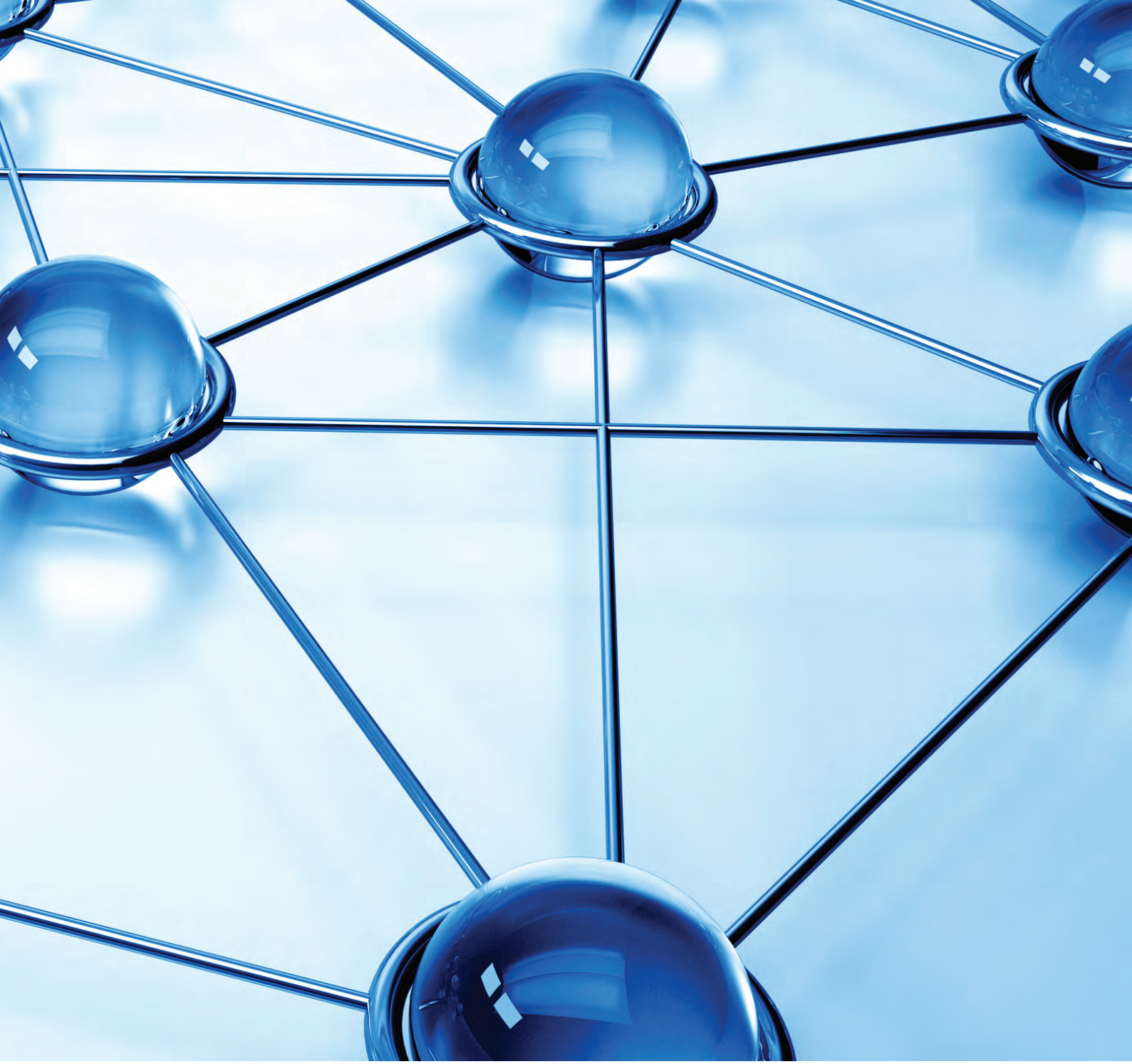


White Paper

Internet of Things: Wireless Sensor Networks

Executive summary

Today, smart grid, smart homes, smart water networks, intelligent transportation, are infrastructure systems that connect our world more than we ever thought possible. The common vision of such systems is usually associated with one single concept, the internet of things (IoT), where through the use of sensors, the entire physical infrastructure is closely coupled with information and communication technologies; where intelligent monitoring and management can be achieved via the usage of networked embedded devices. In such a sophisticated dynamic system, devices are interconnected to transmit useful measurement information and control instructions via distributed sensor networks.

A wireless sensor network (WSN) is a network formed by a large number of sensor nodes where each node is equipped with a sensor to detect physical phenomena such as light, heat, pressure, etc. WSNs are regarded as a revolutionary information gathering method to build the information and communication system which will greatly improve the reliability and efficiency of infrastructure systems. Compared with the wired solution, WSNs feature easier deployment and better flexibility of devices. With the rapid technological development of sensors, WSNs will become the key technology for IoT.

In this White Paper we discuss the use and evolution of WSNs within the wider context of IoT, and provide a review of WSN applications, while also focusing the attention on infrastructure technologies, applications and standards featured in WSN designs. This White Paper is the sixth in a series whose purpose is to ensure that the IEC can continue to contribute with its International Standards and Conformity Assessment services to solve global problems in electrotechnology.

Section 2 starts with the historical background of IoT and WSNs, then provides an example from the power industry which is now undergoing power grid upgrading. WSN technologies are playing an important role in safety monitoring over power transmission and transformation equipment and the deployment of billions of smart meters.

Section 3 assesses the technology and characteristics of WSNs and the worldwide application needs for them, including data aggregation and security.

Section 4 addresses the challenges and future trends of WSNs in a wide range of applications in various domains, including ultra large sensing device access, trust security and privacy, and service architectures to name a few.

Section 5 provides information on applications. The variety of possible applications of WSNs to the real world is practically unlimited. On one hand, WSNs enable new applications and thus new possible markets; on the other hand, the design is affected by several constraints that call for new paradigms. This section outlines WSN uses for the smart grid, smart water, intelligent transportation systems, and smart home domains.

Section 6 offers analysis of standardization being a major prerequisite in achieving the interoperability of WSNs, not only between products of different vendors, but also between different solutions, applications and domains.

Section 7 concludes with a number of key recommendations for industry, regulators, the IEC, and general observations on WSN security and data topics.

Acknowledgments

This White Paper has been prepared by the Wireless Sensor Networks project team, in the IEC Market Strategy Board. The project team includes:

Dr. Shu Yinbiao, Project Leader, MSB Member, SGCC

Dr. Kang Lee, Project Partner, NIST

Mr. Peter Lanctot, IEC

Dr. Fan Jianbin, SGCC

Dr. Hu Hao, SGCC

Dr. Bruce Chow, Corning Incorporated

Mr. Jean-Pierre Desbenoit, Schneider Electric

Mr. Guido Stephan, Siemens

Mr. Li Hui, Siemens

Mr. Xue Guodong, Haier

Mr. Simon Chen, SAP

Mr. Daniel Faulk, SAP

Mr. Tomas Kaiser, SAP

Mr. Hiroki Satoh, Hitachi

Prof. Ouyang Jinsong, ITEI China

Mr. Wang Linkun, ITEI China

Ms. Wang Shou, ITEI China

Dr. Zhen Yan, Nari Group Corporation

Dr. Sun Junping, China-EPRI

Prof. Yu Haibin, SIA

Dr. Zeng Peng, SIA

Dr. Li Dong, SIA

Dr. Wang Qin, University of Science and Technology, Beijing

Table of contents

List of abbreviations

Technical and scientific terms

ABS	anti-lock braking system
AMI	advanced metering infrastructure
CAPEX	capital expenditure
CoAP	constrained application protocol
COSEM	companion specification for energy metering
CPU	control processing unit
DLMS	device language message specification
DSN	distributed sensor network
ESC	electronic stability control
FCD	floating car data
FDM	frequency-division multiplexing
FH	frequency hopping
GHG	greenhouse gases
GPS	global positioning system
ICT	information and communication technologies
IoT	internet of things
KPI	key performance indicator
M2M	machine to machine
MAC	media access control
MEMS	microelectromechanical systems
MIMO	multiple-input multiple-output
OEM	original equipment manufacturer
OFDM	orthogonal frequency-division multiplexing
OPEX	operational expenditure
PHY	physical layer
PV	photovoltaic
QoS	quality of service
RES	renewable energy source

RFID	radio-frequency identification
SOA	service oriented architecture
SOAP	service oriented architecture protocol
TDMA	time division multiple access
TSMP	time synchronized mesh protocol
TSP	trust, security and privacy
UCC	urban consolidation centre
USN	ubiquitous sensor network
WIA-FA	wireless networks for industrial automation – factory automation
WIA-PA	wireless networks for industrial automation – process automation
WISA	wireless interface for sensors and actuators
WLAN	wireless local area network
WMAN	wireless metropolitan area network
WPAN	wireless personal area network
WSN	wireless sensor network
WWAN	wireless wide area network
XFCD	extended floating car data

Organizations, institutions and companies

ABB	ABB Group
ARPANET	Advanced Research Projects Agency Network
BBF	Broadband Forum
CAB	Conformity Assessment Board (of the IEC)
China-EPRI	China Electric Power Research Institute
DARPA	Defense Advanced Research Projects Agency (USA)
ETSI	European Telecommunications Standards Institute
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
ISO	International Organization for Standardization
ITEI	Instrumentation Technology and Economy Institute (China)

ITU-T	International Telecommunication Union – Telecommunication Standardization Sector
MSB	Market Strategy Board (of the IEC)
NIST	National Institute of Standards and Technology
OGC	Open Geospatial Consortium
OMA	Open Mobile Alliance
SGCC	State Grid Corporation of China
SIA	Shenyang Institute of Automation (China)
SMB	Standardization Management Board (of the IEC)
UCB	University of California Berkeley (USA)
W3C	World Wide Web Consortium

Glossary

internet of things
IoT
refers to the interconnection of uniquely identifiable embedded computing-like devices within the existing internet infrastructure

media access control layer
MAC layer
part of the data link protocol that controls access to the physical transmission medium in IEEE 802 networks (LANs)

system on a chip
SoC
integrated circuit (IC) that integrates all components of a computer or other electronic system into a single chip

time synchronized mesh protocol
TSMP
a networking protocol that forms the foundation of reliable, ultra low-power wireless sensor networking

wireless local area network
WLAN
local area network in which data are transferred without the use of wires

wireless metropolitan area network
WMAN
also known as a wireless local loop (WLL). WMANs are based on the IEEE 802.16 standard. Wireless local loop can reach effective transfer speeds of 1 to 10 Mbps within a range of 4 to 10 kilometres

wireless personal area network
WPAN
a low-range wireless network which covers an area of only a few dozen metres

wireless sensor network
WSN
self-organizing, multi-hop networks of wireless sensor nodes used to monitor and control physical phenomena

wireless wide area network
WWAN
wireless network that provides communication services to a geographic area larger than a single urban area. The most common of all wireless networks

Section 1
Introduction

1.1 Overview

Today sensors are everywhere. We take it for granted, but there are sensors in our vehicles, in our smart phones, in factories controlling CO_2 emissions, and even in the ground monitoring soil conditions in vineyards. While it seems that sensors have been around for a while, research on wireless sensor networks (WSNs) started back in the 1980s, and it is only since 2001 that WSNs generated an increased interest from industrial and research perspectives. This is due to the availability of inexpensive, low powered miniature components like processors, radios and sensors that were often integrated on a single chip (system on a chip (SoC)).

The idea of internet of things (IoT) was developed in parallel to WSNs. The term internet of things was devised by Kevin Ashton in 1999 [1] and refers to uniquely identifiable objects and their virtual representations in an "internet-like" structure. These objects can be anything from large buildings, industrial plants, planes, cars, machines, any kind of goods, specific parts of a larger system to human beings, animals and plants and even specific body parts of them.

While IoT does not assume a specific communication technology, wireless communication technologies will play a major role, and in particular, WSNs will proliferate many applications and many industries. The small, rugged, inexpensive and low powered WSN sensors will bring the IoT to even the smallest objects installed in any kind of environment, at reasonable costs. Integration of these objects into IoT will be a major evolution of WSNs.

A WSN can generally be described as a network of nodes that cooperatively sense and may control the environment, enabling interaction between persons or computers and the surrounding environment [2]. In fact, the activity of sensing, processing, and communication with a limited amount of energy, ignites a cross-layer design approach typically requiring the joint consideration of distributed signal/data processing, medium access control, and communication protocols [3].

Through synthesizing existing WSN applications as part of the infrastructure system, potential new applications can be identified and developed to meet future technology and market trends. For instance WSN technology applications for smart grid, smart water, intelligent transportation systems, and smart home generate huge amounts of data, and this data can serve many purposes.

Additionally, as the modern world shifts to this new age of WSNs in the IoT, there will be a number of legal implications that will have to be clarified over time. One of the most pressing issues is the ownership and use of the data that is collected, consolidated, correlated and mined for additional value. Data brokers will have a flourishing business as the pooling of information from various sources will lead to new and unknown business opportunities and potential legal liabilities. The recent US National Security Administration scandal and other indignities have shown that there is wide interest in gathering data for varied uses.

One of the more complex issues which arise within this new world is the thought of machines making autonomous decisions, with unknown impact on the environment or society within which

it functions. This can be as simple as a refrigerator requesting replenishment for milk and butter at the local store for its owner, or as complex as a robot that has been programmed to survive in a harsh environment that originally did not foresee human interaction. It can also be as simple as a vehicle that records its usage, as does the black box in the aerospace industry, but then not only using the information to understand the cause of an accident, but also to provide evidence against the owner and operator. For example, a machine that notifies legal authorities if it was used against the law.

It comes to the point where a machine starts acting as if it were a legal entity. The question of liability starts to get fuzzy and the liability question for the “owner” and “operator” of the machine gets more difficult to articulate if there is little to no real human intervention in the actions of the machine or robot. This is certainly the worst case scenario, but the question is how to balance the cost of potential liabilities with the benefits of IoT solutions? This quickly starts to become more of a societal or ethical, and moral discussion. That is what we usually refer to as generational shifts in values – but the IoT trend will not wait a generation.

1.2 Scope of this White Paper

This White Paper is the sixth in a series whose purpose is to ensure that the IEC can continue to contribute through its International Standards and Conformity Assessment services solving global problems in electrotechnology. The White Papers are developed by the IEC MSB (Market Strategy Board), responsible for analyzing and understanding the IEC’s market so as to prepare the IEC to strategically face the future.

Section 2

History and industrial drivers of WSNs

The development of WSNs was inspired by military applications, notably surveillance in conflict zones. Today, they consist of distributed independent devices that use sensors to monitor the physical conditions with their applications extended to industrial infrastructure, automation, health, traffic, and many consumer areas.

Research on WSNs dates back to the early 1980s when the United States Defense Advanced Research Projects Agency (DARPA) carried out the distributed sensor networks (DSNs) programme for the US military. At that time, the Advanced Research Projects Agency Network (ARPANET) had been in operation for a number of years, with about 200 hosts at universities and research institutes [4]. DSNs were assumed to have many spatially distributed low-cost sensing nodes, collaborating with each other but operated autonomously, with information being routed to whichever node that can best use the information. Even though early researchers on sensor networks had the vision of a DSN in mind, the technology was not quite ready. More specifically, the sensors were rather large (i.e. the size of a shoe box and bigger), and the number of potential applications was thus limited. Furthermore, the earliest DSNs were not tightly associated with wireless connectivity.

Recent advances in computing, communication and micro-electromechanical technology have resulted in a significant shift in WSN research and brought it closer to the original vision. The new wave of research on WSNs started around 1998 and has been attracting more and more attention and international involvement. The new wave of sensor network research puts its focus on networking technology and networked information processing suitable for highly dynamic ad hoc environments and resource-constrained sensor nodes. Furthermore, the sensor nodes have been much smaller in size (i.e. from that of a pack of cards to dust particle) and much cheaper in price, and thus many new civilian applications of sensor networks such as environment monitoring, vehicular sensor network and body sensor networks have emerged.

Again, DARPA acted as a pioneer in the new wave of sensor network research by launching an initiative research programme called SensIT [5] which provided the present sensor networks with new capabilities such as ad hoc networking, dynamic querying and tasking, reprogramming and multi-tasking. Currently, WSNs have been viewed as one of the most important technologies for the 21st century [6]. China for example has included WSNs in their national strategic research programmes [7]. As a result, the commercialization of WSNs is accelerating and many new technology companies are emerging such as Crossbow Technology (connecting the physical world to the digital world) and Dust Networks.

Today, industrial automation is one of the most important areas of WSN applications. According to Freedonia Group, the global market share of sensors for industrial use is 11 billion USD, while the cost of installation (mainly cabling costs) and usage is up to more than 100 billion USD. This high cost is the main issue hindering the development of industrial communication technology. WSN technology, allowing “ubiquitous sensing” over the whole industrial process, can secure the important parameters which are not available by online monitoring due to the cost reasons stated above. These parameters are important foundations for

the implementation of optimal control in order to achieve the objective of improving product quality, and reducing energy consumption.

According to ON World [8], wireless devices to be installed in industrial fields will increase by 553 % between 2011 and 2016 when there will be 24 million wireless-enabled sensors and actuators, or sensing points, deployed worldwide. Among these, 39 % will be used for new applications that are only possible with wireless sensor networking. By 2014, the number of WSN devices will account for 15 % of the entire industrial measurement and control equipment sensing points, and 33 % by 2016.

In today's market, three-fourths of the industrial WSN income comes from the process industry; with the oil and power industry being the fastest growing ones. For example, PetroChina is carrying out IoT projects in its oil fields, with the purpose to reconstruct 200 000 oil wells. WSN technology applied in the digital conversions of the oil wells will make use of online monitoring to measure oil well production and ensure production safety.

In the power industry which is now undergoing the power grid upgrading, WSN technology is also playing an important role in safety monitoring over power transmission and transformation equipment and the reconstruction of billions of smart meters.

