IF : 4.547 | IC Value 80.26 VOLUME-6, ISSUE-6, JUNE-2017 • ISSN No 2277 - 8160

Original Research Paper Engineering

Recent and Emerging Technologies for Implementation of Reliable and Secure Industrial Wireless Networks: An Overview

Sejal Raval Lecturer in I. C. Engineering Department, Government Polytechnic, Ahmedabad.

ABSTRACT Today, with continuing improvements in WiFi/802.11 technology, including higher bandwidth protocols, IP based networking and faster roaming between access points, users are finally able to use WiFi to construct a reliable mobile wireless communication system in industry that takes advantage of all the latest innovations to deliver substantial cost savings, easier set up and maintenance, and greater operational efficiency.

When wireless links are included in industrial network, reliability and timing requirements are stringent and more difficult to meet, due to the adverse properties of the radio channels. In this paper, we thus discuss some key issues coming up wireless industrial communication systems :1)fundamental problems like achieving timely and reliable transmission despite channel errors; 2) the usage of existing wireless technologies for this specific field of applications; and 3) the creation of hybrid systems in which wireless stations are included into existing wired systems.

KEYWORDS : WiFi Wireless Networking protocol IEEE 802.11, IP Internet Protocol

INTRODUCTION

With the success of wireless technologies in consumer electronics, standard wireless technologies are envisioned for the deployment in industrial environments as well. Industrial applications involving mobile subsystems or just the desire to save cabling make wireless technologies attractive. Nevertheless, these applications often have stringent requirements on reliability and timing. In wired environments, timing and reliability are well catered for by existing communication systems, which are a mature technology designed to enable communication between digital controllers and the sensors and actuators interfacing to a physical process.

Wireless technologies significantly used in voice/video transmission or Internet access at places without cabled networking infrastructure or while being on the move. Wireless technologies have also been identified as a very attractive option for industrial and factory automation, distributed control systems, automotive systems and other kinds of networked embedded systems [1], [2], with mobility, reduced cabling and installation costs, reduced danger of breaking cables, and less hassle with connectors being important benefits, and on the other hand the unfriendly error properties of the wireless channel significantly challenge real-time and reliability. Consequently, significant research is needed to adapt existing wireless technologies and protocols to industrial settings, or, when this is not sufficient, to develop new ones.

However, outdoor and industrial WiFi applications do have some special demands when it comes to protecting radios and other electronics from manmade hazards, such as electrically noisy or unstable power sources and intense radio frequency interference; and natural dangers, including lightning, and static electricity also environmental issues such as extreme temperatures, vibration, dust and humidity.

INDUSTRIAL NETWORK BASICS

Although recent advances in industrial networking such as the incorporation of Ethernet technology have started to blur the line between industrial and commercial networks, at their cores they each have fundamentally different requirements.

The most essential difference is that industrial networks are connected to physical equipment in some form and are used to control and monitor real world actions and conditions [3]. This has resulted in emphasis on a different set of Quality of Service (need for strong determinism and real time data).

TABLE – 1
COMPARISION OF INDUSTRIAL V/S CONVENTIAONAL NETWORK

	Industrial	Conventional
Function	Control of physical equipment	Data processing and transfer
Applicable Domain	Manufacturing, processing and utility distribution	Corporate and home environments
Failure Severity	High	Low
Reliability Required	High	Moderate
Round Trip Times	250 µs - 10 ms	50+ ms
Data Composition	Small packets of periodic and aperiodic traffic	Large, aperiodic packets
Operating Environment	Hostile conditions, often featuring high levels of dust, heat and vibration	Clean environments, often specifically intended for sensitive equipment

Running industrial applications with wireless technologies can be especially challenging. Since wireless channels are prone to possible transmission errors caused by either channel outages and/or interference, the real time and reliability requirements are more likely to be jeopardized than they would be over a wired channel. This is one of the key issues to be resolved in usage of wireless technologies in industrial applications.

These effects can be compensated by designing robust and loss tolerant applications and by improving the channel quality when designing a wireless protocol.

Issues related to wireless network

In Industry wired IT network, which is used for data storage and retrieval. When establishing industrial network it must be coexist with IT network and we need to address some of the issue stated below.

