UDC C 620.9:.658.26

IOT NETWORK: MODELS, STRUCTURE, COMMUNICATIONS, PROBLEMS

U.A. VISHNIAKOU, DU ZONGQI, LIU ZHENHUA, HU JIFENG, YU CHUNYU

Belarusian State University of Informatics and Radioelectronics, Republic of Belarus

Submitted 8 November 2021

Annotation. A brief analysis of the concepts and applications of IoT networks is carried out. Four models of building these networks as variants of component interaction are given: terminal, gateway, cloud, application. Variants of IoT network architectures are presented. Seven variants of interaction in Yota networks are considered. The analysis of problems in these networks and the direction of their solution are carried out.

Keywords: IoT networks, models, architectures, interaction, problems.

Introduction

The concept of Internet of Things (IoT) originated from the network Radio Frequency Identification (RFID) system proposed by the Massachusetts Institute of Technology in the USA in the automatic identification laboratories, created in 1999 [1]. This system can connect all items to the Internet via radio frequency identification (RFID) and other equipment to read information and implement intelligent identification and management.

The Internet of Things is a technology that automates input, processing and optimization based on the obtained values of process characteristics reflected in the indicators of industrial and home sensors. The IoT technology allows the user to receive data and report on the status of equipment or processes in real time, monitor the work of industrial and agricultural enterprises [2]. The IoT has found its application in many areas [3]: smart car, smart home, smart city, smart agriculture, healthcare, etc.

Structurally IoT consists of four main components, which are: IoT devices; communication technologies; platforms for data storage and processing, applications [3]. IoT in a narrow sense refers to a network that connects objects with objects for the implementation of intellectual identification and management of objects. IoT in a broad sense can be considered as the integration of information space and physical space, digitization and integration of everything into a network. To achieve effective information interaction between objects, objects and people, as well as between people and the real environment and communication.

IoT network models

From hardware to software, the IoT system includes a lot of content, but conceptually it is a hierarchical structure. From the bottom up, the IoT system can be divided into three levels: the perception level, the network level and the application level. This three-layer conceptual model of IoT has a great impact, but from a physical point of view, it is possible to imagine four varieties of physical models of IoT systems [3, 4].

The first model: «Cloud Terminal-Cloud» refers to all applications in the IoT system that will be deployed in the cloud; terminal refers to IoT objects, including hardware and software deployed on them. This model refers to the IoT system, divided into two parts: a cloud platform and a terminal. The cloud platform needs to implement a website so that people can manage it through a web page. The cloud platform should also implement a communication interface for interacting with things. The terminal contains sensors, devices, memory, etc. For performing local business functions, as well as for connecting to the Internet using wired and wireless means, this model can meet the requirements of most

IoT systems. The advantages of the model are simple structure, proven technology and relatively simple implementation of the system. However, its disadvantage is that the cost of the terminal is high and it is difficult to achieve large-scale deployment, and when using a wireless connection, high operating costs are required.

The second model: «Cloud-Terminal application». In this model, mobility has become an element that must be taken into account when designing application systems. To implement this model, the cloud platform needs to organize interaction with the application.

Application development is carried out on iOS, Android and Windows platforms, the background is connected to the cloud platform of IoT, and the application runs on a smartphone, computer and tablet. The model can accommodate complex functions that require significant system resources.

The disadvantage of this model is the increased complexity of the system, the need to provide real-time communication between the application and the client, security requirements and the need to establish various methods of interaction between the application and the terminal, for example, QR code, RFID, Bluetooth communication.

The third model: «Terminal-Gateway-Cloud-Application». Technical means require the endpoint to be connected to the Internet via a network port or via 2G/3G/4G means. But the first option has low mobility, the second has higher operating and maintenance costs, which does not contribute to the promotion of the system.

The gateway of the IoT is usually designed as an «Intermediate Software» for connecting the terminal to the Internet, up, it can be accessed via fiber, Ethernet, Wi-Fi or 2G/3G/4G, and down – via Wi-Fi, Bluetooth, ZigBee and other means of communication. The addition of a gateway allows the terminal to connect to the IoT using some short-range communication protocols, especially short-range wireless protocols such as Bluetooth, Wi-Fi, etc. This can reduce the cost of the terminal while improving usability. In addition, the gateway implements a small local network and various local terminals in this network can work together, which expands the application functions of the IB. But adding a gateway improves the overall performance of the system.

Fourth model: «Sensor-Networks». A sensor network is a network consisting of sensor nodes. Wireless sensor network is the main focus of this model development. In order to save energy, wireless sensor networks are usually designed with a low transmission rate, and it is difficult to provide real-time downlink control. From the point of view of communication, the wireless protocol network for sensors is basically not based on IP, so it is connected during the operation of the platform, the work on converting the existing protocol is also difficult to apply.

Because of these two limitations, wireless sensor networks are more commonly used in monitoring systems. For example, in agriculture and forestry, WSN (Wireless Sensor Network) can be used to monitor the growth environment, temperature, humidity, etc. The WSN can monitor various parameters of rivers and oceans; in the field of intelligent transport, the WSN can control street lights, etc.