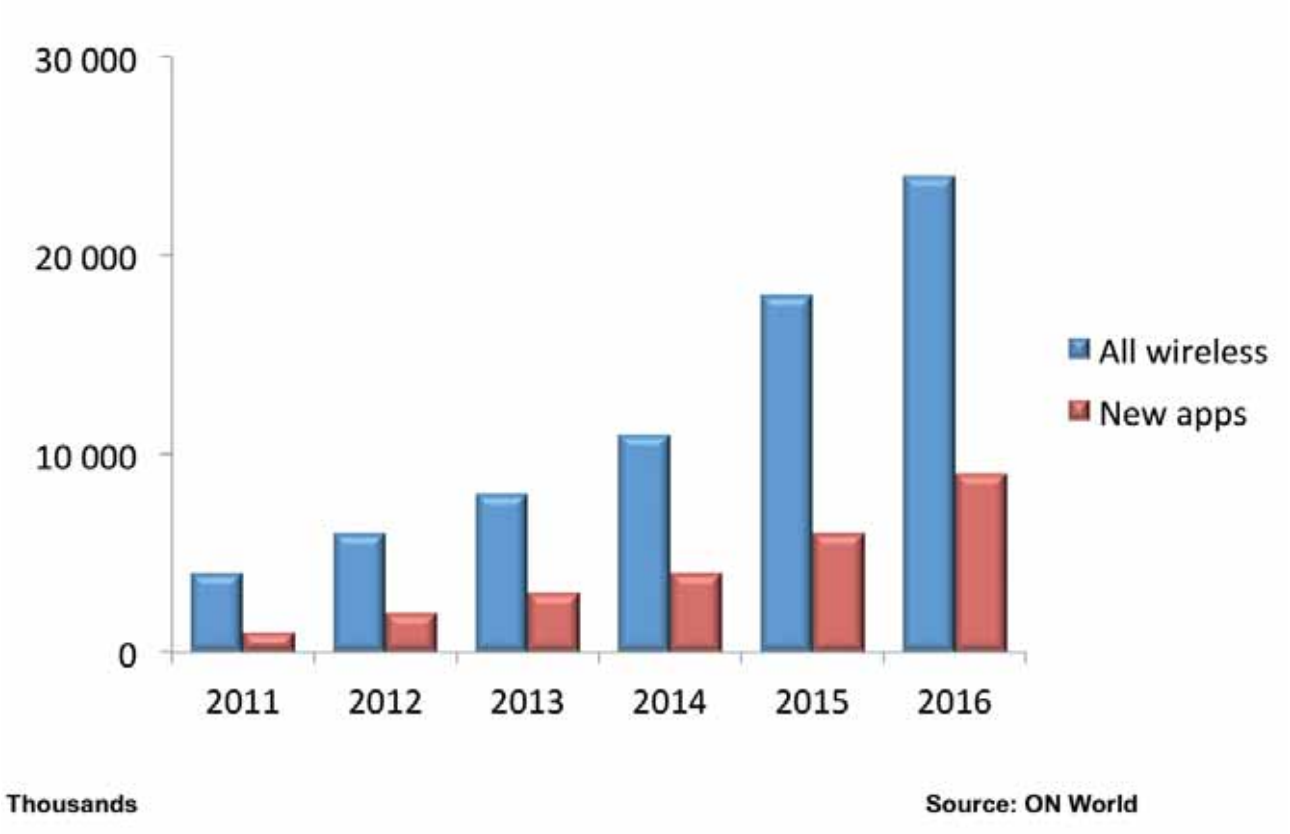


Figure 2-1 | Global installed industrial wireless sensing points [8]

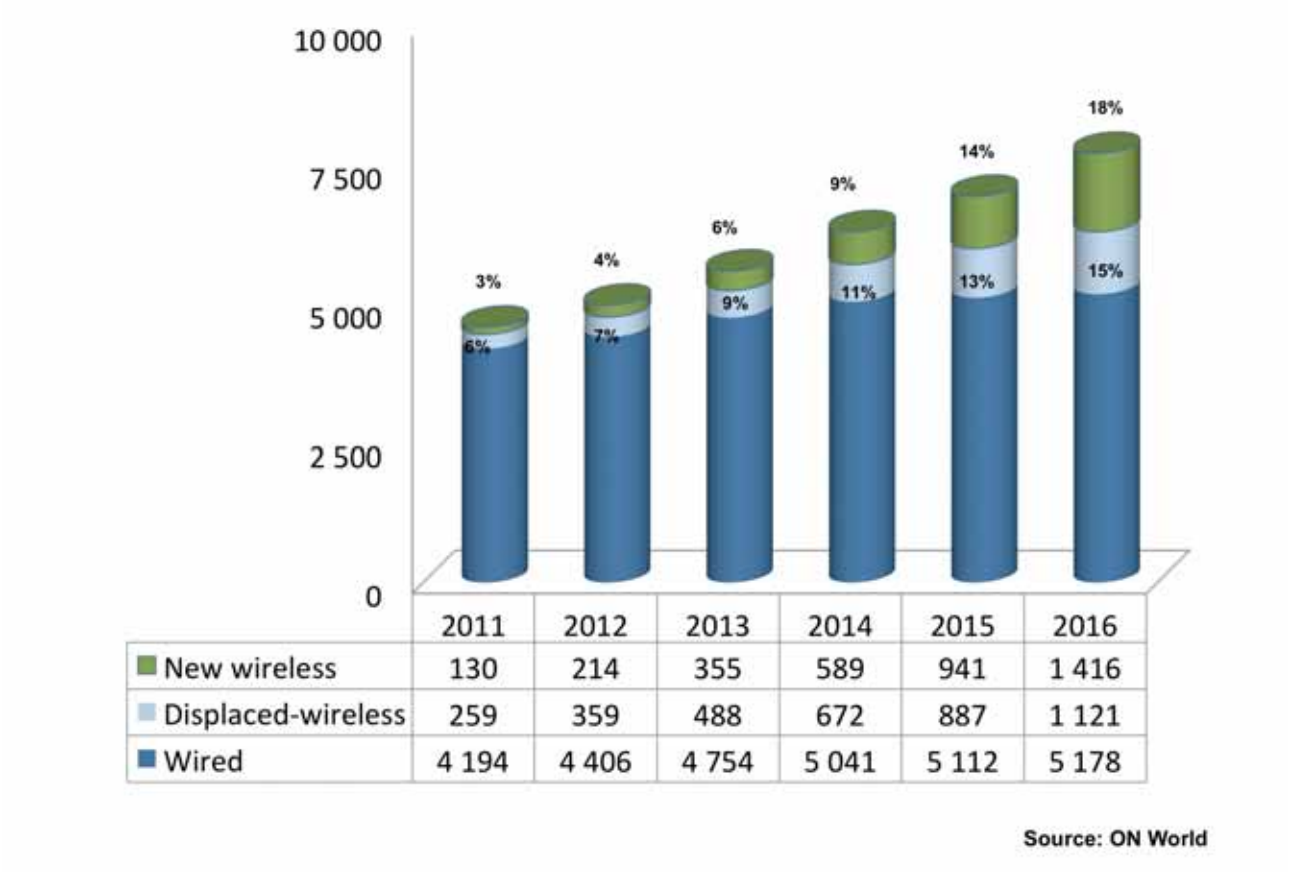


Figure 2-2 | Global industrial field instrument shipments, wired and wireless [8]

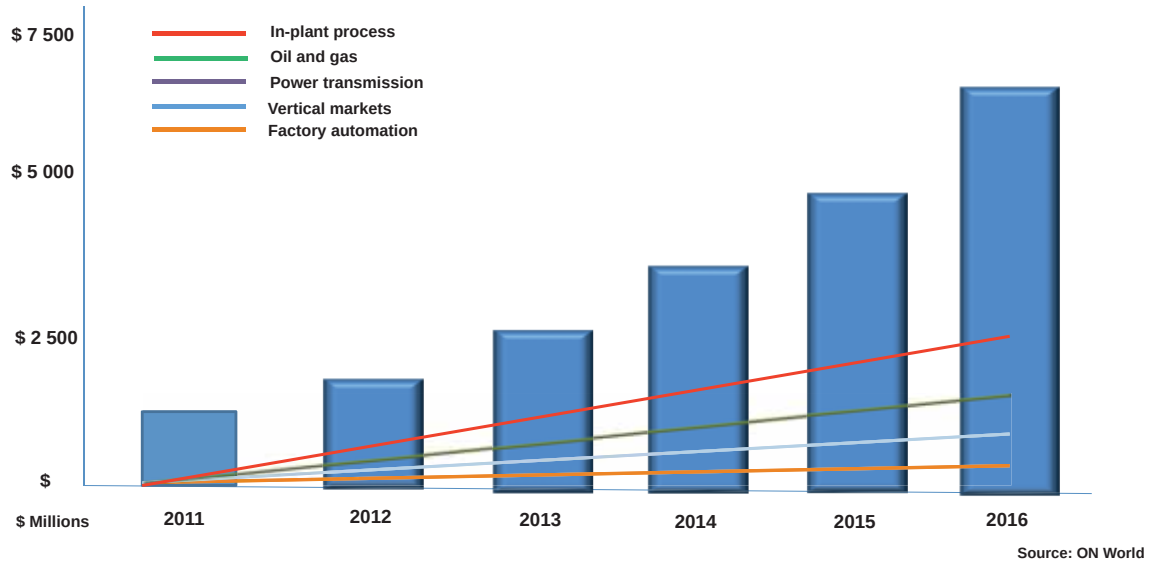


Figure 2-3 | WSN revenue growth in all industries [8]

Section 3

WSN technology

3.1 Characteristic features of WSNs

A WSN can generally be described as a network of nodes that cooperatively sense and control the environment, enabling interaction between persons or computers and the surrounding environment [2]. WSNs nowadays usually include sensor nodes, actuator nodes, gateways and clients. A large number of sensor nodes deployed randomly inside of or near the monitoring area (sensor field), form networks through self-organization. Sensor nodes monitor the collected data to transmit along to other sensor nodes by hopping. During the process of transmission, monitored data may be handled by multiple nodes to get to gateway node after multi-hop routing, and finally reach the management node through the internet or satellite. It is the user who configures and manages the WSN with the management node, publish monitoring missions and collection of the monitored data.

As related technologies mature, the cost of WSN equipment has dropped dramatically, and their applications are gradually expanding from the military areas to industrial and commercial fields. Meanwhile, standards for WSN technology have been well developed, such as Zigbee®[1],

1 Zigbee® is an example of a suitable product available commercially. This information is given for the convenience of users of this standard and does not constitute an endorsement by IEC of this product.

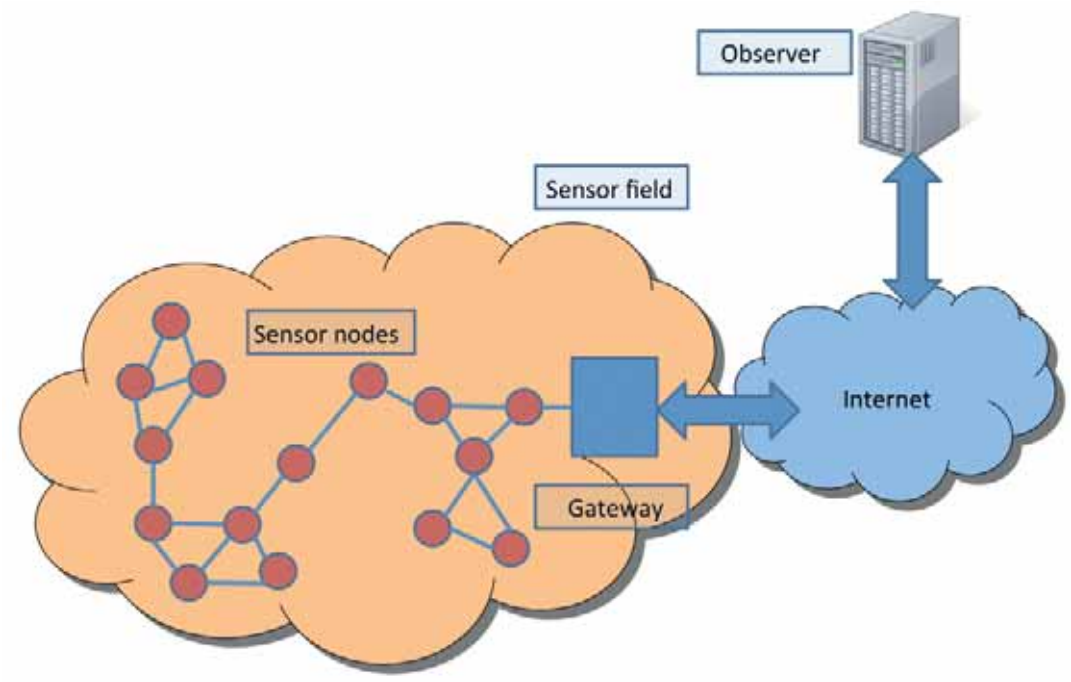


Figure 3-1 | Wireless sensor networks

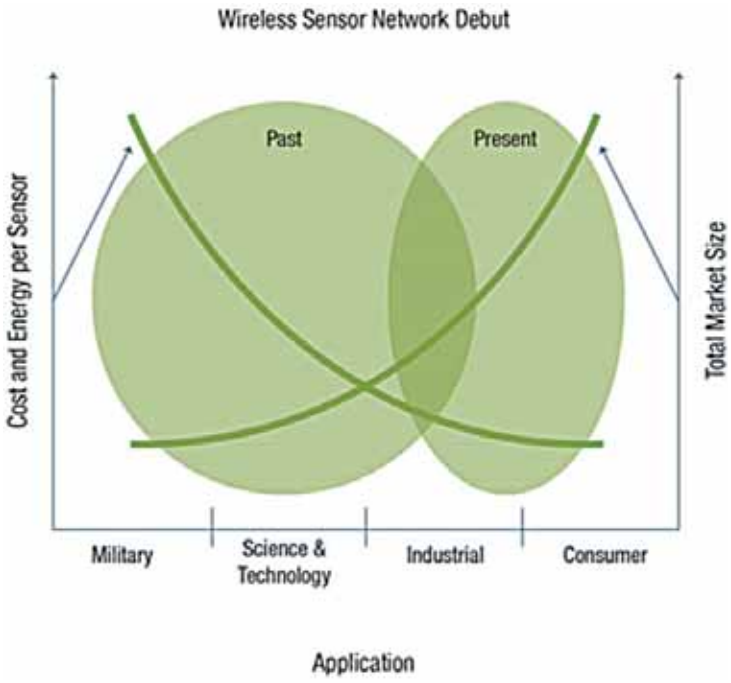


Figure 3-2 | Market size of WSN applications [9]

WirelessHart, ISA 100.11a, wireless networks for industrial automation – process automation (WIA-PA), etc. Moreover, with new application modes of WSN emerging in industrial automation and home applications, the total market size of WSN applications will continue to grow rapidly.

3.2 Sensor nodes

The sensor node is one of the main parts of a WSN. The hardware of a sensor node generally includes four parts: the power and power management module, a sensor, a microcontroller, and a wireless transceiver, see Figure 3-3. The power module offers the reliable power needed for the system. The sensor is the bond of a WSN node which can obtain the environmental and equipment status. A sensor is in charge of collecting and transforming the signals, such as light, vibration and chemical signals, into electrical signals and then transferring them to the microcontroller. The microcontroller receives the data from the sensor and processes the data accordingly. The Wireless Transceiver (RF module) then transfers the data, so that the physical realization of communication can be achieved.

It is important that the design of the all parts of a WSN node consider the WSN node features of tiny size and limited power.

3.2.1 Miniaturization technology of sensor based on MEMS

The miniaturization technology of WSN nodes based on microelectromechanical systems (MEMS) has made remarkable progress in recent years. The core technology of MEMS is to realize the combination of microelectronics technology, micro-machining technology and the packaging technology. Different levels of 2D and 3D micro-sensitive structures can be produced based on microelectronics and micro-machining technology, which can be the miniature sensing elements. These miniature sensing elements, associated power supply and signal conditioning circuits can be integrated and packaged as a miniature MEMS sensor.

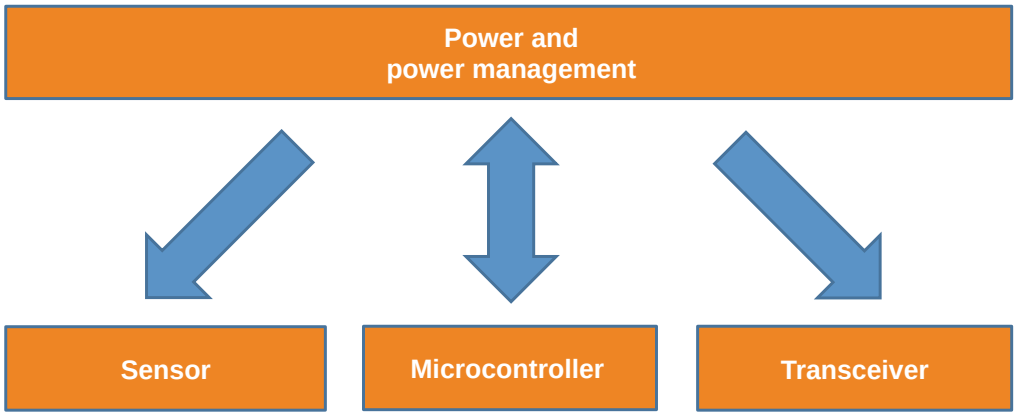


Figure 3-3 | Hardware structure of a WSN sensor node

At present, there are already many types of miniature MEMS sensors in the market which can be used to measure a variety of physical, chemical and biomass signals, including displacement, velocity, acceleration, pressure, stress, strain, sound, light, electricity, magnetism, heat, pH value, etc. [10]. In 2003, researchers at the University of California Berkeley (UCB) developed a WSN sensor node (mote) with a micro sensor. The actual size of its MEMS sensing module was only 2.8 mm × 2.1 mm [11].

3.2.2 Ambient energy harvesting technology

Nodes need an energy source, and ambient energy harvesting from external sources are used to power small autonomous sensors such as those based on MEMS technology. These systems are often very small and require little power, however their applications are limited by the reliance on battery power.

Ambient energy harvesting cannot only be realized by conventional optical cell power generation, but also through miniature piezoelectric crystals, micro oscillators, thermoelectric power generation elements, or electromagnetic wave reception devices [12] [13].

Some companies have begun to commercialize sensor network applications using energy acquisition devices. For example, the German company EnOcean has provided light energy harvesting devices, vibration energy harvesting devices and temperature-based energy harvesting devices for smart building lighting and air monitoring applications. For equipment and construction health monitoring applications, a variety of piezoelectric vibration energy harvesting products have entered the market. The British company of Perpetuum provides a series of products that converts mechanical vibration into electrical energy used to perpetually power autonomous, maintenance-free industrial wireless sensor nodes. For these sensor nodes the energy of vibration made by your fingers knocking the desk can support the sensor node sending 2 kB data to 100 m away every 60 seconds.

For the monitoring applications of piping systems, a large number of products based on temperature difference energy harvesting have been developed. Nextreme Company's products can produce 0.25 W of power by a temperature difference of 60 °C in an area of 3.2 mm × 1.6 mm energy harvesting materials. Figures 3-4 and 3-5 show some sensor nodes configured with ambient energy harvesting devices.