1: Security -Security is the first issue to arise when implementing wireless in a plant network. In the plant engineers want to ensure uninterrupted production, and that security measures are in place to protect their process and plant floor equipment. It is also necessary to ensure that systems deployed in the plant coexist well with networks in the rest of the organisation and security of corporate information is also ensured.

Modern encryption techniques can be utilised to avoid someone interpreting your data maliciously. Filtering and strong authentication allow only authorised devices on the network.

2: Capacity-To know your industrial network demand several parameters like the environment where network is to be implemented, what are the distances and speeds required?, whether mobile worker access necessary? Application is indoor or outdoor? Moving, rotating, or vibrating machinery? To be noted down and then we be able to articulate what traffic network is expected to support. There are many types of wireless, each suited for different applications.

Some applications having production lines using 1000 I/O points with millisecond scan rates but Wireless technologies today cannot deal with this level of capacity.

3: Reliability -In the same way that a user would not run cable next to drives because of interference, wireless interference must be considered. Wireless simply requires different steps. Factors like line of sight and selection of radio, antenna and cable become important. Consider the specific performance features of these devices against your application.

Challenges in wireless industrial implementation

1: Signal coverage – WiFi has limited signal coverage, so multiple access points are necessary for full coverage throughout an entire warehouse. It is critical to ensure that the clients can roam smoothly between these access points with minimal handover time.

2: Power supply quality – Robots and other mobile devices often have very limited space and weight-carrying capacity for a WiFi module, and the power system usually cannot be properly grounded. So system integrators must dedicate considerable effort to ensuring onboard devices cannot be affected by the inrush current that is created by the robot's motors – otherwise there is even a risk that electronics could burn out or suffer significantly reduced lifespan.

3: Communication blockage – Unfortunately, metal is extremely effective at blocking radio signals, and large metal objects, such as vehicles and metal shelving, are common in industrial, freight and transport environments. System integrators need wireless expertise and experience to devise the most efficient positioning of APs and antennas, in order to avoid the risk of communication blind spots caused by stationary or moving metal objects.

4: System adaptability – There are many kinds of warehouses; some require special environments such as very high or low humidity, or sub-zero storage temperatures. System integrators need to be able build a system that is adaptable to different customer needs and many different environments. So it is important to choose hardware that can handle extreme temperature ranges and has good ingress protection to keep out dust and moisture.

5: Wireless interference-The wireless medium is an open medium and without countermeasures, it is easy for an attacker to eavesdrop, to insert malicious packets, or to simply jam the medium, this way challenging reliable and timely transmission. Security or accountability was not the main focus in the many of existing communication protocols. [4], [5]. The recent trend to connect industrial network to the Internet by means of gateways has led to research toward securing the gateway [4], [6].

6: Energy supply-In some network systems, the same cable is used for communication purposes and to supply a station with energy. So for wireless alternative ways needed to supply energy. Some options are wireless energy transmission [7], [8], energy-scavenging methods [9], or using batteries. However, the main concern was real-time communications, not energy efficiency. There are efforts to combine both targets [10].

WIRELESS TECHNOLOGY IN INDUSTRIAL NETWORK

The wireless transmission used in large scale cellular networks such as UMTS, to data oriented solutions like wireless LANs (WLANs), wireless personal area networks (WPANs) and wireless sensor networks. WLAN systems, like the IEEE 802.11 family of standards [11]–[13], are designed to provide users with high data rates (tens of megabits per second) over ranges of tens to hundreds of meters. WPAN systems, such as Bluetooth (BT) [14], [15] and IEEE 802.15.4 [16], [17] have been designed for connecting devices wirelessly while taking energy efficiency into account. They support medium data rates in the order of hundreds of kilobits per second to a few megabits per second and have ranges on the order of a few meters.

A. BT Technology/IEEE 802.15.1

BT was originally designed as a cable replacement technology aimed at providing wireless connectivity for consumer devices in an *ad hoc* fashion [18]–[22]. The BT used in the unlicensed industrial, scientific, and medical (ISM) band at 2.4 Ghz.