With the development of technology, the ZigBee protocol has begun to fully support IPv6, and the development of low-power chips, security technologies, energy and other technologies will continue to contribute to the wider application of wireless sensor networks in more application areas [5].

Architecture of IoT network

There are various models of the IoT architecture [6]: the reference architecture of the Industrial Internet of Things (IIRA), the reference model of the Industry 4.0 architecture (RAMI 4.0) and the reference model of the IoT Cisco. IoT architectures, such as P2413 (standard for the architecture of the IoT), the reference architecture of the Internet of Things (IoT RA), the Telecommunication standardization sector of the International Telecommunication Union (ITU-T), etc. However, no standard reference architecture has been widely adopted, because some IoT architectures are outdated, they do not define new technologies, such as cloud and fog computing, big data. The simplified IoT architecture is shown in Fig. 1.

It is necessary to classify the universal and simple architecture of the Internet of Things – a five-level model. This architecture includes the perception layer, network layer, platforms, application layer and business layer. Different levels include different technologies, depend on different areas and scenarios, and also include different technologies.

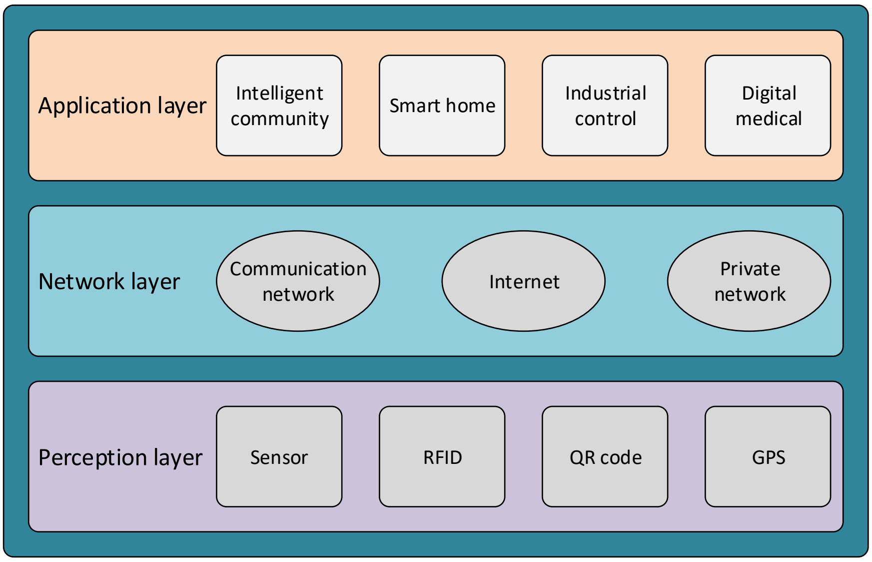

Fig. 1. IoT architecture

For the perception level, the main function is to collect and identify data, as well as transfer the necessary data to the network layer. For the network layer – identification, communication, security and routing are the four main functions. For the identification function at this level, the technology of a single resource identifier (URI), the electronic product code standard (EPC), the ubiquitous code system (UCODE) and IPv6 addressing protocols can be implied. To communicate with other nodes or server servers, it is necessary to use protocols such as power line communication (PLC), near field communication (NFC), ANT+, DASH7 Alliance Protocol (D7A). Standards such as X10, IEEE 802.15.4, Bluetooth with low power consumption, and technologies such as ultra-broadband (UWB), Wi-Fi, long-range broadband network (LORA WAN), 5G and Light Fidelity (Li-Fi), etc. for IoT are used.

There are many nodes with limited capabilities to ensure security, so this is a big problem, in addition, different communication technologies require different security technologies, so at this level, lightweight security technologies can be used, for example, Internet Protocol security (IPsec), transport layer security (TLS), TLS datagram (DTLS), IEEE 1888, etc. For routing, it is very important to find the optimal route for each node.

For the platform layer, also called the service management layer, which is the core of the IoT environment, data modification, processing, and the service discovery function should be taken into account. At this level, technologies such as, CoAP, MQTT, foggy, cloud should be used. At the application level, the main function is to provide services for Internet of Things users. At this level, the services provided are usually divided into four categories according to different application scenarios: identity-related services, information aggregation services, collaboration services, and ubiquitous services.

Two technologies are recommended for the IoT business level: semantics and big data analysis. To achieve semantics, the sensor model language (sensor ML), media types for the sensor markup language (SENML), the Internet of Things database (IOTDB), the RESTful API modeling language (RAML) and Wolfram data removal technologies will be used. To analyze big data, you can use Apache Spark, a distributed processing technology that includes caching, and to improve performance, it uses Apache Apex, Apache Flink and Apache Kafka technologies.

Ways to interact with the IoT

Interaction in IoT networks faces some difficulties: how to make the IoT system distinguish between service objects and avoid the impact of non-service objects; the complexity of the environment, since the environment will not always be stable; hardware failure, it is very important for IoT devices to avoid failures depending on the actual state of the device. There are the following ways of interaction [4].