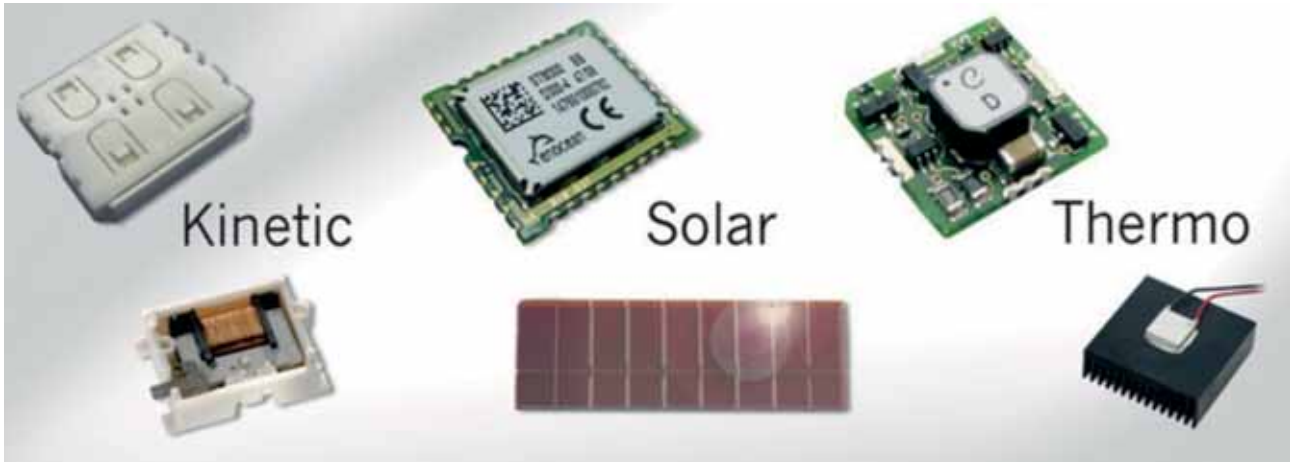


Figure 3-4 | Sensor nodes configured with ambient energy harvesting devices [14]

Figure 3-5 | Motor monitoring system based on vibration energy harvesting [14]

3.3 Access network technologies

The access network, whose length ranges from a few hundred meters to several miles, includes all the devices between the backbone network and the user terminals. It is thus aptly called “the last mile”.

Because the backbone network usually uses optical fibre structure with a high transmission rate, the access network has become the bottleneck of the entire network system.

As shown in Figure 3-6, due to the open property of wireless channels, conflicts will happen in time, space or frequency dimension when the channel is shared among multiple users. The function of access network technologies is to manage and coordinate the use of channels resources to ensure the interconnection and communication of multiple users on the shared channel.

According to the distance and speed of access, existing access technologies can be classified into four categories: wireless local area network (WLAN), wireless metropolitan area network (WMAN), wireless personal area network (WPAN) and wireless wide area network (WWAN). However, the overall developing trend of high transmission rates is not suitable for the application requirements of WSNs. The main reasons are as follows:

§ In terms of reliability, the working environment of WSNs is usually rather severe. The bad environment with narrow-band multi-frequency noise, interference and multi-path effects makes the reliable communication based on the rare channel resources an urgent problem which needs to be resolved.

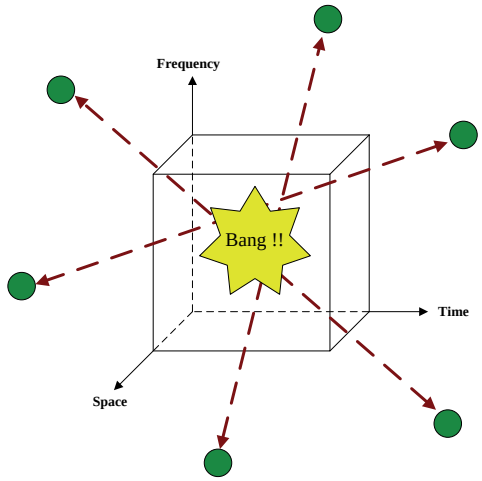


Figure 3-6 | Access technologies [14]

§ In terms of real-time capability, applications for WSN and IoT have stricter real-time requirements than the others. A tiny latency may lead to a major mishap. Therefore, hard real-time communication has to be guaranteed in many applications.

§ In terms of energy efficiency, low energy consumption is the key to support the long-flow of independent battery-powered devices and to reduce maintenance cost. This is also another requirement for WSNs and IoT applications, especially for the devices with batteries difficult to be replaced.

According to the current specific requirements for WSN applications, the development of

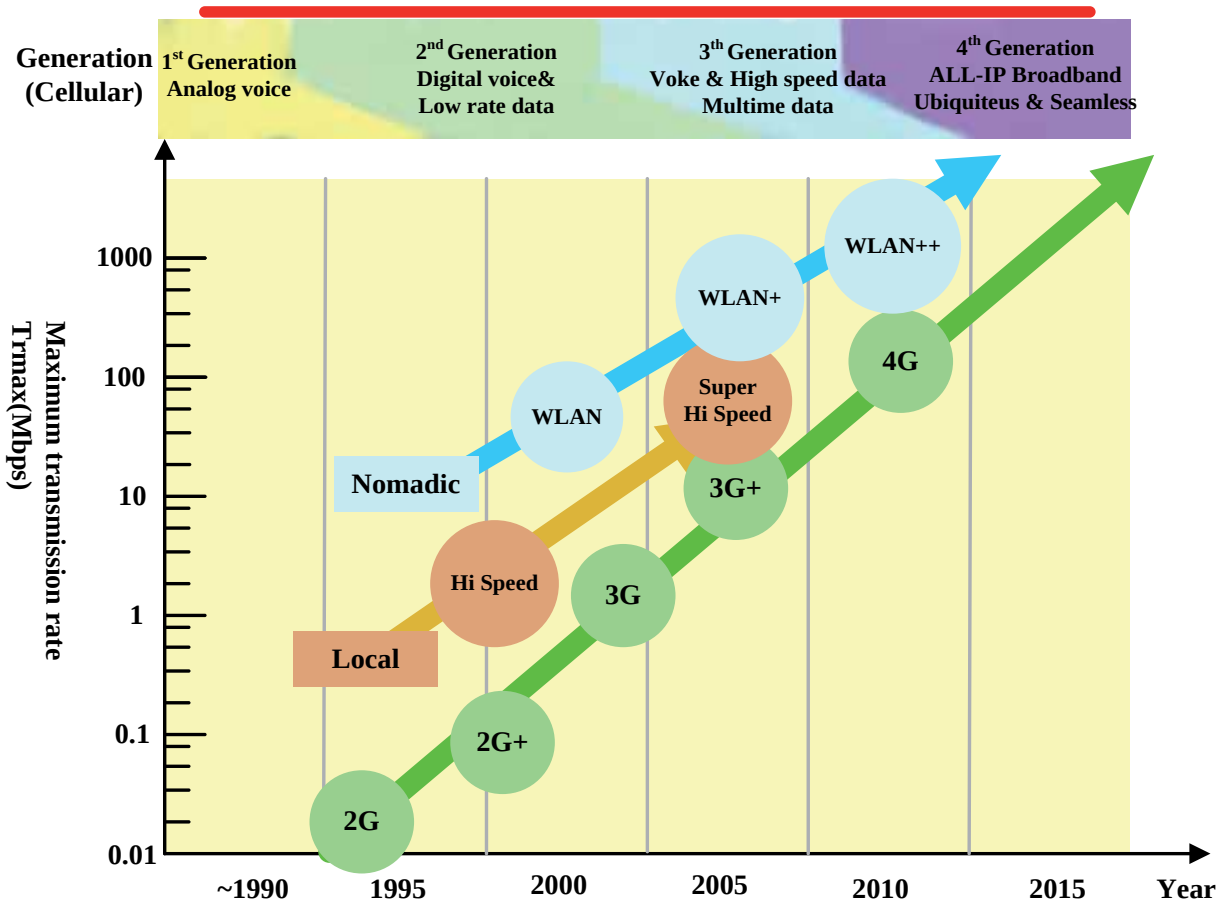


Figure 3-7 | Developing trends of access technologies [15]

access network technology has already made significant progresses. The representative access technologies that are more systematic and noteworthy are Bluetooth 4.0 oriented towards medical WSN; IEEE 802.15.4e [16] oriented towards industrial WSN; and WLAN IEEE 802.11™ [17] in view of the IoT. These technologies are described further in Annex A.

3.4 Topology

Generally, a WSN consists of a number of sensor network nodes and a gateway for the connection to the internet. The general deployment process of a WSN is as follows (see Figure 3-8): firstly, the sensor network nodes broadcast their status to the surroundings and receive status from other nodes to detect each other. Secondly, the sensor network nodes are organized into a connected network according to a certain topology (linear, star, tree, mesh, etc.). Finally, suitable paths are computed on the constructed network for transmitting the sensing data. The power of sensor network nodes is usually provided by batteries, so the transmission distance of WSN nodes is short. The transmission distance can be up to 800 to 1 000 meters in the open outdoor environment with line of sight. It will sharply decline in the case of a sheltered indoor environment to an estimated few meters. In order to expand the coverage of a network, the sensor network uses multi-hop transmission mode. That is to say the sensor network nodes are both transmitter and receiver. The first sensor network node, the source node, sends data to a nearby node for data transmission to the gateway. The nearby node forwards the data to one of its nearby nodes that are on the path towards the gateway. The forwarding is repeated until the

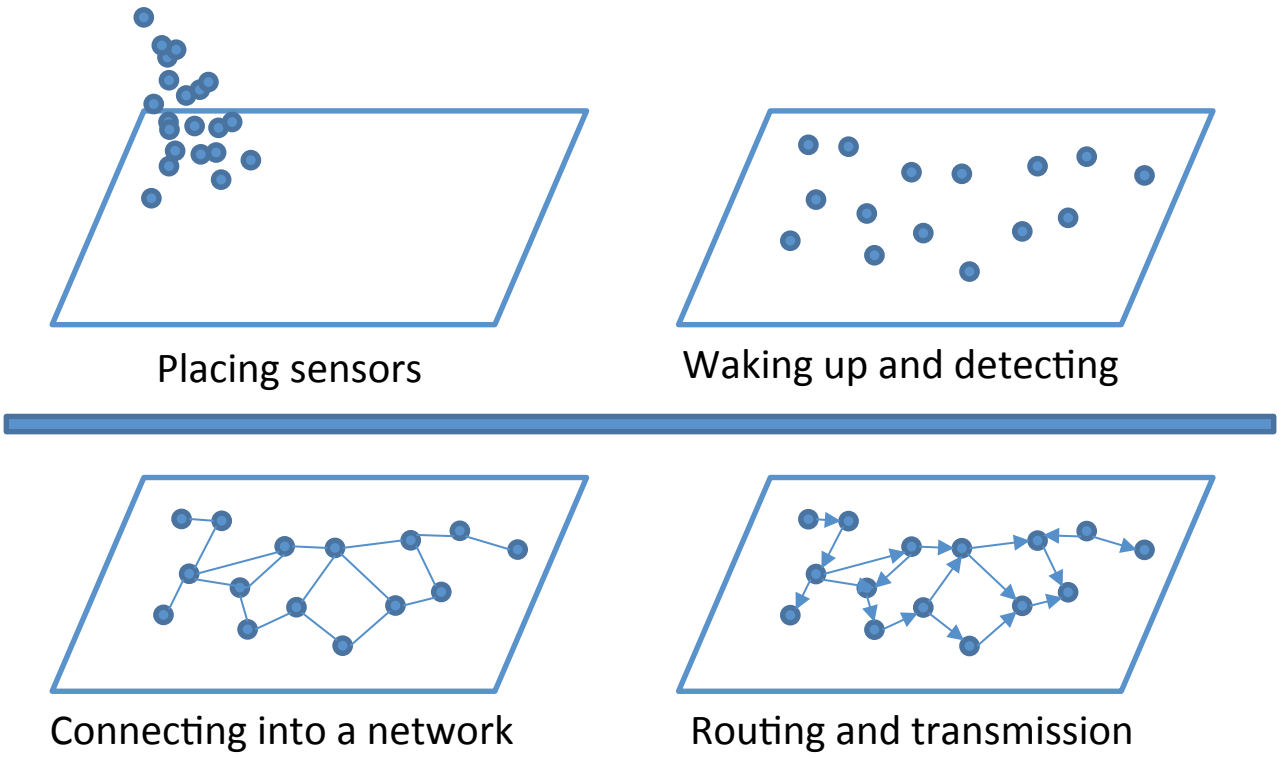


Figure 3-8 | Organizing and transmitting process of WSNs [18]

data arrives at the gateway, the destination. The protocols and some implementation techniques of WSNs can be adapted to the mature architecture and technologies of wireless and wired computer networks. However, the features of WSNs are self-organization, self-adaption, limited nodes energy, and unstable transmission links.

3.4.1 Self-organizing and reliable networking technology

The positions of WSN nodes are random, and the nodes can be moved, sheltered and interfered with. The topology of mesh networks have great advantages in flexibility and reliability compared with other network topologies. The self-organizing management approach of network nodes can greatly improve the robustness of the network, resulting in a smart mesh networking technology, as shown in Figure 3-9. In smart mesh ad hoc networking technology, the node first monitors the neighbour nodes and measures the signal strength, and then it selects the appropriate neighbour node for time synchronization and sends a joining request. Then the neighbour node delivers the request to the gateway. The gateway receives the request and assigns network resources for the node. Based on the mesh network, the sensor network nodes can be assigned with two or more transmission paths to improve the reliability of network. Time synchronized mesh protocol (TSMP) network [19] of the dust network can support self-organizing network and maintain a network consisted of one hundred nodes.

3.4.2 Low cost IP interconnection technology

The design of early sensor networks commonly used internal addresses to manage the sensor network nodes. The address length was relatively short and suitable for implementing in low-power embedded sensor network nodes. However, the internal address management method is not compatible with the IP method of the internet, which increased the difficulty of interacting between the sensor network nodes and the traditional IP network nodes. Therefore, there is a need to resolve

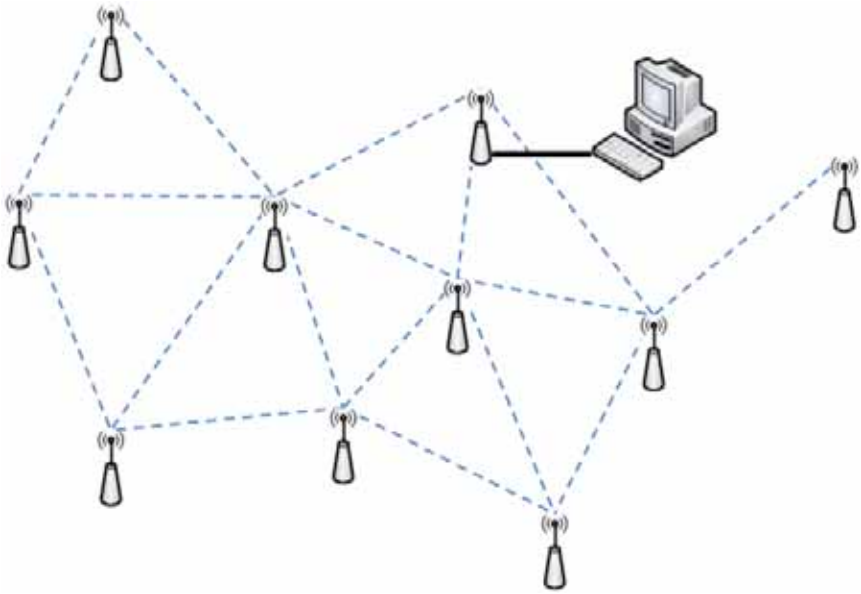


Figure 3-9 | Mesh self-organizing network [14]

the connectivity problem of WSN and IP network. Traditional IPv4 addresses have been gradually depleted, and the new IPv6 technology has an enormous address resource which is suitable for a wide range of sensor network deployment. As a result, 6LoWPAN low-power wireless technology based on IPv6 has emerged [20]. 6LoWPAN has generally implemented a simplified IPv6 protocol above the link layer of the IEEE 802.15.4 protocol. Header compression and packet fragmentation reloading is implemented by adding an adaptation layer between the IP layer and the link layer, which is a reliable method to achieve protocol adaptive between IPv6 network and the sensor network, as shown in Figure 3-10. The sensor network products of Sensinode Company based on NanoStack [21] and of TI Company based on CC-6LoWPAN [22] all use 6LoPAN technology to provide the capability of scalability, seamless and reliable interconnection between sensor network and IP network.

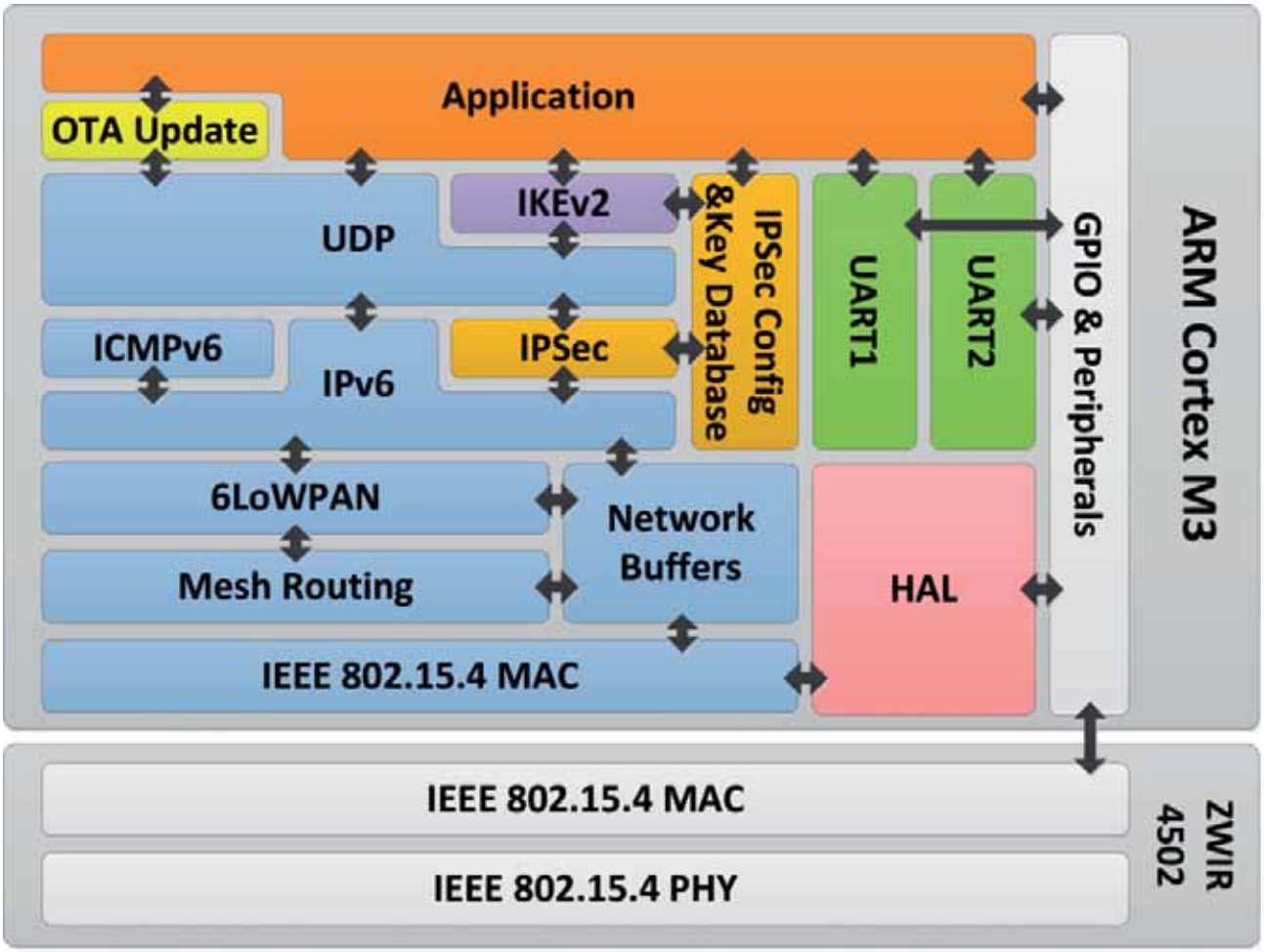


Figure 3-10 | 6LoWPAN protocol stack [14]

