Wireless Networks

Haibin Yu · Peng Zeng · Meng Zheng ·
Chi Xu · Xi Jin · Wei Liang

Performance Controllable Industrial Wireless Networks

Springer

ireless Networks

Series Editor

Xuemin Sherman Shen, University of Waterloo, Waterloo, ON, Canada

The purpose of Springer's Wireless Networks book series is to establish the state of the art and set the course for future research and development in wireless communication networks. The scope of this series includes not only all aspects of wireless networks (including cellular networks, WiFi, sensor networks, and vehicular networks), but related areas such as cloud computing and big data. The series serves as a central source of references for wireless networks research and development. It aims to publish thorough and cohesive overviews on specific topics in wireless networks, as well as works that are larger in scope than survey articles and that contain more detailed background information. The series also provides coverage of advanced and timely topics worthy of monographs, contributed volumes, textbooks and handbooks.

Haibin Yu • Peng Zeng • Meng Zheng • Chi Xu •
Xi Jin • Wei Liang

Performance Controllable Industrial Wireless Networks

Springer

Haibin Yu
Shenyang Institute of Automation,
Chinese Academy of Sciences
Shenyang, Liaoning, China

Peng Zeng
Shenyang Institute of Automation,
Chinese Academy of Sciences
Shenyang, Liaoning, China

Meng Zheng
Shenyang Institute of Automation,
Chinese Academy of Sciences
Shenyang, Liaoning, China

Chi Xu
Shenyang Institute of Automation,
Chinese Academy of Sciences
Shenyang, Liaoning, China

Xi Jin
Shenyang Institute of Automation,
Chinese Academy of Sciences
Shenyang, Liaoning, China

Wei Liang
Shenyang Institute of Automation,
Chinese Academy of Sciences
Shenyang, Liaoning, China

ISSN 2366-1186 ISSN 2366-1445 (electronic)
Wireless Networks
ISBN 978-981-99-0388-7 ISBN 978-981-99-0389-4 (eBook)
https://doi.org/10.1007/978-981-99-0389-4

This Springer imprint is published by the registered company Springer Nature Singapore Pte Ltd.
The registered company address is: 152 Beach Road, #21-01/04 Gateway East, Singapore 189721, Singapore

Preface

The rapid proliferation of information and communications technology has ushered in a new era of intelligent manufacturing in industrial automation. The wireless communication technology is widely recognized as one of the key enablers to support intelligent manufacturing. Industrial automation applications typically require high reliability and low-latency deterministic communication. However, wireless communication in industrial settings is hindered by strictly limited communication resources as well as the shared and error-prone nature of wireless communication channels. Furthermore, the harsh industrial environment poses significant challenges towards achieving reliable and real-time communication in industrial wireless networks.

Resource optimization methods are vital to ensuring the deterministic performance of industrial wireless networks. Existing resource optimization methods mainly adopt the isolated resource optimization methods, which are inherently local-optimal and lead performance uncontrollable. The focus of this book is to give an introduction on performance controllable industrial wireless networks including the state-of-the-art resource optimization methods based on comprehensive literature study. In addition, the joint resource optimization methods for industrial wireless networks are also presented which would benefit researchers in the areas of industrial automation and Industrial Internet of Things. To gain the most from this book, readers should have a fundamental grasp of wireless communication, scheduling theory, and convex optimization.

Below, we provide a summary of each chapter.

- Chapter 1. Overview of Industrial Wireless Networks. This chapter introduces the background and the fundamentals of industrial wireless networks.
- Chapter 2. Literature Study of Resource Optimization In Industrial Wireless Networks. This chapter discusses the resource optimization problem formulations in industrial wireless networks and reviews the state-of-the-art methods for resource optimization.

- Chapter 3. Joint Resource Optimization Methods for Industrial Wireless Networks. This chapter first analyzes the coupling between network resources and proposes a loosely coupled decomposition-based dynamic resource regulation framework. Then, convex optimization-based distributed solution algorithms are presented.
- Chapter 4. Temporal-Spatial-Frequency Resource Allocation. This chapter introduces the temporal-spatial-frequency resource allocation methods by employing cognitive radio and energy harvesting technologies to enhance the real-time and reliability performance of industrial wireless networks.
- Chapter 5. No-Collision Scheduling Methods for Real-Time Transmissions. This chapter introduces real-time scheduling algorithms to allocated time and frequency resources to eliminate transmission collisions in industrial wireless networks.
- Chapter 6. Cross-Layer Flow Control Methods for Reliable Transmissions. This chapter introduces a cross-layer flow control method by jointly optimizing routing and MAC layer retransmissions to achieve reliable communication.
- Chapter 7. Implementation Architecture and Supporting Technologies. This chapter summarizes the implementation requirements of the methods discussed in Chapters 4–6. Then, the detailed implementation architecture and key supporting technologies are described.