BT networks are organized into piconet in which a "master" unit coordinates the traffic to and from up to seven active "slave" units. The master unit originates the request for a connection setup. Within a single piconet, the various slave units can only communicate with each other via the master. Nevertheless, every BT unit can be a member of up to four different piconets simultaneously. A formation in which several piconets are interlinked in such a manner is called a scatternet[23].

Piconet traffic is strictly organized into a time-division multiple access (TDMA)/duplex scheme In this scheme [24]. the master is only allowed to start transmitting in odd-numbered time slots (each slot is 625 s long), while slaves can only respond in even-numbered slots after having been polled by a master packet.

On the physical layer (PHY), data is Gaussian frequency shift keying (GFSK) modulated at 1 M/s and transmitted with a power of 0 dBm (1 mW).

On the data link layer, a distinction is made between asynchronous connectionless (ACL) and synchronous connection-oriented (SCO) packets:

SCO links, support real-time traffic by reserving time slots at periodic intervals. Retransmissions are not allowed with these types of links, but in BT version 1.2/2.0, "extended" SCO links have been introduced where a limited number of retransmissions can be made.

Because of the short range of BT and the small number of slaves that are active at any given time, several independent BT piconets will most likely coexist on a factory floor.

In order to obtain a good throughput and have low interference, it is disadvantageous to use short packet types.

Security is supported in BT by the specification of authentication and encryption. The most recent development for BT is BT version 2.0 BT version 2.0 [25]. has enhanced data rates using $\pi/4$ DQPSK and 8DPSK modulation schemes in addition to the traditional GFSK modulation scheme. The transmission rate resulting from these enhancements is about three times faster than it was in previous versions of BT.

B. IEEE 802.15.4

The IEEE 802.15.4 standard [16] was finalized in October 2003 and specifies the characteristics of the physical layer and the MAC layer of a radio networking stack. The goal of this standard was to create a very low cost, very low power, two-way wireless communication solution that meets the unique requirements of sensors and control devices [16], [17]. IEEE 802.15.4 has been specifically developed for use with applications in which a static network exists that has many infrequently used devices that transmit only small data packets. Such applications are exactly what many industrial environments would require.

IEEE 802.15.4 has been placed in unlicensed frequency bands. The IEEE 802.15.4 standard has also been specified for use in the 868-

MHz ISM band in Europe and in the 915-MHz ISM band in North America.

The IEEE 802.15.4 standard differentiates between two different kinds of devices. A *full-function device* (FFD) can become a network coordinator and can work with other FFDs in a peer-to-peer fashion. *Reduced-function devices* (RFD), on the other hand, are always associated with one of these FFDs and are limited to exchanging data with this device alone.

Among RFDs there is no peer-to-peer communication possible. All devices have a 64-b address, but it is possible for RFDs to obtain a 16-b shorthand address from their coordinator FFD.

With respect to the MAC protocol used by the IEEE 802.15.4 standard, there are two different modes of operation. In *unbeaconed mode*, all stations use an unslotted CSMA variant. Having a backoff time facilitates the avoidance of collisions. In beaconed mode, the network coordinator imposes a superframe structure, which uses slotted CSMA-CA variant, which incurs more overhead than the unslotted variant.

Data packets are acknowledged and the protocol supports retransmissions, but there is no FEC coding. In the beaconed mode, the throughput is smaller than in the unbeaconed mode, in which no beacon frames exist and the unslotted

Similar to BT, IEEE 802.15.4 uses low transmits power levels. In addition to this, IEEE 802.15.4 also uses very short symbol rates (up to 62.5 k symbols/s), allowing the increased delay spread found in industrial plants not to cause a problem.

For security purposes, IEEE 802.15.4 provides authentication, encryption, and integrity service. The developer can choose between no security, an access control list, and a 32–128-b Advanced Encryption Standard (AES) encryption with authentication.