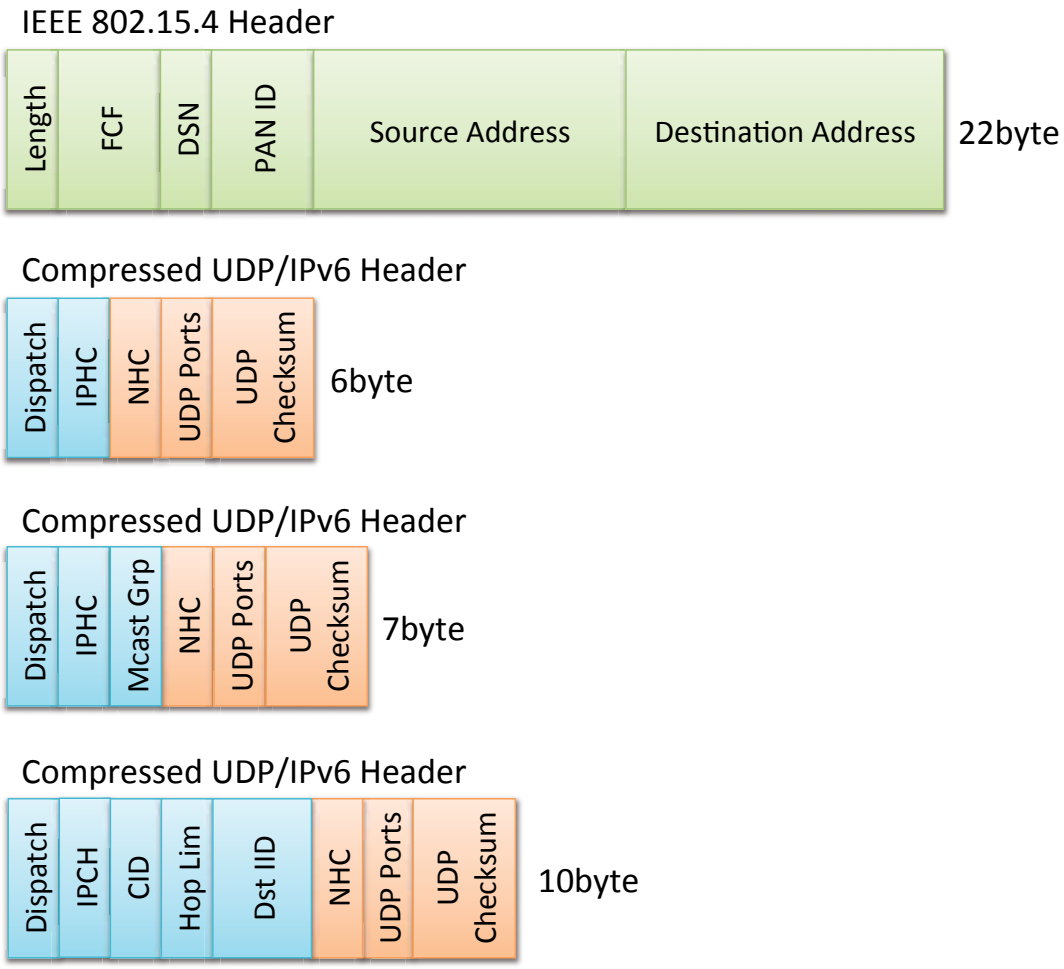


Figure 3-11 | 6LoWPAN improved header compression example [23]

3.4.3 Self-adaptive flow control technology

One of the differences between WSNs and traditional wired networks is the instability of wireless communication. In WSNs, the communication between nodes is susceptible to interference and occlusion, resulting in signal transmission failure. The traditional network is a stable wired network, which data will only be lost due to congestion. The principle of flow control is that the data sender adjusts the sending traffic according to the loss situation of data transmission. When data loss occurs, the sender decreases the transmission rate. And when the data is not lost, the sender increases the transmission rate. Such flow control mechanisms are no longer suitable for WSNs [23], because the data loss in sensor networks is mostly caused by congestion, interference and occlusion. Purely decreasing the transmission rate cannot solve the problem, but only lowers the network performance. In order to solve the network performance degradation problem in unstable transmission conditions, adaptive flow control is proposed. Adaptive flow control checks the reason for packet loss and adjusts the transmission flow. Meanwhile, according to the quality of the link and the

number of transmission errors, the best transmission rate for the data transmission between nodes is prioritized to obtain good network stability while considering the transmission distance and throughput.

3.5 Data aggregation

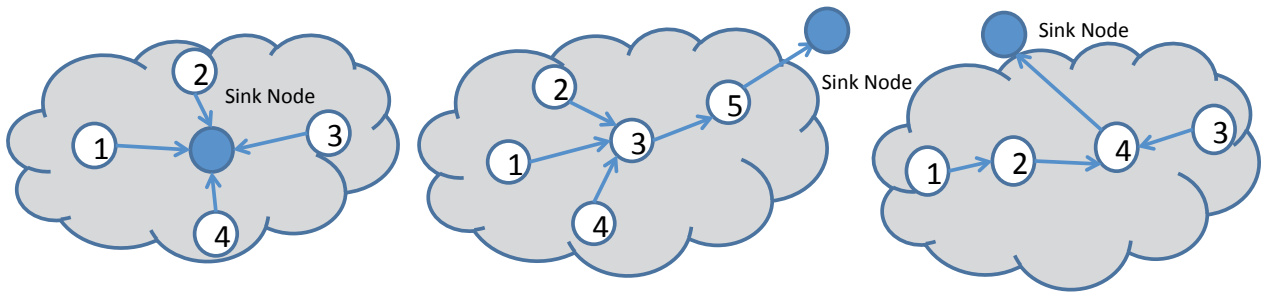
In the energy-constrained sensor network environments, it is unsuitable in numerous aspects of battery power, processing ability, storage capacity and communication bandwidth, for each node to transmit data to the sink node. This is because in sensor networks with high coverage, the information reported by the neighbouring nodes has some degree of redundancy, thus transmitting data separately in each node while consuming bandwidth and energy of the whole sensor network, which shortens lifetime of the network.

To avoid the above mentioned problems, data aggregation techniques have been introduced. Data aggregation is the process of integrating multiple copies of information into one copy, which is effective and able to meet user needs in middle sensor nodes.

The introduction of data aggregation benefits both from saving energy and obtaining accurate information. The energy consumed in transmitting data is much greater than that in processing data in sensor networks. Therefore, with the node's local computing and storage capacity, data aggregating operations are made to remove large quantities of redundant information, so as to minimize the amount of transmission and save energy. In the complex network environment, it is difficult to ensure the accuracy of the information obtained only by collecting few samples of data from the distributed sensor nodes. As a result, monitoring the data of the same object requires the collaborative work of multiple sensors which effectively improves the accuracy and the reliability of the information obtained.

The performance of data aggregation protocol is closely related to the network topology. It is then possible to analyze some data aggregation protocols according to star, tree, and chain network topologies as seen in Figure 3-12.

Data aggregation technology could save energy and improve information accuracy, while sacrificing performance in other areas. On one hand, in the data transfer process, looking for aggregating nodes, data aggregation operations and waiting for the arrival of other data are likely to increase in the average latency of the network. On the other hand, compared to conventional networks, sensor networks have higher data loss rates. Data aggregation could significantly reduce data redundancy but lose more information inadvertently, which reduces the robustness of the sensor network.



a) Star WSN topology b) Tree WSN topology c) Chain WSN topology

Figure 3-12 | Three kinds of WSN topologies: star, tree, chain [14]

3.6 Security

There have been many Hollywood films on how the future will look – and the IoT vision comes close to the Hollywood vision. There is one common theme across both visions: machines become very powerful as a whole within a highly automated society. The question of individual privacy and security within this for the individual becomes more difficult as the complex chain within which the security has been created is infinite and the weakest link defines the overall level of security. With IPv6 there are enough IP addresses to go around for the predicted tens of billions of data points that will form our new world – the question is whether they can all be secured to a level that can ensure individual privacy rights and secure the systems from malicious attacks.

In traditional TCP/IP networks, security is built to protect the confidentiality, integrity and availability of network data. It makes the system reliable and protects the system from malicious attacks which can lead to malfunctioning systems and information disclosure. As the characteristic of node and application environment, WSN security not only needs traditional security protection, but also the special requirements of trust, security and privacy (TSP) WSNs.

3.6.1 Trust, security and privacy

TSP WSNs may, depending on the application scenario, require security protection of integrity, availability, confidentiality, non-repudiation, and user privacy. It supports system integrity, reliability by protecting the system from malicious attacks. TSP WSNs may need to protect the nodes against tampering, protect the communication channel, and routing in the network layer [24]. TSP logging/audit functions may be required to detect attacks.

The technology of TSP WSNs consists of message authentication, encryption, access control, identity authentication, etc. The TSP necessities of WSNs may be categorized as follows: node security, crypto algorithms, key management, secure routing, data aggregation [25] [26].

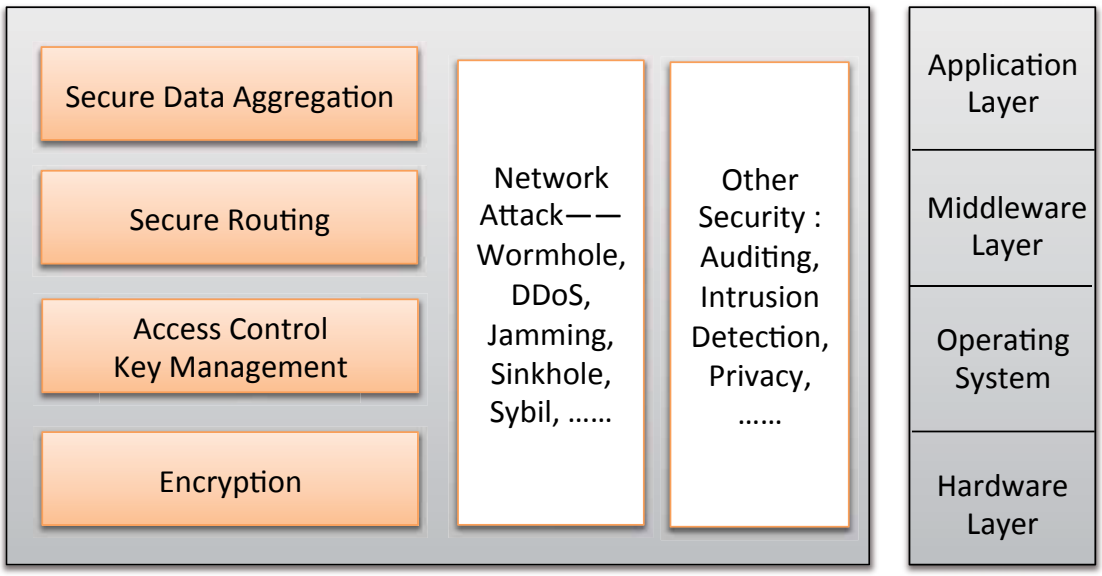


Figure 3-13 | TSP architecture for WSNs [27]

Node security and sleep deprivation

A node of a WSN may be tampered with via its logical interfaces or by direct physical attacks; it may be relocated without authorization, or stolen.

Node security may contain secure wakeup and secure bootstrapping. A low duty cycle is crucial to ensure a long lifetime of battery-powered sensor nodes. A special class of denial of service attacks, the so called sleep deprivation attacks [28] prevents the sensor node from going to the power-saving sleep mode, hence severely reduces the lifetime of an attacked sensor node. Standard security mechanisms like message authentication codes or frame encryption do not prevent sleep deprivation attacks: the node is powered up and energy is spent for processing the received message. The attack can only be noticed when battery power has already been spent. Figure 3-14 shows a sensor node with an additional ultra-low-power wake-up radio. The wake-up radio listens on the channel when the sensor node is in sleep state. It triggers the sensor wake up when it receives a wake-up signal. To add security to the general wake-up radio design, the wake-up signal is an encoded wake-up code [29]. As the wake-up code is used only once and as it is specific for each node, it can be sent in clear when waking up a node.

3.6.2 Crypto algorithms

Encryption is a special algorithm to change the original information of the data sensor node, which makes an unauthorized user not recognize the original information even if he has accessed the encrypted information. The WSNs of public infrastructure are inevitably exposed to the scope of public activities. Traditional message authentication code, symmetric encryption and public-key encryption have exposed their shortcomings [30] [31]. So an encryption system, which is more suitable for WSNs, needs to be proposed. The Spanish company Libelium developed waspmote encryption libraries to ensure the data security of smart city's WSN in 2010. Their wireless sensor devices have supported those libraries basically. Libraries are designed for different encryption mechanism and consultation mechanisms at data link layer, network layer and application layer. And they extend the Zigbee® protocol and make Zigbee® more secure, see Figure 3-15.

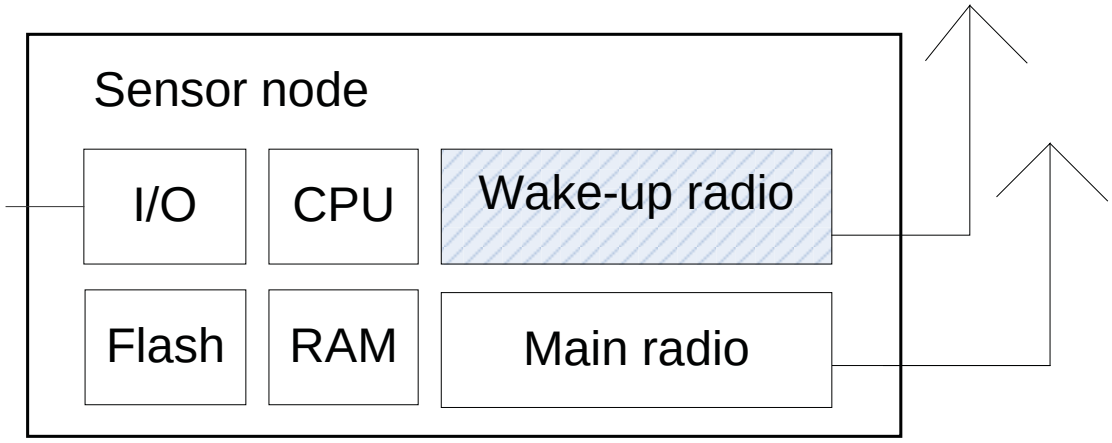


Figure 3-14 | Secure wake-up radio [29]

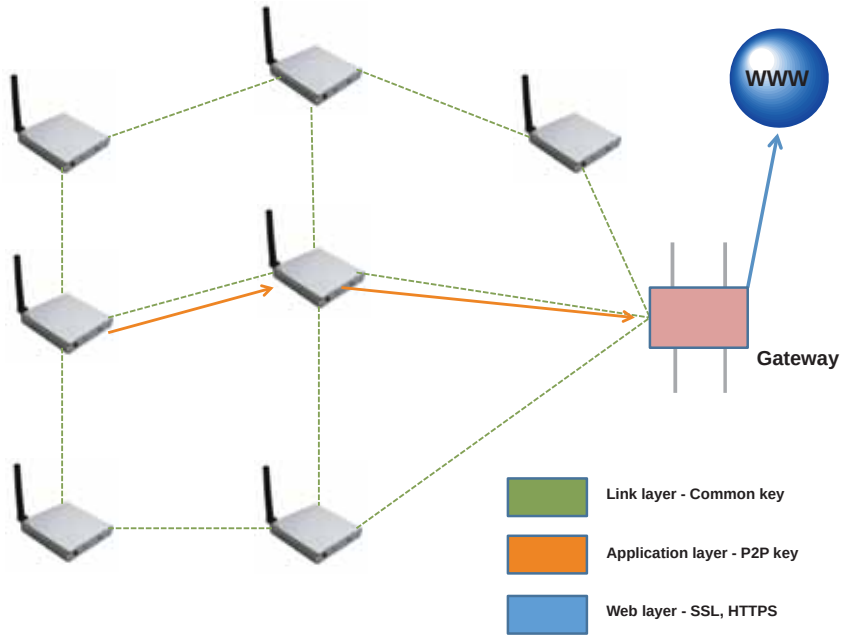


Figure 3-15 | Typical application of waspmote encryption libraries [32]

3.6.3 Key management of WSNs

Key management is focused on the area in WSN security. Key management includes key generation, distribution, verification, update, storage, backup, valid and destroy. An effective key management mechanism is also the foundation of other security mechanisms, such as secure routing, secure positioning, data aggregation. Typical key management schemes in WSNs include global key management, random key management, location key management, clustering key management and public key-based key management [33].

The security bootstrapping procedure establishes the security configuration of a sensor node, e.g. a join key is established during the bootstrapping. As there are multiple bootstrapping procedures and the choice of an appropriate bootstrapping procedure heavily depends on the environment, normal operation of the sensor network is decoupled from the bootstrapping such that it is possible to change the bootstrapping procedure without any change on the security architecture for normal operation. The appropriate bootstrapping procedure depends to a high degree on the application and its environment. Therefore, several different bootstrapping procedures have been proposed [34]: token based, pre-configuration of the keys during manufacturing of the nodes, physical protection of messages, in-band during a weak security set-up phase, out-of-band communication.

3.6.4 Secure routing of WSNs

Since WSNs using multi-hop in data transfer and self-organization in networking, each node also needs routing discovery, routing establishment, routing maintenance. Secure routing protocol is that complete effective routing decisions and may be a prerequisite for data aggregation and redundancy elimination safe from a source node to a sink node. Many secure routing networks have been specifically designed for WSNs, they can be divided into three categories according to the

network structure: flat-based routing, hierarchical-based routing, and location-based routing [35].

Typical methods of secure routing protocols include methods based on feedback information, location information, encryption algorithm, multi-path selection method and hierarchical structures. Different secure routing protocols can solve problems of different types of attacks [36], such as the secure routing protocol based on the feedback information that includes the information of delay, trust, location, excess capacity in acknowledgment frame of the media access control (MAC) layer. Although not using encryption, this method can resist common attacks such as false routing information, cesspool attack and wormhole. Most current secure routing protocols assume the sensor network is stationary, so more new secure routing protocols need to be developed to satisfy mobility of sensor nodes [37].