Shenyang, Liaoning, China

Haibin Yu
Peng Zeng
Meng Zheng
Chi Xu
Xi Jin
Wei Liang

Acknowledgments

We would like to thank Dr. Changqing Xia, Dr. Chunhe Song, Dr. Tianyu Zhang, Dr. Jintao Wang, Dr. Yang Xiao, and Dr. Yingchang Liang for their helpful discussions and contributions to this book.

This book was also supported in part by the National Natural Science Foundation of China (62022088, 62133014, 62173322, 92267108); in part by the International Partnership Program of Chinese Academy of Sciences (173321KYSB20200002); in part by the Youth Innovation Promotion Association CAS (Y2021062, 2019202); in part by the LiaoNing Revitalization Talents Program (XLYC1902110); in part by the Science and Technology Program of Liaoning Province.

Contents

Chapter 1
Overview of Industrial Wireless Networks

Throughout the development of analog and digitalization, industrial control systems are rapidly developing in the direction of networking and wireless technology. It is expected that industrial wireless networks (IWNs) will become a key component of industrial control systems. In this chapter, we first introduce the background of IWNs by analyzing the development of industrial control systems and describing the limitations of industrial wired networks and the increasing deployment of IWNs. Afterwards, the fundamentals of IWNs are discussed, including the IWN components, representative communication requirements along with the key challenges to achieve them.

1.1 Background of IWNs

1.1.1 Industrial Control Systems

Industrial automation systems are changing because of the deep integration of information and communication technology (ICT) and industrial operation technology (OT). Emerging network and communication technologies are being applied and deployed in the management level, control level, and field equipment level from factories to enterprises. To this end, fully distributed network-integrated control systems and enterprise management information systems are being built. The development of industrial control systems has broadly gone through the following three stages [1].

In the first stage, from the 1960s to the 1970s, analog control systems dominated, using 2-wire cables with 4–20 mA current or 1–5 V voltage to transmit point-to-point signals among different sensors (shown Fig. 1.1). This approach suffers from high wire cost, low signal accuracy, and poor anti-interference properties, and thus has been gradually eliminated as technology progressed.

H. Yu et al., *Performance Controllable Industrial Wireless Networks*, Wireless Networks, https://doi.org/10.1007/978-981-99-0389-4_1

Fig. 1.1 Analog control system architecture

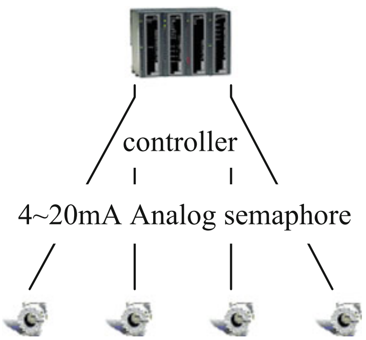
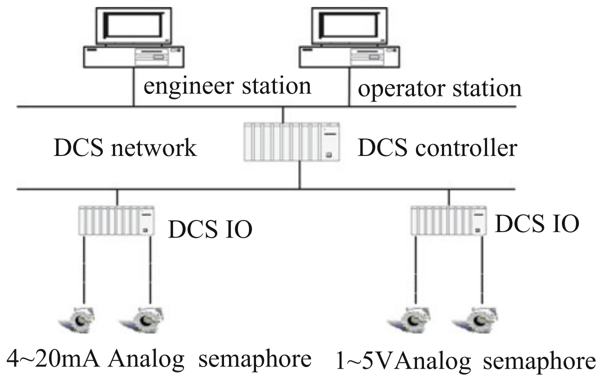


Fig. 1.2 Distributed control system architecture



In the second stage, from the 1970s to the 1990s, with the introduction of digital communication technology into control systems, industrial wired networks emerged (shown in Fig. 1.2). The mechanism of signal transmission between sensors and field control stations, namely using analog current or voltage signals to transmit sensor signals, is comparable to that of the earlier stage. However, the use of serial data interface standards, e.g., RS-232 and RS-485, enables the digital communication among field control stations.

In this stage, distributed control systems (DCSs) emerged and gained widespread adoption. Centralized management and decentralized control both play critical roles in DCS implementation. That is, management and control are performed in a separated manner. Specifically, management machines deployed in the upper layer are used for centralized monitoring and functional management. Many other machines deployed in the lower layer are scattered throughout the site to achieve distributed control. These machines across different layers are connected through the control networks to exchange necessary information.