C. IEEE 802.11 Technologies

IEEE 802.11 is composed of a number of specifications that primarily define the physical and MAC layers of WLAN systems [11]–[13], [26] The IEEE 802.11 MAC suggests the IEEE 802.2 logical link control (LLC) [27] as a standard interface to higher layers. Since IEEE 802.11 is a WLAN standard, its key intentions are to provide high throughput and a continuous network connection. Technologies for wireless connections in industrial deployments, only the most common variations and extensions of IEEE 802.11 systems include the general 802.11 MAC, IEEE 802.11a, IEEE 802.11b, and IEEE 802.11g are discussed here. The main parameters of IEEE 802.11 a/b/g are the following.

IEEE 802.11a is placed in 5-GHz bands in Europe (5.15–5.35 GHz and 5.47–5.725 GHz) and in the United States (UNII bands, 5.15–5.35 GHz and 5.725–5.825 GHz). Over the whole spectrum, this allows for 21 systems to be running in parallel in Europe and eight in the United States The IEEE 802.11a physical layer (PHY) is based on the multicarrier system orthogonal frequency-division multiplexing (OFDM) [29]. The maximum user-visible rates depend on the packet sizes transmitted. Larger the packet size better the user rate achieved. The throughput of 2.6 Mb/s is used for industrial applications, as small packet sizes are dominant in industrial networks.

IEEE 802.11b is a high-rate extension to the original IEEE 802.11 DSSS mode and thus uses the 2.4-GHz ISM band. Although in principle either 11 or 13 different center frequencies can be used for the DSSS (depending on whether you are in the United States or in Europe), only three systems can actually operate in parallel. The maximum user data rates are 7.11 Mb/s in the case of Ethernet packets and 0.75 Mb/s in the case of packets with user payloads of 60 B in length.

IEEE 802.11g is an extension to the IEEE 802.11b specification and is consequently also placed in the 2.4-GHz band. It supports four different physical layers of which two are mandatory Because of the different frequency band, the maximum user transmit rates are about 26 Mb/s for Ethernet packets and about 2 Mb/s for packets with user payloads of 60 B.

IEEE 802.11 has been specifically optimized to transmit large data files, therefore it can be seen that when transmitting packets that contain small payloads, throughput values are significantly reduced. This reduction is due to the comparably large overhead of IEEE 802.11 packets and the different parameters present in the CSMA protocol

IEEE 802.11 employs immediate MAC-layer acknowledgment and retransmissions.

To organize the traffic on the radio link, the IEEE 802.11 MAC provides two coordination functions. The first of these coordination functions, the distributed coordination function (DCF), is mandatory and requires that all stations compete for the channel according to a CSMA-CA

The second coordination function, point coordination function (PCF) [11], is not mandatory and is designed to provide time bounded services by means of subdividing time into (variable-length) super frames. The use of PCF is not very widespread and it has a reputation of being slightly inefficient.

For security, IEEE 802.11 WLAN's support several authentication processes which are listed in the specification.

CONCLUSIONS

Wireless technologies can bring many benefits to industrial applications, one of them being the ability to reduce machine setup times by avoiding cabling. The market offers mature wireless solutions, such as the IEEE 802.11 standard, the IEEE 802.15.4 standard, or BT. So far, however, wireless technologies have not gained widespread acceptance on the factory floor. One reason for this lack of acceptance is the difficulty in achieving the timely and successful transmission of packets over error-prone wireless channels, but in manufacturing, Ethernet is now widely used in control; and where there is Ethernet, wireless often follows. Some wireless devices are sophisticated enough to act as managed switches, providing intelligent packet filtering. Some support deterministic applications, and can provide a high level of flexibility, speed, precision and predictability.

Many real-world wireless applications have actually improved efficiency and reliability by trading their wires for antennas. Applications with moving equipment can dramatically reduce costs, downtime, and maintenance using wireless.