3.6.5 Secure data aggregation of WSNs

Secure data aggregation is to ensure each node data is secure. Therefore, the general processes of secure data aggregation are as follows: first nodes should be possible to provide reliable date and securely transmit them to the higher aggregation nodes. The higher aggregation nodes judge the credibility of data and do aggregation calculation based on redundancy. Each aggregation nodes select the next safe and reliable hop, transmit data to the central node. The central nodes judge the credibility of data and do the final aggregation calculation [38].

Initially, data aggregation regarded energy as the object and barely considered security issues. Now secure data aggregation is mostly realized by authentication and encryption based on the theory of cluster, ring, and hierarchical. The University of Munich developed a data aggregation prototype, which is based on DTLS protocol to realize secure transmission schemes. The red circle of Figure 3-16 represents their secure data aggregation prototype.

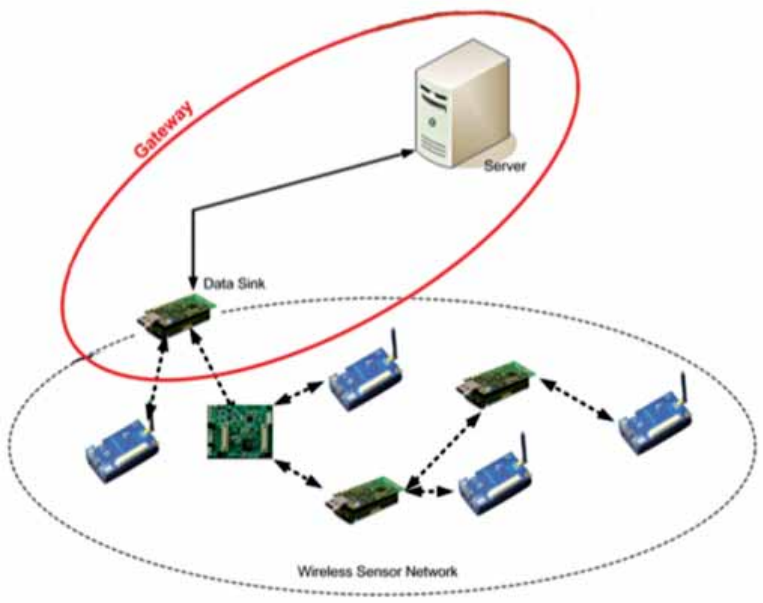


Figure 3-16 | Secure data aggregation products [39]

Section 4

Challenges of WSNs

4.1 System qualities, architecture divergence, and the need for an architecture framework

IoT is characterized by a wide range of challenges that can be characterized by a single word: scale. Every challenge that is known in the context of the current internet also pertains to IoT, but its scale is generally much larger and the implications even more severe. Examples for such challenges are:

§ Range of use-case domains: while the current internet already has made inroads into the lives of denizens and also that of businesses and organizations, this penetration will increase in scope and depth due to IoT. Not only will new application fields be opened up (real-time remote life-stock monitoring; monitoring interest groups; participatory traffic monitoring; etc.), but also the penetration of processes and actions by information and communication technologies (ICT) will increase. A taste of this has been provided by the adoption of radio-frequency identifications (RFIDs) in value chains. While business IT already had made it possible to trace gross flows of products within a company, RFID penetrated entire value chain down to single items and across organizational units (production; outbound logistics; retail, etc.).

§ Difference in business models: while Web 2.0 has already led to a diversification of business models and the proliferation of new, disruptive business model, this trend is expected to amplify once IoT becomes a sizable part of the future internet.

§ Ownership and tenancy: in the current internet, exclusive ownership and exclusive usage are very much the rule, but the sociology of the IoT will be different. Complex systems, for instance city-wide sensor networks, will not necessarily be owned by one group, and the influence of non-owner groups will increase (advocacy groups, public bodies, legislative bodies, etc.). Also, more often than not, more than one organization will operate in the same system. For, instance, an original equipment manufacturer (OEM) might outsource the maintenance of its production-machinery to several off-location service providers, which will, in turn, need remote access to the production IoT system.

§ Range of objects covered: the range of “things” that will be sensed, tracked, and manipulated through IoT will truly be overwhelming. It will span from microscopic and even sub-microscopic entities (bacteria, nanobots, etc.) to macroscopic objects on the scale of planets and larger. The digital shadows of these will be very different, and what constitutes them will also depend on the context. For instance, while for a shipping company whole containers usually constitute the finest scale of granularity and thus “things”, the individual pieces of products in such a container constitute “things” for the receiving retailer as well as the end-customer.

§ Time scales and reliability: IoT will be applied to areas in which real-time control with high reliability will be mandatory (factory automation, air-plane control, etc.), while other applications (glacial monitoring, herd monitoring, etc.) might be conducted in a quasi-offline manner over time scales of minutes to years.

The mere scale of the above challenge will lead to very diverse problems IoT systems will have to solve. This, of course, will translate into diverse system concerns and aspirations, many, if not most, of which will be formulated at a cross-system level. Specifically, concerns and aspirations will address the performance of the entire IoT systems and less of individual members or even parts. IoT architects will thus be faced with diverse, qualitative requirements, and there will be more than one design choice that will fulfil the same qualitative requirement. This problem is exemplified in Table 1. For each system quality there is more than one architectural view through which this quality can be influenced. Take, for instance, system scalability. One view through which to influence scalability is the functional view. For example, to champion distributed functionalities over centralized functions. The same strategy can be pursued in terms of information that is handled in the system.

In other words, system qualities cut across more than one architectural view. Also, achieving one quality through one view (for instance, scalability) can have adverse impacts on other system qualities (for instance, security).

Since the solution space for architectures is multi-dimensional and entangled, and since qualitative requirements cut across more than one system aspect, and since there is usually more than one tactic to achieve a certain quality, this leads to architecture divergence. Particularly, different development teams will derive different architectures and implement incompatible system implementations for the same requirement set if no mitigating actions are taken. Note that this is not an entirely novel problem but that it is even more accentuated in IoT due to the huge range of use-case domains covered and the different cultures and best practices that have evolved in each use-case domain.

Next to endangered interoperability, there is another downside to architecture divergence: lowered "horizontal recycling" of functions, modules and concepts from one domain to another. That is, the flow of best-practice solutions, functional modules, etc. across usage-domain borders will be hampered by a diverse, uncontrolled ecosystem of divergent architectures. This both impacts the capital expenditure (CAPEX) (for instance, innovation and development cost) and operational expenditure (OPEX) (for instance, systems of high complexity that are hard to understand and need time to be understood by new staff). Therefore, architecture divergence also negatively influences the business viability of IoT.

Table 4-1 | Leverage of architectural views on system qualities (selection) [40]

		System quality			
		Trust, security, privacy	Performance and scalability	Availability and resilience	Scalability
Architectural view	Functional	Medium	Medium	Low	**High**
	Information	Medium	Medium	Low	**High**
	Concurrency	Medium	**High**	Medium	Medium
	Deployment	**High**	**High**	**High**	Low
	Operational	Medium	Low	Medium	Low

The above problems will not solve themselves, rather, corrective action is needed. An architecture framework (reference model, reference architecture plus guidance of how to apply them) that fosters the reuse of architectural principles and the reuse of system modules and concepts is needed. A reference model provides a coherent ontology and semantic for describing and analyzing IoT use cases and IoT systems. A reference architecture provides high-level advice on how to build IoT systems that meet IoT stakeholder concerns and expectations. The guidance of how to apply both also answers the question of how to tackle qualitative system requirements while, at the same time, avoiding architecture and system divergence.

4.2 Ultra-large sensing device access

The installation of WSN sensing devices in the future will grow exponentially due to the needs for comprehensive monitoring in transportation, electricity, industry and other critical infrastructures. For example, in the monitoring of production equipment in factories, it is necessary for each device to install a variety of sensors to measure such device states as temperature and vibration. An estimate by ABI Research, 50 billion new machine-to-machine (M2M) devices will appear in the next 10 years, and the number of the WSN devices will account for most of the scale [41]. As a result, how to cope with a very large scale of WSN device access is an important challenge.

4.2.1 Massive heterogeneous data processing

With the large-scale application of WSN technology in the information and intelligence process of infrastructures, the amount of data produced by WSN sensors will grow from today's EB level (1 018 bytes) to ZB (1 021 bytes) level. According to IDC statistics and forecasts, in 2009, the global data volume was 0.8 ZB (1 021 bytes), and will be 35 ZB by 2020 [42]. As a major part of the data, the amount of sensing data from the physical world is 30 times more than that from human society. In this sense, the storage and transmission as well as timely treatment of mass data will be an unprecedented challenge.

WSN sensing data, including those of temperature, pressure, flow, speed and other physical dimensions, have multi-dimensional heterogeneous characteristics. The application of information and intelligent infrastructure require the fusion processing of those multi-dimensional heterogeneous data. However, the existing information processing technology is difficult to meet the growing demand for WSN.

4.2.2 Intelligent control and services to dynamic changes

Future operation and management of city infrastructures are required to meet the needs for safety, energy conservation, efficiency, convenience, etc. In the existing mode, information is automatically collected and processed through manual analysis, decisions and responses are made accordingly. Yet, this mode is no longer applicable. Intelligent control that is ready to respond to dynamic changes must be implemented. Firstly, WSN application mode should transform from simple perception to closed-loop control. For example, in intelligent transportation applications, to guarantee smooth urban transportation, it is necessary to make dynamic analysis on traffic conditions and real-time adjustments of traffic lights. Nevertheless, the infrastructure control is of great significance, so ensuring the security and reliability of intelligent control will be a major challenge. Secondly, the WSN service mode should transform from the single and predefined into the dynamic and personalized. For example, in smart power utilization, to ensure both the user's electricity demand and improve the efficiency of grid operation, the setting of the air conditioning temperature and light levels should be dynamically adjustable in

accordance with the grid current load, environmental conditions and personal preferences. Although, dynamically generating services in accordance with environmental changes will be a major challenge.

4.3 Sensor network architecture

Sensor network technology has been widely used in urban infrastructure construction with marked achievements. However, in different sensor network applications, network embedded sensing or controlling devices are usually based on different hardware platforms, operating systems, databases and middleware. And they cannot be deployed in a variety of heterogeneous network environments with free exchange of information except if supported by dedicated business systems and application management platforms. In terms of architecture design, most application environments of sensor network are designed in tightly coupled closed architectures. In this sense, the system presents features of an information silo and is only suitable for the application environment in small-scale industries. Moreover, it is difficult to share and reuse the infrastructure system architecture and services. Also, third-party resources are difficult to be cost-effectively integrated into the system. As a result, the application and promotion of large-scale sensor network technology is limited.

Thus, there is an urgent need to build a more open and flexible system framework to break this bottleneck of IoT. In order to share with convenience sensor information or control demand and integrate isolated data into sensor network, pervasive computing is inevitable for the development of sensor networks.

Web technology is the natural choice of technology to achieve pervasive computing and share heterogeneous resources, as it is a basic framework for the sharing of resources and services among platforms.

Currently, there are two trends in the world for web-related sensors: one enables people in different places around the world to easily share sensors and the other enables sensors to cooperate with other sensors.

4.4 High concurrent access

As wireless access technology proliferates in smart grids and other industrial applications, more rigorous performance requirements (large scale, low latency) are expected at the same time. Taking smart grid as an example, control applications in transformer substations usually requires a latency of 0.667 ms to 2 ms for networks with dozens of nodes, second-level latency for networks with thousands of nodes within the substation area, and second or minute-level latency for future advanced metering infrastructure (AMI) applications with thousands of nodes. Though current access technologies of WSNs can support second-level latency for the end-to-end transmission in hundred-scale networks, which is sufficient for monitoring applications, the demand for high concurrent access for future applications cannot be met yet. The drawbacks of the existing access technology when dealing with WSN applications with such characteristics as light traffic and high concurrency are given as follows:

- The existing scheduled-based access technology usually adopts such strategies as reserving retransmission time slots, frequency division among multiple users, non-reusable resource allocation etc., to guarantee transmission reliability. These protected resources are extremely underutilized.
- Contention-based access technology has to cope with the conflicts over resource utilization. As the data traffic of concurrent applications increases, the network performance will dramatically degrade.
- Applications with high concurrency characteristics, especially control applications, whose payloads are normally small, will suffer heavy overhead due to the large head of the packets

if existing access technologies are employed, and the efficiency of the spectrum access is also very low.

So far two solutions have been proposed to solve the problems above. One is the Bluetooth-based wireless interface for sensors and actuators (WISA) proposed by ABB; and the other is the IEEE 802.11™-based wireless networks for industrial automation – factory automation (WIA-FA) proposed by a group of Chinese organizations (more than ten members) led by Shenyang Institute of Automation, Chinese Academy of Sciences.

4.4.1 High concurrent access with frequency division multiplexing

Bluetooth technology operates within the range of 2 400 MHz to 2 483.5 MHz, has 79 designated Bluetooth channels and exchanges data over short distances. Bluetooth can be used on the physical layer to meet the requirements for light traffic and high concurrency. Besides, MAC layer can be designed to support time division multiple access (TDMA), frequency division multiplexing (FDM) and frequency hopping (FH) techniques. Long-wave radio frequency power supply is an advanced technology for power supplies.

4.4.2 High concurrent access with distributed antenna systems

IEEE 802.11™ [17] is a set of MAC and physical layer (PHY) specifications for implementing WLAN communication in the 2.4 GHz, 3.6 GHz, 5 GHz and 60 GHz frequency bands. Following the network architecture of distributed antenna systems, IEEE 802.11™–based PHY and the FDM and TDMA-based MAC layer are suitable for long distance communication. Besides, by jointly utilizing channel states-aware resource allocation, data aggregation, packet aggregation and other performance optimization methods, data latency can be reduced to 10 ms. IEEE 802.11™–based high concurrent access technologies can be broadly applied in industries, such as beer bottle filling and robotic production lines, see Figure 4-2.

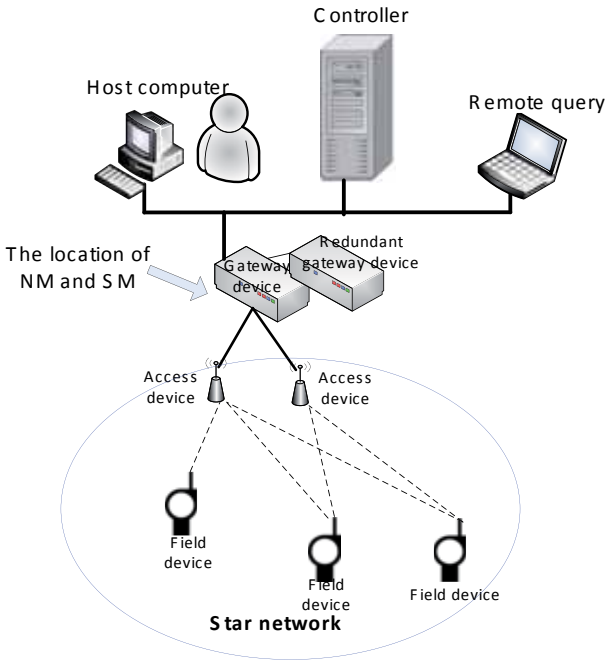


Figure 4-2 | High concurrent access with distributed antenna systems [14]

4.5 High real-time transmission

Traditional WSNs are used to perceive, collect and process information of the objects in the network covered areas and forward it to observers for offline or online analysis with low real-time requirements, such as meter reading, environmental monitoring, etc. The network coverage is limited (in a housing estate or an open space of several square kilometres) and the delay requirements are low (minute or hour levels). Therefore, traditional WSN research focuses on how to improve network reliability and reduce power consumption. However, with the continuous development of the infrastructures in smart cities, the network coverage area is increasing and so are the real-time requirements for transmission. Take the urban traffic control system for example. Information

such as road conditions and the number of vehicles, rate of speed, etc. must be collected in the whole city and then transmitted real-time to the control centre where the most appropriate traffic scheduling scheme is calculated and transmitted again real-time to the crossroads. This process needs to be completed within one second, which presents new demand for the real-time transmission of the sensor network system in wide areas.

Other network technologies can be used to build a wide-area sensor network (such as Ethernet, WLAN, mobile communications networks, etc.) and build heterogeneous networks with a variety of physical media and management mechanisms. Wired networks such as Ethernet use copper twisted pairs or optical fibres as a physical medium, with a rate of 100 Mbps to 1 000 Mbps or more and have a transmission delay of a few milliseconds; the transmission rate of wireless networks based on IEEE 802.11™ and IEEE 802.15.4 can be from 250 kbps to 72.2 Mbps, and the transmission delay ranges from a few hundred milliseconds to several minutes. The development of these network technologies, especially multiple-input multiple-output (MIMO) and orthogonal frequency-division multiplexing (OFDM) technologies in wireless communication, greatly increases the spectral efficiency of the wireless network and improve network performance, and thus lays a foundation for the building of a wide-area sensor network. However, these networks are operated in a best-effort manner, and have not taken into consideration the interconnection with other networks on how to ensure real-time transmission, which is the focus of future sensor networks research. The research of real-time sensor networks in wide area is a great concern throughout the world, and the solutions can be roughly divided into distributed and centralized ones.

4.5.1 Distributed solution

At the entrance of the network, the distributed solution divides transmission tasks into several levels according to the task requirement. Each part of the network schedules different levels of tasks according to the local network operating conditions, to ensure a wide-area and real-time protection. Distributed solution features a relatively high robustness, so damage to parts of the network does not affect the entire network. Besides, a distributed solution is implemented in the same manner as the internet, and is thus compatible with the existing web and can evolve smoothly. However, the local scheduling strategy of the distributed solution lacks an overall perspective and it is hard to make the best overall decision.

A proposed architecture is in Figure 4-3, which is a wide-area transmission network architecture establishing a cross-regional, real-time data integration and sharing mechanism in the smart grid. This architecture is based on mature IP, and IP's best-effort service model is both simple and unchanging, well-suited for distributed algorithms.

4.5.2 Centralized solution

The centralized solution, from the overall view, manages heterogeneous networks composed of wide area networks in a unified way. To meet such needs as the transmission tasks' delay, throughput, reliability, etc., the centralized solution reserves communication resources and conducts cooperative scheduling in various heterogeneous networks, which ensures the overall end performance requirements. A centralized solution is superior in that it can optimize global scheduling with better transmission performance. Nevertheless, complexity is its weak point so it can only be installed on certain private networks in specific areas.

