lock uses a frequency below 1 GHz as a long-distance communication protocol and Bluetooth Low Energy function to provide control over each residence and centralized control of the security gateway. Here it is important to consider the amount of memory, especially when developing many protocol programs.

The SimpleLink wireless microcontroller is ideal for simultaneous

Bluetooth and 1GHz low energy operation, with flash memory and a built-in power amplifier to extend the range to cover large buildings.

If the electronic lock software needs to be updated, additional memory may be required to enable wireless firmware or features loaded with the latest protocol specifications, such as physical encryption levels for Bluetooth LE, which increases the range of component choices.

Another application example: heating, ventilation and air conditioning system. If using a thermostat system, temperature sensors can be added to the system so that users can monitor and adjust the temperature in their room.

For the thermostat gateway, multi-protocol concurrent multi-protocol dispatcher systems are designed with flash memory and protected memory to support sub-1 GHz low power or Zigbee stacks.

To reduce the cost of the system, TI developed a single wireless microcontroller protocol for a simpler and less expensive system.

This provides freedom both during the initial design process and for future innovations. Microcontrollers come with a pre-certified system-in-package option for faster time-to-market. In addition, software interoperability for wireless microcontrollers is critical for cost optimization and reusability across multiple generations of products.

4. Components of Wireless Networks

Broad spectrum microcontrollers or multi-protocol, multi-band and wireless microcontrollers with built-in power amplifiers, such as SimpleLink wireless microcontrollers, CC family from TI in Figure 2, are usually used to build a wireless sensor network [3,4].

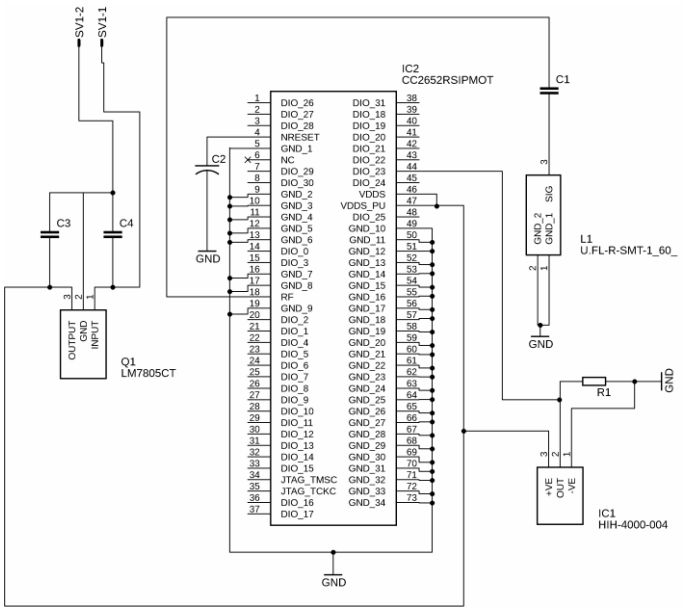

Figure 2: Electrical schematic diagram of a wireless sensor network with a humidity sensor

In this work, the types of control and management networks and the features of the construction of a distributed control and management system, namely a wireless sensor network, are considered.

As a result of the study, conclusions were drawn about a number of undeniable advantages of wireless sensor networks:

- ease of system design and maintenance;
- high data transfer rate and noise protection;
- mobility of network deployment.

5. References

[1] Shafiq Muhammad Gu, Zhaoquan Cheikhrouhou, Omar Alhakami Wajdi Hamam, Habib (3 August 2022). "The Rise of "Internet of Things": Review and Open Research Issues Related to Detection and Prevention of IoT-Based Security Attacks". Wireless Communications and Mobile Computing.

[2] A quick guide to industrial network security 2023. URL: https://www.embedded.com/a-quick-guide-to-industrial-network-security/

[3] LP-CC2652R7 CC2652R7 LaunchPad™ development kit for SimpleLink™ multi-standard wireless MCU 2023. URL: https://www.ti.com/tool/LP-CC2652R7?keyMatch=LP-CC2652R7

[4] A Guide to Texas Instruments WiFi Modules and Development Boards for IoT 2020. URL: https://www.nabto.com/texas-instruments-iot-wifi-modules-development-boards/