REFERENCES:

[1]. A. Willig, K. Matheus, and A. Wolisz, "Wireless technology in industrial networks," Proc. IEEE, Jun. 2005.
[2]. J. R. Moyne and D. M. Tilbury, "The emergence of industrial control networks for manufacturing control, diagnostics, and safety data," Proc. IEEE, Jan. 2007.
[3]. K. Stoufer, J. Falco, and K. Scarfone, "Guide to industrial control systems security," National Institute of Standards and Technology, Final Public Draft, Sep 2008.
[4]. C. Schwaiger and T. Sauter, "Security strategies for field area networks," in Proc. IEEE 2002
[5]. A. Treytl, T. Sauter, and C. Schwaiger, "Security measures for industrial fieldbus system State of the art and solutions for IP-based approaches," in Proc. 2004 IEEE Int. (WFCS).
[6]. C. Schwaiger and T. Sauter, "A secure architecture for fieldbus/internet gateways," in Proc. 8th IEEE Int. Conf. (ETFA), 2001.
[7]. J. Hirai, T.-W. Kim, and A. Kawamura, "Practical study on wireless transmission of power and information for autonomous decentralized manufacturing system," IEEE Trans. Ind. Electron.,Apr. 1999.
[8]. D. Dzung, C. Apneseth, G. Scheible, and W. Zimmermann, "Wire- less sensor communication and powering system for realtime industrial applications," presented at the WFCS 2002.
[9]. S. Roundy, D. Steingart, L. Frechette, P. Wright, and J. Rabaey, "Power sources for wireless sensor networks," presented at the Wireless Sensor Networks 1st Eur. Workshop (EWSN 2004).
[10]. A. Stankovic, T. F. Abdelzaher, C. Lu, L. Sha, and J. C. Hou, "Real-time communication and coordination in embedded sensor networks," Proc. IEEE, Jul. 2003.
[11]. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY)

Specifications, 1999
[12]. Part 11: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications: High Speed Physical Layer in the 5 GHz Band, IEE1999.
[13]. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Higher Speed Physical Layer (PHY) Extension in the 2.4 Ghz Band, IEEE1999.
[14]. Specification of the Bluetooth System, Version 1.1, Dec. 1999.
[15]. J. C. Haartsen, "The Bluetooth radio system," IEEE Pers. Feb. 2000.
[16]. Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low Rate Wireless Personal Area Networks (LR-WPAN's), IEEE, Oct. 2003.
[17]. E. Callaway, "Home networking with IEEE 802.15.4: A developing standard for low-rate wireless personal area networks," IEEE Commun. Mag., Aug. 2002.
[18]. http://www.bluetooth.com
[19]. J. Haartsen, "Bluetooth—The universal radio interface for ad hoc, wireless connectivity," Ericsson Rev., 1998.
[20]. J. Bray and C. F. Sturman, Bluetooth: Connect Without Cables. Eaglewood Cliffs, NJ: Prentice-Hall, 2000.
[21]. C. Bisdikian, "An overview of the Bluetooth wireless technology," IEEE Commun. Mag., Dec. 2001.
[22]. Bluetooth 1.2 Core Specification, Nov. 2003.
[23]. G. Miklòs, A. Ràcz, Z. Turànyi, A. Valkò, and P. Johansson, "Performance aspects of Bluetooth scatternet formation," in Proc. 1st ACM Int. Symp. Mobile Ad Hoc Networking and Computing, 2000.
[24]. A. C. V. Gummalla and J. O. Limb. (2000) Wireless medium access control protocols. IEEE Commun. Surveys Tuts.
[25]. Bluetooth 2.0 Core Specification cdr., Nov. 2004.
[26]. B. O'Hara and A. Petrick, IEEE 802.11 Handbook—A Designer's Companion. New York: IEEE Press, 1999
[27]. International Standard ISO/IEC 8802-2:1998: IT—Telecommunications and Information Exchange Between Systems—LAN/MAN—Specific Requirements—Part 2: Logical Link Control, 1998.
[28]. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, Amendment 5: Spectrum and Transmit Power Management Extensions in the 5 GHz Band in Europe, Oct. 2003.
[29]. R. van Nee and R. Prasad, OFDM for Wireless Multimedia Communications.
[30]. Andreas Willig, Recent and emerging topics in Wireless industrial communications: A selection.
[31]. Brendan Galloway and Gerhard P. Hancke, Introduction to Industrial control networks.
[32]. http://www.belden.com, Designing and securing industrial wireless network.
[33]. Adrienne Lutovksy, Planning and implementing secure industrial wireless networks.
[34]. Jeffrey Ke, How to build reliable low cost Wifi networks for industrial internet of things, Nov. 2015.