The wide-area real-time network based on cognizing and coordination is proposed as follows. Cooperative scheduling of heterogeneous networks is conducted in a centralized manner through cross-layer sensing to obtain information about the network operation status, in accordance with the

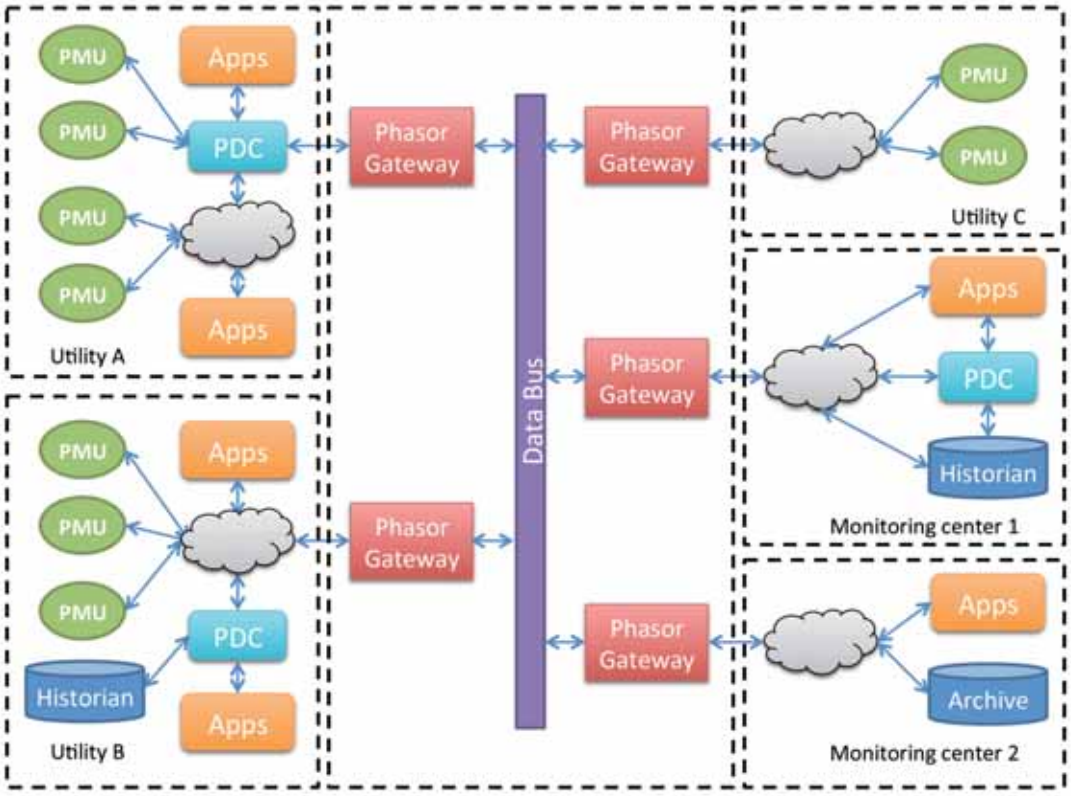


Figure 4-3 | Wide-area transmission network architecture [43]

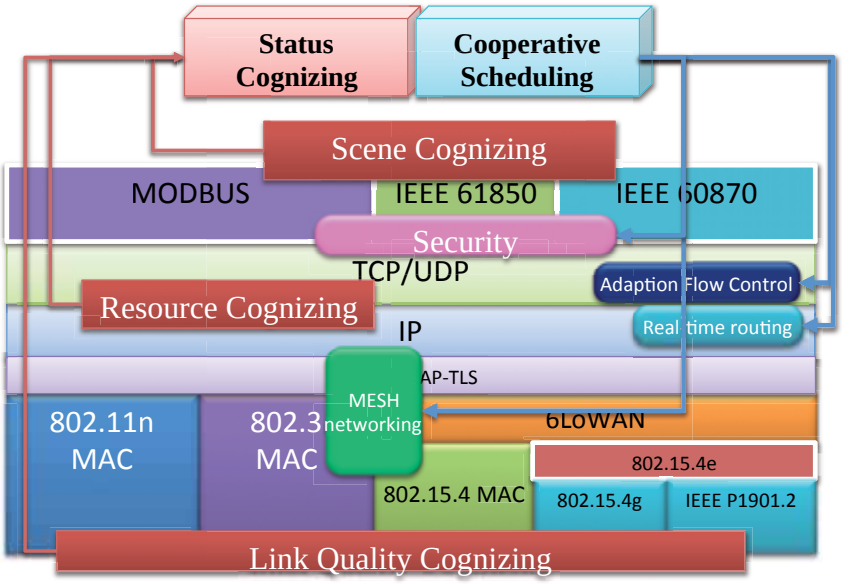


Figure 4-4 | Architecture of centralized wide area real-time network [14]

real-time requirements for task transmission. The solution is to focus on overall network management, which is complex and requires strong consistency, making it suitable in a centralized manner.

4.6 Semantic representation and processing

Semantic technology is one of the most important research fields in information technology in recent years, mostly due to huge expectations and demands for knowledge sharing and exchanging through networks. Semantic research on WSN information becomes a hot topic especially with the development of WSN and the expansion from the traditional concept of the internet to sensing layer devices. WSN semantic research focuses on the semantic representation of the physical world perceived by sensor nodes. In brief WSN semantics refers to the meaning or sense of the information perceived by sensor nodes [44], with which the underlying data can be put into better use.

Semantic WSN research originated in the semantic web. The existing web content gives priority to unstructured and semi-structured text. While the semantic web can give information on the web to a correctly defined meaning, it aims at ensuring a better cooperation between computers and people. However, the medium of WSN is the sensor node, whose information content is completely different from that of the web, in order to accommodate the semantic information of WSN nodes to the WSN application, scientific research institutes and standardization organizations have put forward corresponding solutions in the field.

Three areas have been identified as becoming hot research topics for the realization of sensor semantic issues:

1) semantic representation technology for terminal devices, directly adds semantic tags to sensor data in terminal device levels to achieve semantic representation,
2) semantic platform based on querying implements the sensor data query through the semantic interpretation of sensor data, and,
3) semantic analysis and management of sensor information based on cloud computing technology. It is expected that this could support large-scale sensor nodes, semantic expression, and processing based on cloud computing platforms.

4.7 More secure WSNs

Nowadays, WSNs connect the infrastructure of physical entities tightly with the information network. Damage to the infrastructure (such as power, transportation, chemical plant and national security) by virus threats will result in unimaginable consequences. WSN is usually more exposed to various security threats as the unguided transmission medium is more susceptible to security attacks than those of the guided transmission medium. TSP problems have to be taken into account right from the beginning. The threats to which a WSN is exposed can only be partly addressed by network security technologies. The defence against complex attack forms, such as Sybil, Dos and abnormal nodes, is not satisfactory [45].

As the goal of TSP in WSNs is to protect the information and resources from attacks and misbehaviour, the possible requirements to implement this goal are huge, like availability, authorization, authentication, anonymity, confidentiality, freshness, integrity, node protection, non-repudiation, privac, etc. In the future, the scale of WSNs could become greater and the combination of WSNs with the internet tighter. Although research efforts have been made with regard to node security, cryptography, key management, secure routing, secure data aggregation, something will do to ensure more secure WSN in the future.

4.7.1 Protocol security framework

In view of the computing ability, energy consumption and communication bandwidth of sensor node limits, protection of privacy and identity management, studies need to be made on the protocol security framework which is suitable and a common model for each layer in WSN. Because a single security solution for a single layer may not be a more efficient solution, the holistic approach for security would involve all the layers for ensuring overall security in a network [46]. Its goals aim at improving the performance of WSN with respect to security, longevity and connectivity. Its principle is that the cost for ensuring security should not surpass the assessed security risk at a specific time.

There are many methods that are now being proposed to ensure special layer security in WSNs, such as secure wakeup for nodes, tamper-proofing, authentication and encryption for network layers, logging for application layers. Nevertheless, how to structure other layers protocol and make up a common protocol security framework is a major research issue in future.

There will be a common model that can combine all security layers mechanisms together. The others can protect WSNs from attacking even if a layer is failing. But the cost-effectiveness and energy efficiency could still pose great research challenges in the coming years.

4.7.2 Trust, security and privacy

Confidentiality, personal rights to privacy, data security and integrity come at a cost. The question is: what is the cost benefit ratio when looking at the benefit the solution provides? Is the individual willing to forfeit his or her rights in order to gain the benefit? Google and Apple have been able to take great liberties with personal data in return for

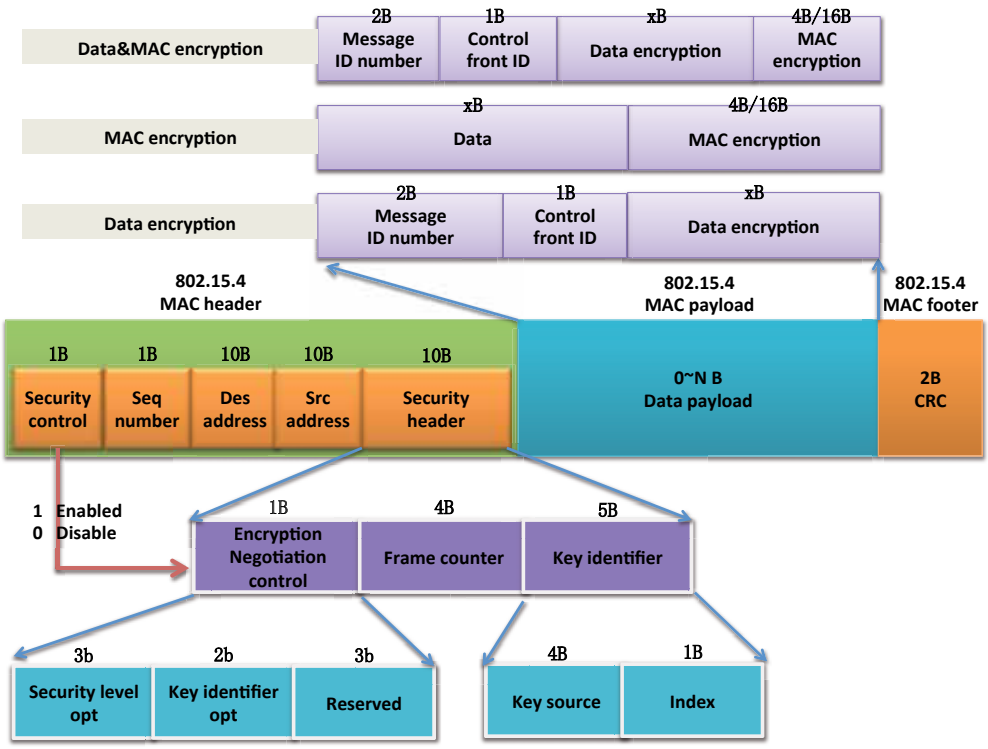


Figure 4-5 | Link layer security protocol framework [14]

benefits that outweigh the risks – at least for many consumers. Within an enterprise context, losing control of customer data and potentially sharing with data brokers breaks the trusted relationship that often legally unties longstanding confidential business to business relationships.

The personal key infrastructures and certificate authority responsibilities within an infinite number of data sources will tax the system and many will look to minimize proactive security measures and only look to deal with cyber-attacks when they actually happen – thus forcing the risk onto the overall system. IoT networks sending malware packets to all connected systems start to sound like the worst nightmare of any Hollywood science fiction film. In the end, it will be important to keep as many systems as possible separate from another to ensure the vulnerability of one system does not infect all systems. This potential domino effect is probably the worst case scenario as poor data integrity can lead to failures in magnitude that were not envisioned by any one system. The proactive security systems will be dependent on understanding what is “normal” cyber-physical data traffic, but this again might be excessively costly and reduce the benefits or increase costs of mandatory IoT solutions.

For safety, there are four qualities of WSN frameworks to consider. Firstly, the security of WSNs are vulnerable to network attacks due to the broadcast nature of the transmission medium and the limitation of computing resources of sensor nodes, like smaller power and smaller bandwidth. Secondly, identity and trust management are more complicated and difficult due to the deep integration of information space with the physical world and ubiquitous access to information technology. Thus, identity management and trust systems are faced with great challenges. Thirdly, the dynamic, heterogeneous and mass characteristics of WSN perception and computing model are also great challenges to the protection of effective system integrity, data integrity, data confidentiality, user privacy, like identity, behaviour, and environment. Finally, since the WSN has a large number of terminals, various terminal types and dynamic adaptive network structures, the size and complexity of environmental data are major challenges for the existing security posture monitoring system.

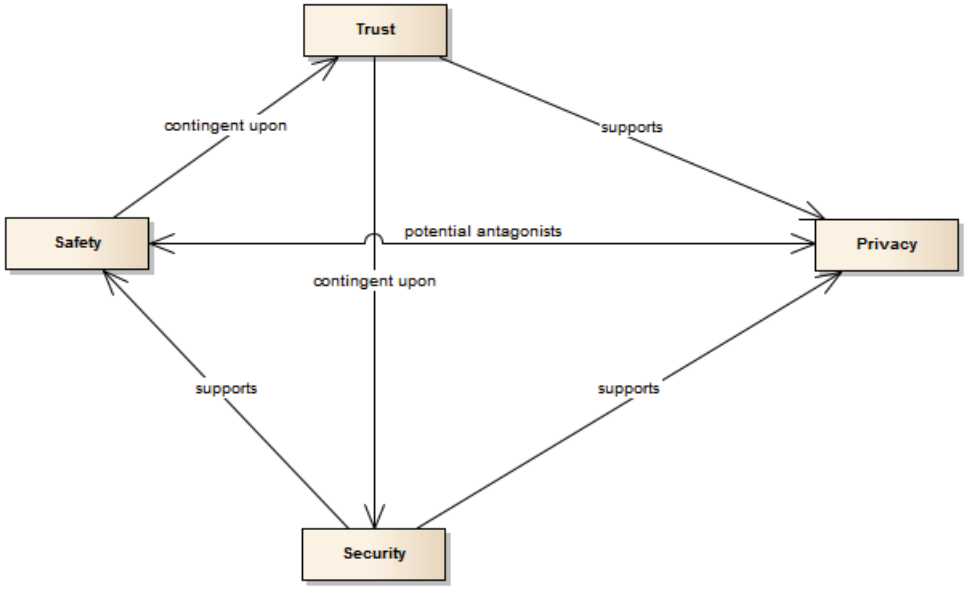


Figure 4-6 | Trust security and privacy [14]

Section 5

WSN applications in the infrastructure systems

5.1 WSN application in the smart grid

The power grid is not only an important part of the electric power industry, but also an important part of a country's sustainability. With the dependence on electric power gradually increasing, demand for the reliability and quality of the power grid is also increasing in the world. Utilities, research institutions and scholars have researched how to modernize the power grid to one that is efficient, clean, safe, reliable, and interactive.

A smart electricity grid opens the door to new applications with far-reaching impacts: providing the capacity to safely integrate more renewable energy sources (RES), electric vehicles and distributed generators into the network; delivering power more efficiently and reliably through demand response and comprehensive control and monitoring capabilities; using automatic grid reconfiguration to prevent or restore outages (self-healing capabilities); enabling consumers to have greater control over their electricity consumption and to actively participate in the electricity market.

Sensors will be a key enabler for the smart grid to reach its potential. The idea behind the "smart" grid is that the grid will respond to real time demand; in order to do this, it will require sensors to provide this "real time" information. WSNs as "smart sensing peripheral information" can be an important means to promote smart grid technology development. WSN technology in the smart grid will also further promote the industrial development of WSNs.

5.1.1 Online monitoring system for transmission lines

The condition of transmission lines are directly affected by wind, rain, snow, fog, ice, lightning and other natural forces; at the same time industrial and agricultural pollution are also a direct threat to the safe operation of transmission lines. The operating environment of transmission lines and the operating states are very complex, which requires more automatic monitoring, more control and protection equipment to automatically send alarms when accidents occur and dispatch strategy adjustment according to the operation mode, thus the faults will be processed at the early phase or be isolated in a small range.

Traditional wired communications cannot meet the communication needs of online monitoring of transmission lines. WSNs have an advantage of the strong ability to adapt to harsh environments, large area coverage, self-organization, self-configuration and strong utility independence and are very suitable for data communication monitoring systems for transmission lines.

With the technical advantages of WSNs, establishing a full range, multi element online monitoring system can send timely warnings of disasters, rapidly locate the positions of faults, sense transmission line faults, shorten the time of fault recovery and thus improve the reliability of the power supply. WSN use can not only effectively prevent and reduce power equipment accidents, when combining with the conductor temperature, environmental and meteorological real-time online monitoring, but can also provide data to support transmission efficiency improving and increasing dynamic capacity for transmission lines.

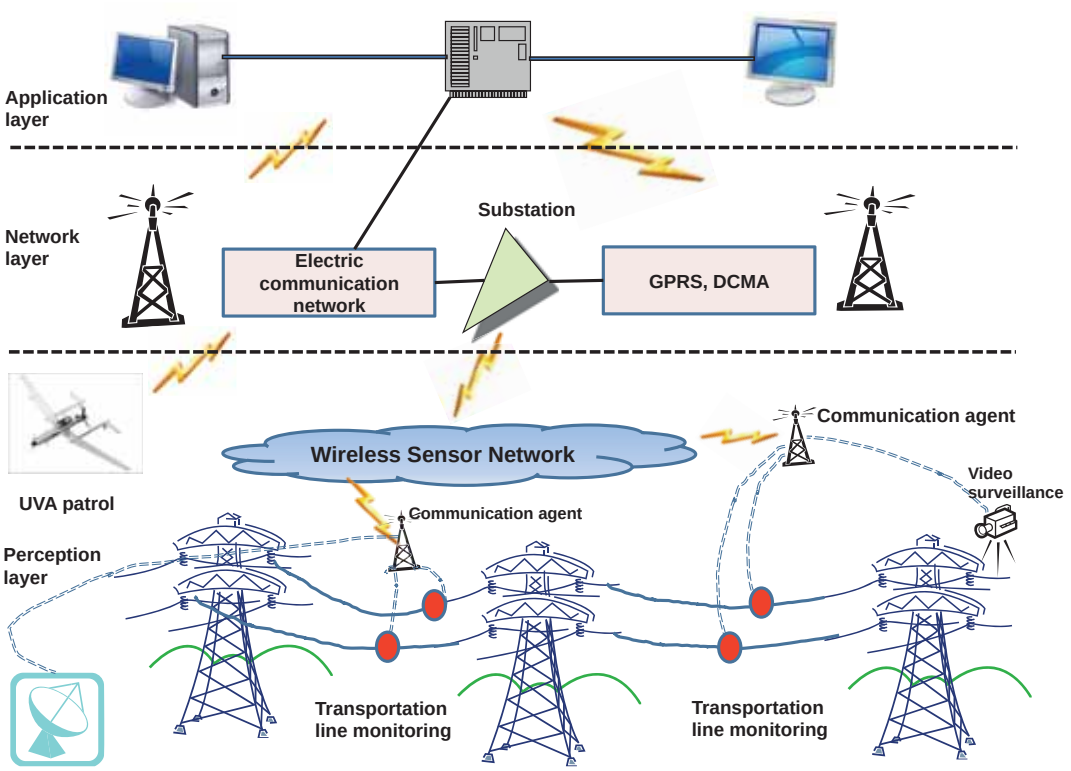


Figure 5-1 | General architecture of online monitoring system for transmission line based on WSNs [47]

The general architecture of online monitoring systems for transmission lines is shown in Figure 5-1.