This distributed control architecture effectively overcomes the defects of centralized control systems which require high processing capability and high reliability of the controllers. In the centralized control systems, some distributed control functions can be realized benefiting from the development and application of networking technology. To ensure monopolistic functioning, however, many DCSs

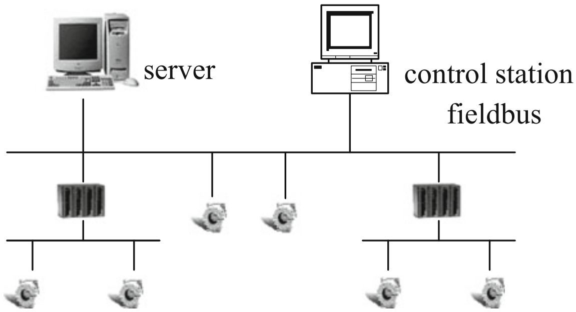


Fig. 1.3 Fieldbus control system architecture

manufacturers create their own dedicated closed form for their control networks. Thus, it is difficult to achieve network interconnection and information sharing between DCSs from different manufacturers, as well as those between DCSs and Internet. DSC is still a form of closed or dedicated distributed control systems where the interoperability between systems is poor. Therefore, users put forward the urgent requirements of open information, unified standards and lower cost for emerging networked control systems.

In the third stage, starting from the 1990s, fieldbus control systems (FCSs) were created, in line with the development of digital communication. Fieldbus is an all-digital, open two-way communication network connecting intelligent field devices and control rooms. The continuous development of fieldbus motivates its application in most local measurement and control networks, which can connect with Internet by gateways and routers. As shown in Fig. 1.3, open and interoperable networks established by fieldbus are able to interconnect different controllers and instrumentation devices in the industrial field. At the same time, the control functions are decentralized to the industrial field, which can reduce the installation and maintenance costs. Therefore, fieldbus control systems are essentially distributed control systems with open information, interoperability and fully decentralization.

In the twenty-first century, FCSs have taken over as the standard industrial control system.

1.1.2 Limitations of Industrial Wired Networks

Observing from the development of industrial control systems, it reveals that industrial networks have evolved into the system's primary enabling technology. The industrial network plays the critical role in the entire industrial control system, which is comparable to that of the central nervous system in human body. Industrial wired networks (e.g., fieldbus) have been widely applied in industry. Compared to the traditional point-to-point communication method, fieldbus technology saves money and lowers the cost of design, installation and maintenance. Fieldbus technology, which breaks down information silos and enables the integration of management control and remote monitoring, also offers comprehensive system status information for control systems. It also disseminates all system control functions to the industrial field.

However, existing industrial wired networks like fieldbus still have several limitations in light of the complicated industrial application environment and increasing demands for low-cost and flexible use of industrial production. Some representative limitations are given as follows.

- High wiring cost

  Wired communication requires the design of communication cable layout, wherein the cost of this work covers both the cable and its construction costs as well as the cost of corresponding accessories. It is reported that the cost of cable and its installation in fieldbus is generally in the range of \$50–\$100 per foot. This cost may reach \$2000 per foot in certain harsh environments. Therefore, a significant amount of the cost of wired industrial communication systems is accounted for by the cable and the cost of installation. More significantly, the price of communication cable and the cost of installation are both necessary costs which are challenging to be reduced.
- High maintenance cost

  The use of cables in industrial wired networks also adds necessary maintenance and operating costs. The inspection, testing, and troubleshooting of lines as well as the repair and replacement of cables will take a lot of time, labor, and material resources since cables are susceptible to aging, breakage, or failure in industrial environment. Therefore, cable maintenance is another key factor increasing the maintenance cost of industrial wired networks. Particularly, greater losses are caused if manufacturing is stopped or other major effects result from the cable failing.
- High failure rate at the connection point

  In industrial wired networks, communication cables and devices are connected by connectors, where the connection points between cables and devices are particularly vulnerable. The connecting points can be damaged and malfunctioned as a result of abrasion, collision, and vibration during the production process. This can interrupt network communication, which further affects the production process monitoring and control. Then, checking and troubleshooting the connection points will further enhance the production cost.
- Limitations of practical application

  Industrial wired networks have several limitations when deployed in mobile industrial applications and harsh industrial environments. First, the wired communication method is not suitable for mobile scenarios, e.g., mobile robots and Automated Guided Vehicles (AGVs). Second, a large number of cable connections are difficult to deploy when massive sensors are used for ubiquitous sensing. Similarly, it is quite challenging to deploy cables in harsh industrial environments, e.g., high temperature and heavy vibration.