1. Touch screen interaction. The interactive method is widely used in the field of mobile phones and touch-screen devices, traditional and easy to use, it is not easy to make a mistake.

2. Voice interaction. By recognizing voice prints or initiating a command to interact, this interactive method is commonly used in voice assistants, voice speakers, and other areas. Based on energy consumption and privacy considerations, active voice activation is required.

3. Virtual Reality. This is a new visual perception technology, the technology is interactive, technological and more exciting for a real virtual experience.

4. Biometrics. This technology uses the unique information of a biological individual as a key and information transmission. Unique information usually refers to fingerprints, palm prints, voice prints, facial and iris recognition, etc. This type of interaction is very secure and unique.

5. Somatosensory technology. This type of interaction mainly includes gesture recognition, face recognition, body movement recognition, etc.

6. Information recognition technology. This type of interaction includes image recognition, text recognition, and object recognition. Simple processing and evaluation of information using intelligent recognition. This type of interaction can recognize a wide range of categories, but has limited processing complexity.

7. Traditional buttons. Control the user using physical buttons that directly provide the corresponding functions.

Using the IoT in production quality control

The IoT is a technology that automates input, processing and optimization based on the obtained values of process characteristics reflected in the indicators of industrial and home sensors. The IoT technology allows some user to receive data and report on the status of equipment or processes in real time, monitor the work of industrial and agricultural enterprises [3].

Due to the advantages of the Internet of Things, the Internet of Things technology has a wide range of applications for product quality control. K. Rajalashmi [7] et al. sensors are used to monitor the pH and oxygen content in the water, the purity of the water can be easily calculated using sensors.

In [8], the architecture of the Internet of Things and network protocols for product quality control in the aerospace industry are proposed, and in [9], the model and structure of the Internet of Things network for milk quality control is proposed.

Problems in networks

In real IoT networks, the placement and number of components can also cause some problems when connecting various components to the network [3, 4].

Overload: when the gateway location is placed unreasonably, it will lead to insufficient use of resources, that is, some gateways are overloaded, and some gateway resources are not fully used. This will not only lead to a significant reduction in the use of resources in the border network, but will also cause serious network congestion, which directly affects the quality of service for mobile users. Therefore, when deploying a gateway, it must be placed in a suitable location to achieve load balancing, improve the use of network resources and reduce network congestion, thereby ensuring the quality of user service.

Coverage: each gateway has its own coverage area. If the distance between the terminal device and the gateway is too large, this will lead to a decrease in the reception signal level. Therefore, we need to make sure that all terminal devices are in the gateway's coverage area, but at the same time it is necessary to minimize overlapping coverage and cover most devices with the least number of gateways, thereby ensuring network performance while increasing resource utilization and minimizing gateway deployment costs.

Interference: the location and number of gateways have a big impact on network performance. If the location of the gateways is unreasonable or the density of the gateway deployment is too high, there will be serious interference problems that will affect the SINR received by the terminal equipment., which will lead to a decrease in throughput, as well as an increase in construction costs, so optimizing the location and number of gateways is very important to reduce interference when deploying gateways.

All these problems require the use of system analysis and various optimization methods. Optimization models in infocommunication systems are considered in [10].

Conclusion

1. A brief analysis of the concepts and applications of IoT networks is carried out. Four models of building these networks as variants of component interaction are given: terminal, gateway, cloud, application.

2. Variants of IoT network architectures are presented, including the perception level, network level, platform, application levels and business level. For each level the functions and technologies and protocols used are considered.

3. Seven variants of interaction in IoT networks are considered. The analysis of problems in these networks, such as overload, limited coverage, overload is carried out. To overcome them, it is proposed to use methods and technologies of system analysis and optimization.

References

1. AutoID Labs homepage. [Electronic resource]. URL: https://www.autoidlabs.org.
2. International Telecommunication Union, Internet Reports 2005: The Internet of things[R]. Geneva: ITU, 2005.
3. Roslyakov A.V. Internet of things: textbook manual. Samara: Pgutii, 2015.
4. IoT Platforms. [Electronic resource]. URL: http://www.tadviser.ru/index.php.
5. Four models of IoT systems. [Electronic resource]. URL: https://blog.csdn.net/lihongzhai/article/%20details/80370369.
6. Sun QiBo, IoT: Architecture and key technology research review [J]. Journal of BeiJing University of Posts and Telecommunication, 2010,33(03):1–9.
7. Rajalashmi K. [et al.] IoT based water quality management system [J]. Materials Today: Proceedings, 2020.
8. Visniakou U.A. [et al.] // Siberian Journal of Science and Technology. 2020. № 4. P. 478-482.
9. Visniakou U.A. [et al.] // SA&AI. 2021. № 1. P. 39-44.
10. Nikulshin B.V. [et al.]. System analysis and decision-making in project and management activities: an educational and methodological manual on the academic discipline «Theory of system analysis and decision-making in infocommunications» for students of the II stage of the specialty «Systems and networks of infocommunications» of all forms of education. Minsk: BGUIR, 2021.