Currently, some provincial power companies of the State Grid Corporation of China (SGCC) are promoting applications of WSN technology in the online monitoring of transmission line. For example, since 2013, Liaoning and Ningxia electric power companies are developing demonstration projects based on WSN for transmission lines online monitoring system.

5.1.2 Intelligent monitoring and early warning system for substations

After decades of development, the domestic substation automation technology has reached the international standards level. Most of the new substations, regardless of voltage level difference, adopt integrated automation systems. It is estimated that since 2005, more than 200 digital substations with different degrees of automation, voltage grades and modes have been put into operation.

Compared with the conventional substations, digital substations focus on the network information digitization, substation information standardization and networked transmission. For substations in smart grid, more attention is focused on smart power equipment, information exchange, interoperability and the intelligence application functions of the inner station. Now many smart monitoring functions can be realized and can improve the intelligent substation management, including the transformer/breaker/temperature monitoring, current leakage monitoring of lightning arrester,

electric leakage monitoring equipment, SF6 leakage monitoring of combined electric equipment, secondary equipment environmental monitoring, equipment anti-theft monitoring, etc. Applications of WSNs, can provide reliable, accurate, real-time, safety, sufficient information for the substation management, not confined to the traditional electrical quantities information of telemetry, remote communication, remote control, remote adjustment, but also including equipment information, such as the cooling system condition, the circuit breaker action times, the energy storage state of transmission mechanism, size of breaking current, and environmental information, video information, etc., finally achieve digitalization of information description, integration of data acquisition, data transmission by network, intelligent data processing, data display visualization and scientific production decision-making.

For example, SGCC joined forces with Shenyang Institute of Automation (SIA) of Chinese Academy of Sciences to establish the state maintenance system using WSN technologies. In Liaoning province and in Panjin south circle, China, 220 kV smart substations were successfully used to establish the auxiliary control systems. After the two systems were put into operation, the power grid was stable and data transmission ran well. It achieved the anticipated effect of communication, was accepted and made a good demonstration model.

It should be noted that service solutions based on WSNs will have to be aligned with the international standardization activities going on within smart metering (e.g. series of International Standards IEC 62056 (DLMS/COSEM), driven by the DLMS user group).

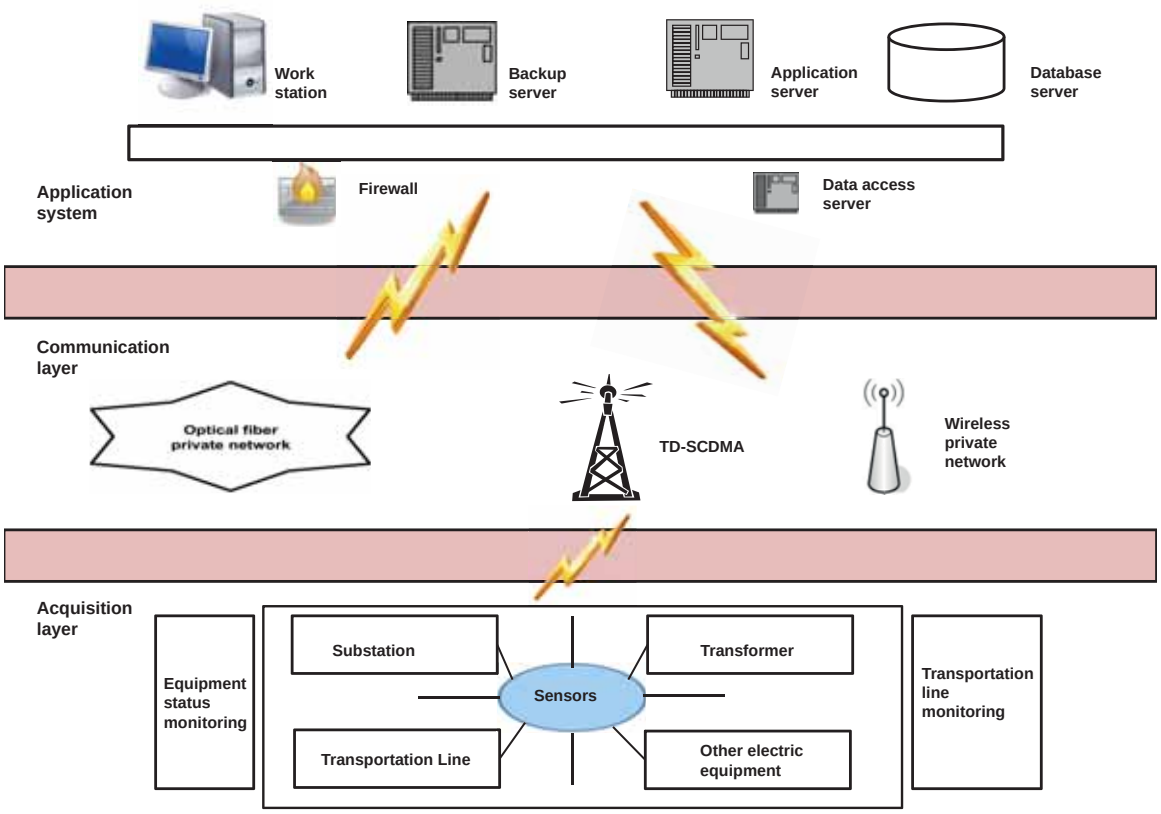


Figure 5-2 | Architecture of operation status monitoring for equipment [47]

5.1.3 Online monitoring and early warning system for distribution networks

Distribution networks directly connect the power grid with users, and distribute electrical energy to them. Reliability and quality of distribution network is an important element for reliable power supplies. The distribution network consists of primary equipment such as feeders, distribution transformers, circuit breakers, switches, and secondary equipment such as relay protections, automatic devices, measurements and meters, communication and control equipment, etc.

Distribution networks have characteristics of a massive number of points, large coverage areas and long distance power lines. The application of WSN in distribution fields can strengthen management, save manpower, improve the reliability of the power supply and accelerate the recovery efficiency of fault handling. SGCC supported an IoT application demonstration project in Ningxia Yinchuan, Henan Hebi, China, and verified that the application of WSN technology in power distribution networks can provide protection and support for the construction of distribution networks in the following aspects:

1) By deploying integrated sensing equipment, power quality variations and load situation of large electricity can be monitored, moreover the accuracy and timeliness of voltage, current, harmonics and other information are improved.

2) By utilizing RFID, navigation, video surveillance, smart wearable technology together, capability of the real-time monitoring over the status of distribution equipment and environment parameters is strengthened. It can improve the fault location of distribution lines.

3) By monitoring distribution line conditions, underground distribution pipe networks, higher automatic levels of field operation monitoring and anti-theft facilities can be achieved.

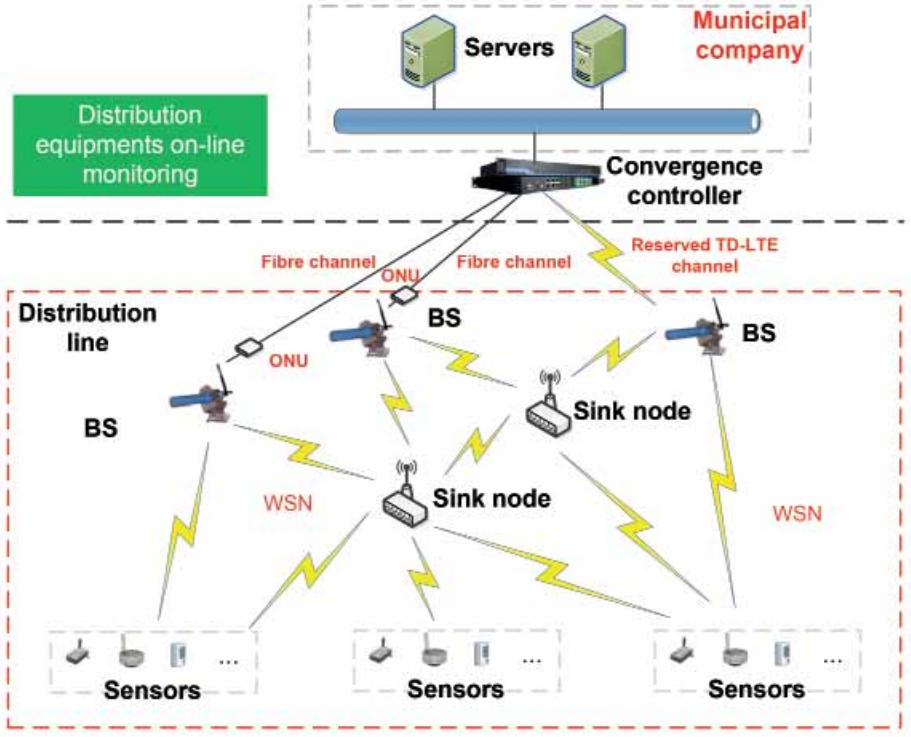


Figure 5-3 | WSN technology used in distribution network monitoring applications [47]

5.1.4 Smart electricity consumption services

Intelligent electricity consumption services rely on a strong power grid and the concept of modern management, based on advanced metering, high efficiency control, high speed communication, and quick energy storage technology, to realize the real time interaction between power networks, customer energy flow, information flow, and business flow.

WSNs can connect the terminal equipment of the supply side and the user side with sensors to form a complete interactive network for electric energy consumption information and realize electricity information acquisition in a complex environment. Information integration analysis based on WSNs can guide the user or directly adjust the electricity consumption style, to achieve the best configuration of power resources, reduce the electrical supply costs, improving reliability and efficiency. WSNs have broad application prospects in the intelligent electricity consumption fields such as intelligent communities, intelligent industrial parks, etc.

The electric energy data acquisition system is a basis for intelligent electricity consumption services. The system could comprehensively collect several kinds of large users data. This includes data for special transformers, medium and small users of special transformers, three-phase general business users, single-phase general industrial and commercial users as well as resident users and public distribution transformer data for examination of metering points. This data can be combined to construct integrated power information platforms. The architecture of a WSN-based electric energy data acquisition system is shown in Figure 5-4.

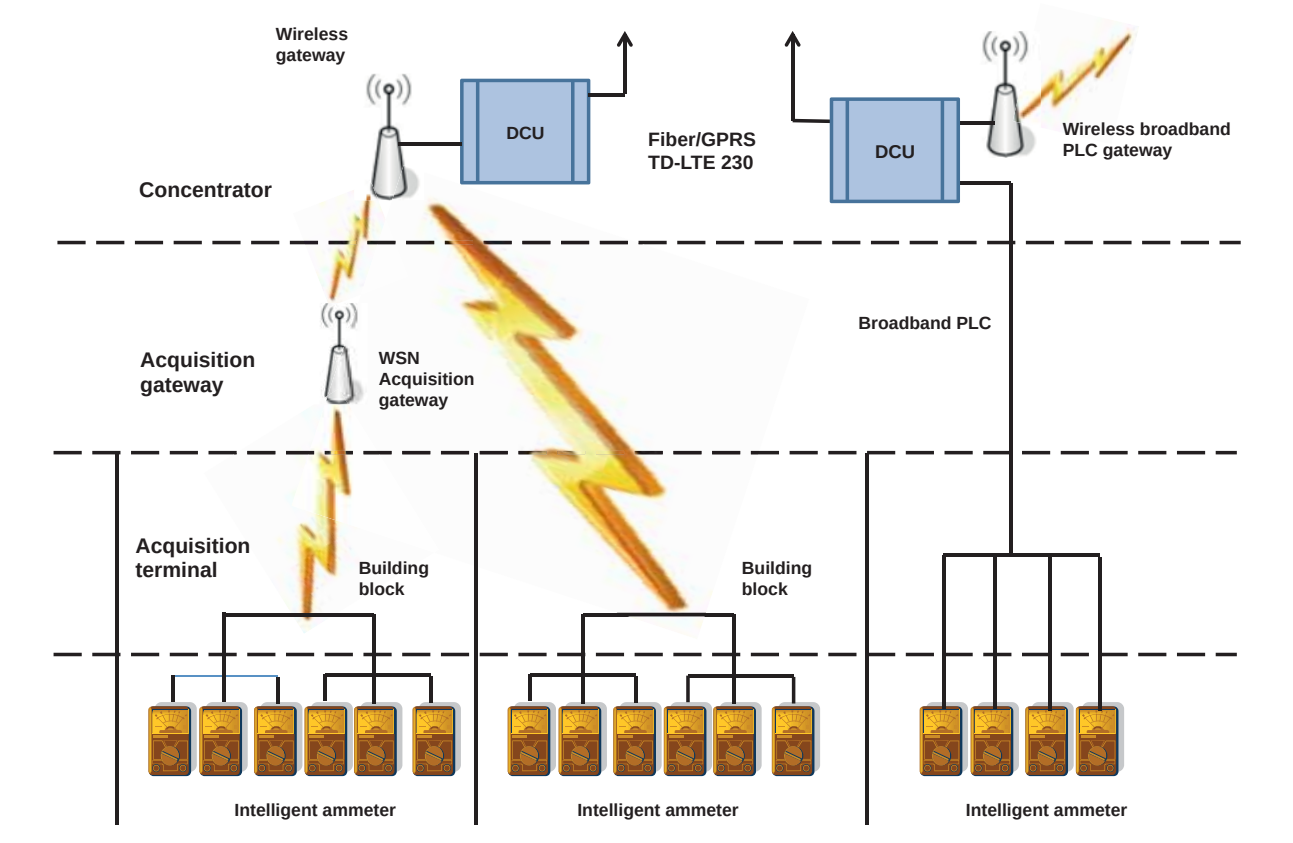


Figure 5-4 | Architecture of WSN based electric energy data acquisition system [47]

At present, some provincial power companies of SGCC have begun to use the automatic meter reading system based on WSN technology. For example, Liaoning Province Electric Power Limited Company has carried out WSN-based electric energy data acquisition system for more than 20 000 households. The communication system is based on the industrial wireless network standard WIA, and has achieved good results during operation testing. The main station has an accurate clock, thus the concentrator clock can be synchronized by the upstream communication network.

5.2 WSN application in smart water networks

Today, the world's water consumption is 300 % of what it was in 1950. The strong growth of the world's population combined with a strong growth of what is known as the middle class will continue to create increasing demand for the planet's limited resources. An example of a key resource in this context is the availability of clean water. In addition to the usual governmental regulation and policing of the exploitation of natural resources, many corporations are seeing the impact on the environment. They also see social and commercial advantages in taking steps to ensure the negative impact their operations have on natural resources is minimal. These are usually captured by monitoring environmental impact within a complex score card such as Figure 5-6 where the monitoring of impact on water pollution would be just one example.

Figure 5-5 | Monitoring of water networks [48]

5.2.1 Sustainability (water resource focus)

There are share price implications as well as regulatory requirements that drive this new green behaviour. It can be said that it is generally accepted in modern society that the perceived need to better manage the environmental impact corporations have on scarce resources and the CO_2 footprint as an indication of pollution costs to society versus profit will become increasingly important. Thus the trend for corporations to invest in this area in addition to governments creating regulations demanding compliance to new environmental rules and creating new national market entry costs is clear.

When focusing on clean water, a monitoring system has to be built to determine base line quality as well as monitor the various potential sources of contaminants to clean water. Traditional operational technology systems are not usually created to monitor potential pollutants, thus new sensors and actuators need to be used to monitor also air-born pollutants that are usually the most difficult pollutants to track and manage. The information gathered can not only be used as a key performance indicator (KPI) dashboard but also be used to predict water quality based on real-time monitoring of related events, such as manmade (pollution) or environmental (weather) events. This can be useful for corporations who are always working within an international regulatory framework, and can potentially lead to additional value creation in the form of emission/pollution certificates.

This mind shift means that corporations need to shift from a mentality of traditional operational efficiency to sustainability as a competitive advantage in an ever aware market. This means that value has to be captured and given to products and services that have the least negative impact on the environment.

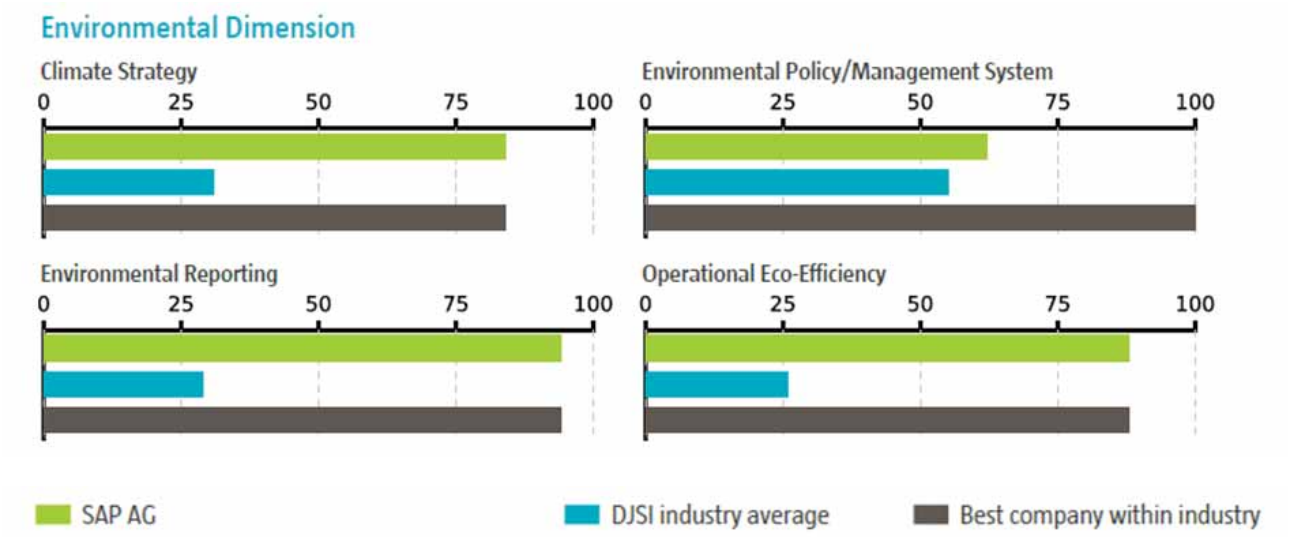


Figure 5-6 | Example of score card [49]

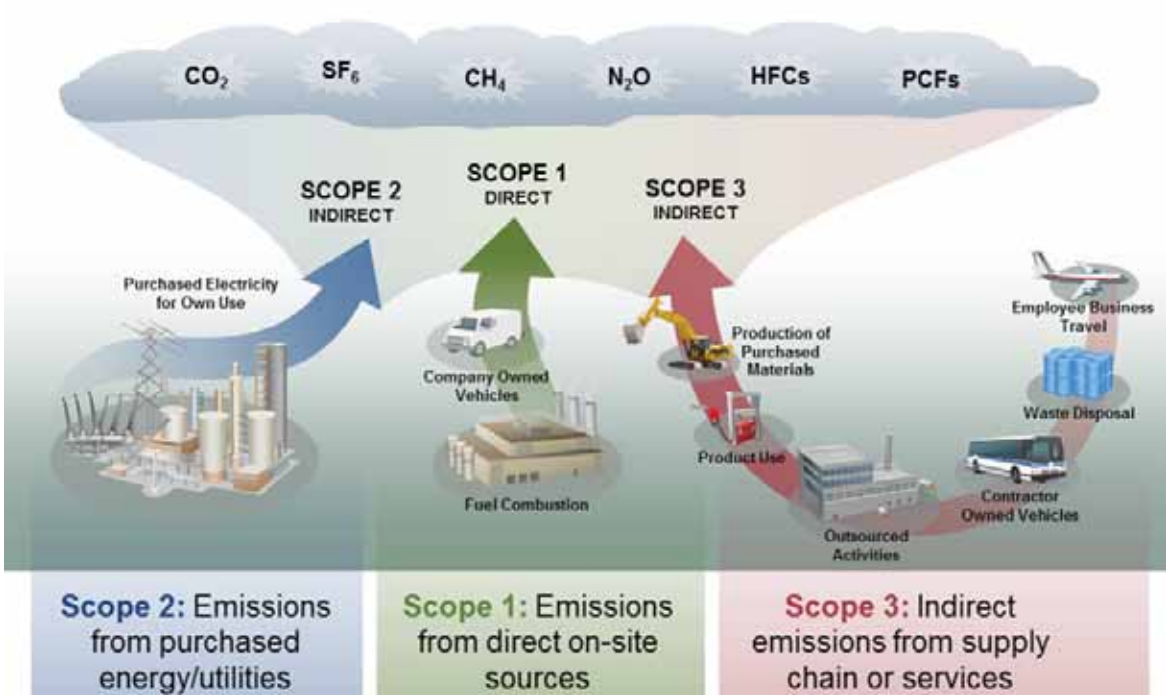


Figure 5-7 | Airborne pollutants greenhouse gases (GHG) a threat to water [48]

5.3 WSN application in intelligent transportation

Wireless sensing in intelligent transportation differs on several points from the traditional concepts and design requirements for WSN. In most cases, sensors can rely on some sort of infrastructure for power supply, for example the aspect of energy efficiency is usually of secondary importance in these systems.