Therefore, the inherent defects of industrial wired network technologies such as Fieldbus limit the application of industrial networks for the monitoring and control in production process. There is an urgent need to develop new industrial network technologies with low cost, high efficiency and high flexibility. In this case, IWNs are developed.

1.1.3 Development of IWNs

The significant benefits that wireless communication technology has brought to industrial company production are being recognized and highly valued by an increasing number of advanced industrial nations. In the beginning of this century, the U.S. President's Council of Advisors on Science and Technology pointed out that the deployment of industrial wireless control can lower energy consumption and pollution emissions of U.S. industrial production by 10% and 25%, respectively [2]. In 2004, initiated by the U.S. Department of Energy, Honeywell, RAE and more than 70 major companies participated in the establishment of Wireless Industrial Networking Alliance (WINA) [3] which is dedicated to promoting the application of wireless communication technologies in industry. The members of WINA consist of technology suppliers, end users, industry organizations, system integrators, etc.

Then, three industrial wireless networking technologies for process automation, including WirelessHART, WIA-PA, and ISA100.11a, were developed in Europe, China, and the United States, respectively. Furthermore, they are standardized by International Electrotechnical Commission (IEC) as international standards.

1.1.3.1 WirelessHART

WirelessHART is the first open, interoperable industrial wireless communication standard specifically designed for the process industry. It was released by the HART Foundation in September 2007. In September 2008, WirelessHART was released as a publicly available specification IEC/PAS 62591. In March 2010, WirelessHART was officially released as the official international standard IEC 62591 [4], which is the first IEC international standard for industrial automation.

The main features of WirelessHART are summarized as follows.

- Reliability. WirelessHART defines a self-organizing, adaptive and self-healing mesh network that provides redundant transmission paths for devices and automatically repairs failed transmission paths. At the same time, WirelessHART uses direct sequence spread spectrum and frequency hopping technology, and applies time synchronization-based time division multiple access (TDMA) to provide reliable data transmission for complex industrial environments.
- Compatibility. WirelessHART is compatible with existing HART systems, providing a safe, easy and reliable user experience for interconnecting with HART products.

- Security. WirelessHART uses multiple security keys (including join key, network key and session key) for encryption and authentication, and changes keys periodically to guarantee the security of the network and data in real time.

1.1.3.2 WIA-PA

WIA-PA was proposed by the China Industrial Wireless Alliance in 2006. It is a highly reliable, ultra-low power, multi-hop intelligent wireless sensor network technology that provides an intelligent network routing mechanism with self-organization and self-healing capability and can maintain high reliability and strong stability of network performance in response to dynamic changes in industrial field. In October 2008, it was released as a public specification IEC/PAS 62601. In October 2011, WIA-PA officially became an international standard IEC 62601 [5]. In December 2015, WIA-PA was officially accepted as a European standard after the joint vote of IEC and the European Committee for Electrotechnical Standardization (CENELEC).

The main features of WIA-PA are summarized as follows.

- Reliability. To overcome the interference in industrial field and improve the network reliability, WIA-PA proposes key technologies such as adaptive frequency hopping communication, TDMA-based deterministic communication, and redundant mesh network. Among them, adaptive frequency hopping adopts three different frequency hopping techniques, namely adaptive frequency switching, adaptive frequency hopping and timeslot hopping.
- Real-time. To meet the strict requirements of real-time industrial applications, WIA-PA proposes a hybrid access technology of TDMA and CSMA, which improves the real-time performance of the system while ensuring reliability.
- Low-power. To reduce power consumption and support long-term unattended operation of devices, WIA-PA proposes aggregation and disaggregation technology, which can effectively reduce the number of data transmissions by aggregating and disaggregating data at different protocol levels in field devices and routing devices to reduce the network burden and system power consumption.
- Scalability. WIA-PA employs a hierarchical topology with hybrid star and mesh, which can be expanded according to application requirements. Correspondingly, WIA-PA defines a combined centralized and distributed network management architecture, which can ensure the effectiveness and reliability for large-scale networks.
- Compatibility. WIA-PA is compatible with the prevalent IEEE STD 802.15.4 and other communication technologies, e.g., HART, WirelessHART, fieldbus.
- Security. WIA-PA provides three types of security services, including data integrity, confidentiality and security authentication. It performs key management and device authentication via a specially configured security manager.