WSN applications in intelligent transportation can be subdivided into two categories:

1) Stationary sensor networks, either on board of a vehicle or as part of a traffic infrastructure.
2) Floating sensor networks, in which individual vehicles or other mobile entities act as the sensors.

The latter category comprises applications related to the tracking and optimization of the flow of goods, vehicles and people, whereas the former comprises mainly applications that were formerly covered by wired sensors.

5.3.1 Sensing of traffic flows

Intelligent traffic management solutions rely on the accurate measurement and reliable prediction of traffic flows within a city. This includes not only an estimation of the density of cars on a given street or the number of passengers inside a given bus or train but also the analysis of the origins and destinations of the vehicles and passengers.

Monitoring the traffic situation on a street or intersection can be achieved by means of traditional wired sensors, such as cameras, inductive loops, etc. While wireless technology can be beneficial in reducing deployment costs of such sensors, it does not directly affect the accuracy or usefulness of the measurement results.

However, by broadening the definition of the term “sensor” and making use of wireless technology readily available in many vehicles and smart phones, the vehicles themselves as well as the passengers using the public transportation systems can become “sensors” for the accurate measurement of traffic flows within a city.

Techniques for collecting traffic flow data from vehicles are collectively referred to as floating car data (FCD). This includes methods relying on a relatively small number of vehicles explicitly transmitting their position information to a central server (e.g. taxis or buses sending their position obtained via GPS) as well as approaches relying on location information of mobile phones obtained from real-time location databases of the cellular network operators. The latter approach does not actually involve any sensing by the vehicle itself, but still makes use of a wireless network (i.e. the existing cellular network) to sense or rather infer the current characteristics of traffic flows. The technical challenges lie particularly in the processing of the potentially large amounts of data, the distinction between useful and non-useful data and the extrapolation of the actual traffic flow data from the observation of only a subset of all vehicles.

Extensions of the FCD idea involving information gathered from the on-board electronics of the vehicles have been proposed under the term extended floating car data (XFCD). Collecting and evaluating data from temperature sensors, rain sensors, ABS, ESC and traction control system of even a relatively small number of cars can be used to derive real-time information about road conditions which can be made available to the public and/or used for an improved prediction of traffic flows based on anticipated behaviour of drivers in response to the road conditions.

Privacy issues must be taken into consideration whenever location or sensor data is collected from private vehicles. However, this is a general concern related to the monitoring of traffic flows, and schemes that don’t make use of wireless technology (e.g. relying on license-plate recognition) also have to consider the car owners’ privacy.

Equivalent to the measurement of vehicle movement by FCD, passenger behaviour in public

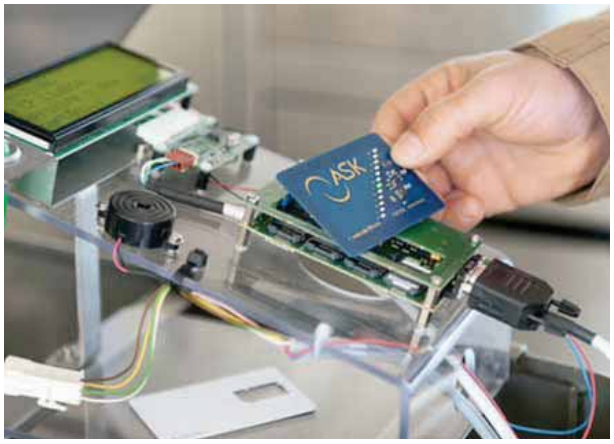


Figure 5-9 | Electronic tickets for smarter travel [50]

transportation systems can be analyzed with the help of wireless technology. For example electronic tickets, which typically employ RFID technology for registering the access to a subway station, bus or tram, effectively turn the passenger into a part of a sensor network.

The possibilities for gathering information about passenger movement and behaviour can be further increased if smart phones are used to store electronic tickets. Especially for gathering information about intermodal transportation habits of passengers, electronic ticket applications for smart phones offer possibilities that conventional electronic tickets cannot provide. It remains to be seen, however, to which extent users will be willing to share position data in exchange for the convenience of using their mobile phone as a bus or metro ticket.

5.3.2 City logistics

Urbanization is posing a lot of challenges, especially in rapidly developing countries where already huge cities are still growing and the increasingly wealthy population leads to a constantly rising flow of goods into and out of the city centres.

Delivery vehicles account for a large portion of the air pollution in the cities, and streamlining the flow of goods between the city and its surroundings is the key to solving a lot of the traffic problems and improving the air quality.

A promising approach towards reducing the traffic load caused by delivery vehicles is the introduction of urban consolidation centres (UCCs), i.e. warehouses just outside the city where all the goods destined for retailers in a city are first consolidated and then shipped with an optimized routing, making the best possible use of truck capacity and reducing the total number of vehicles needed and the total distance travelled for delivering all goods to their destinations.

To achieve such optimization, careful analysis and planning of traffic flows in the city as well as monitoring of the actual flow of the goods are needed. The challenges and the solutions are similar to the ones discussed in 5.3.1, but with a finer granularity. Rather than just tracking a subset of vehicles as they move through the city, tracking of goods at least at a pallet level is required. The pallet (or other packaging unit) thus becomes the “sensor” for measuring the flow of goods, and a combination of multiple wireless technologies (GPS, RFID, WLAN, cellular) in combination with sophisticated data analysis techniques are applied to obtain the required data for optimizing the scheduling and routing of the deliveries and ensure timely arrival while minimizing the environmental impact of the transportation.

5.3.3 On-board WSNs

Vehicles of all kinds rely on an increasingly large number of sensors to ensure safe and smooth operation. This includes sensors primarily providing information to the driver as well as sensors that are part of the propulsion or vehicle dynamics systems. Due to the safety-critical nature of those subsystems, wireless technology is not usually a feasible option for these applications.

However, especially in large vehicles such as busses, trains, and airplanes, a lot of sensors and actuators serve non-safety-critical purposes, e.g. monitoring cabin temperature, collecting data used in preventive maintenance of the vehicle or monitoring the status of transported goods.

In railway applications, WSNs can play an important role in the refurbishment of old carriages with state-of-the-art electrical systems.

In airplanes, saving the weight of copper or aluminium cables by applying wireless sensors for non-critical applications is an important consideration. Wireless sensors employing energy harvesting techniques have been discussed even for monitoring the mechanical stress on composite materials forming part of the aircraft structure. Wiring the sensors in such "smart materials" would increase the weight of the structure and therefore significantly reduce the advantages of the composite material over conventional metal structures.

5.3.4 WSN in traffic infrastructures

Traffic lights at intersections are usually controlled by units located close to the intersection, taking inputs from a set of sensors (e.g. inductive loops) as well as commands from a centralized control unit and switching the individual lights (also known as signal heads) according to the traffic rules and situational requirements.

With the number and complexity of sensors and display elements increasing, the task of a traffic controller today is really based on communication rather than a pure switching of the connected components. Traffic lights may be equipped with count-down timer displays, variable message signs display updates speed limits, and optical or radar-based sensors deliver information about the occupancy of individual lanes or the speed of vehicles passing the intersection.

Upgrading the infrastructure of an existing intersection with state-of-the-art technology requires also providing the necessary communication links between sensors, signal heads, variable message signs, traffic controllers and other components. Wireless technology can help reduce the cost by eliminating the need to route communication cables (e.g. Ethernet) to all devices in an intersection. Such an installation will in most cases not be a pure sensor network, as it will usually also include display components or actuators. Furthermore, a combination of wired and wireless communication links and possibly even a combination of different wired/wireless standards within the same system due to a combination of components from different vendors are not unlikely.

Interaction of the traffic infrastructure with vehicles through wireless communication (e.g. granting priority to busses or emergency vehicles at intersections) is another promising application for wireless technology in traffic infrastructure. Though not all possible applications actually involve the exchange of sensor data over the wireless communication links, there are also a number of scenarios in which either vehicles share their sensor data with the infrastructure elements (e.g. regarding speed when approaching the intersection) or where the infrastructure provides sensor data to the vehicles (e.g. regarding road congestion on the other side of the intersection).

5.4 WSN application in smart homes

5.4.1 The energy challenge

Faced with growing consumption and high energy costs, as well as the scarcity of fossil fuels, all of the scenarios developed by public institutions and experts to curb energy demand and our CO_2 emissions at the same time converge on: energy efficiency being an absolute priority.

In Europe, the energy consumption of buildings (residential and tertiary) represents 40 % of the total energy consumption, industry is 30 % and transportation is 30 %.

Public authorities take it very seriously. As an example in Europe, the Energy Efficiency Directive, adopted in October 2012, heads in this direction. It includes measures about buildings renovation; long term renovation roadmaps for commercial and residential buildings and 3 % renovation rate for central public buildings. Each member state of the European Union had to translate these objectives into national law by June 2014.

5.4.2 Energy efficiency in buildings – Case study

A collaborative programme named HOMES has been launched by Schneider Electric in France in 2008 [51], and over a four year period the programme was designed to provide buildings with solutions to achieve better energy efficiency. The HOMES programme enabled the study, improvement and testing of simple, effective, economically sustainable active energy efficiency solutions using active control with the possibility of optimizing energy use by means of automated control and monitoring systems.

One of the achievements of this programme was to understand that the energy system is composed by three (quasi) independent subsystems, each one being responsible of useless energy consumptions:

1) Distribution subsystem (world of machines): energy production, transformation, storage.
2) Usage subsystem (world of people): energy services delivered to the occupants.
3) Constructive subsystem (world of materials): energy transfer between indoors and outdoors.

This programme has delivered a new vision of the energy performance of a building, built around solutions that simultaneously involve the quality of the enclosure, equipment performance and active control. These are three independent vectors of intervention, without a specific order of application and complementary to each other.

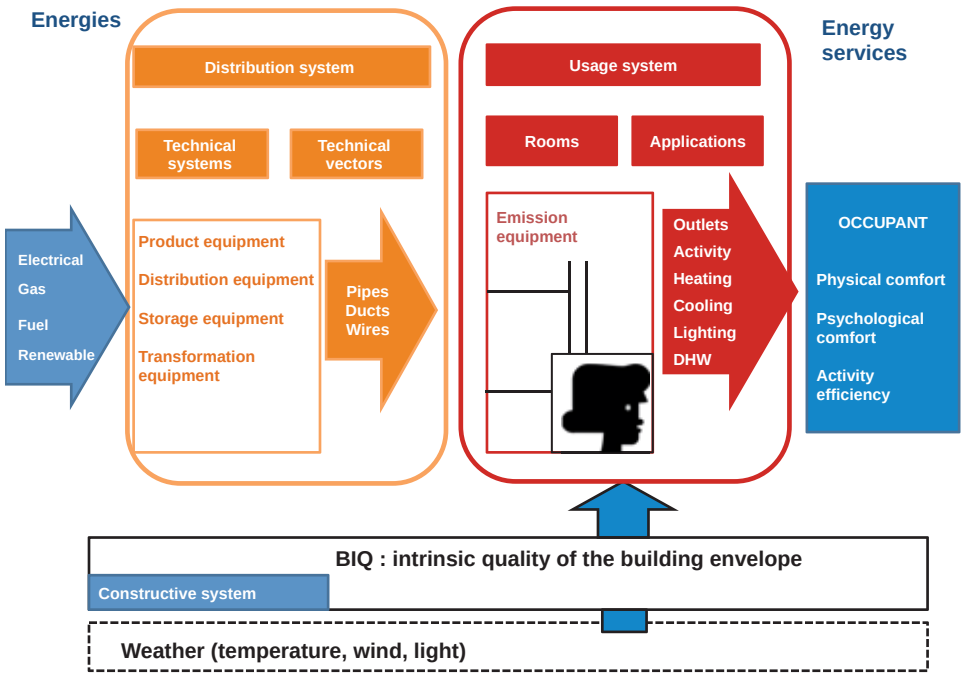


Figure 5-10 | Systemic approach of energy in buildings

5.4.3 Active control in buildings

Based on the vision described above, the HOMES programme has thus proposed a protocol of active control articulated around the three strategies to maximise building performance while making it smart grid compatible.

1) Act room by room: for maximizing the energy performance of a building, it is necessary to optimize the services rendered to the occupant, which is to say at the level of a room or a zone in a tertiary building. Thanks to the zone control, the occupant can adapt the environment to his or her activities and comfort.

2) Optimize energy supplies: to serve the needs of the occupants of a building, it is necessary to optimize the supply of energy based on the economic and carbon costs. The supply and distribution of energy are then managed as a function of the sum of the needs of each location. It enables control of the energy sources and the relationship with the upstream ecosystem consisting of the district, city, etc. This strategy facilitates anticipation of the development of smart grids. It creates a system where each level contributes to optimization at a higher level. It also participates in developing the demand management potential for electricity in buildings. Therefore, it is necessary to move from vertical independent application control to a multi-application control by zone.

3) Act on the engagement of the stakeholders: to improve the energy performance of a building, it is necessary to establish an incremental action plan to progressively look for sources of savings. However, the needs differ depending on the stakeholders involved. Information strategies must be implemented that are tailored to the specific needs of each stakeholder and their areas of responsibility for helping them to take energy efficient decisions.

Space and time fragmentation of the building and its technical systems have a strong impact on the efficiency of monitoring and energy savings through active control. Therefore, the implementation of active control strategies modify the sensing and control command architectures of active control solutions, to be based on a zone control ecosystem

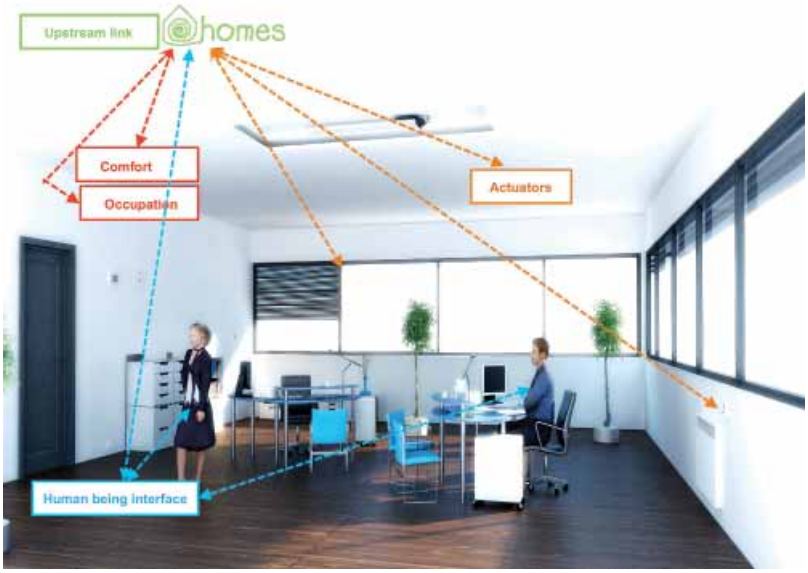


Figure 5-11 | Zone control [50]

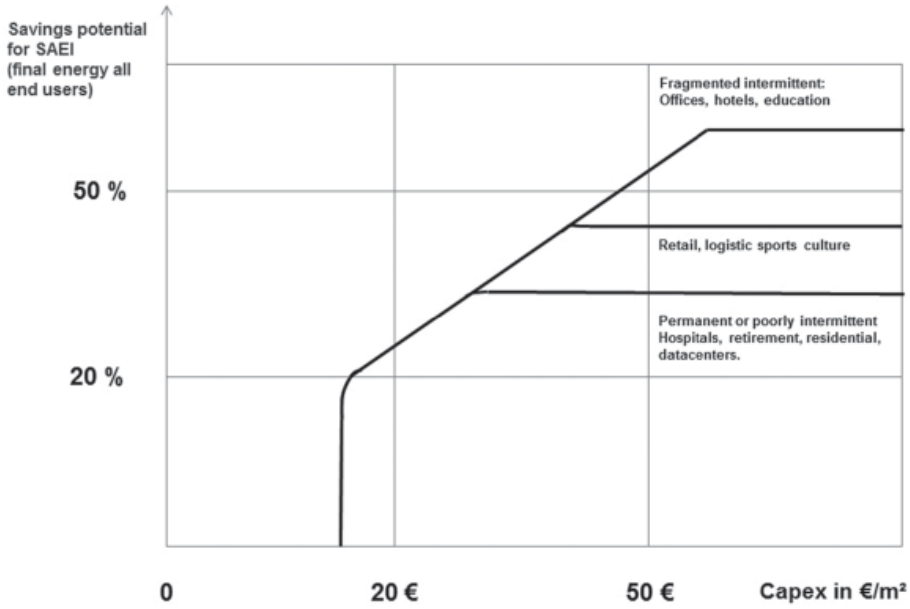


Figure 5-12 | Incidence on time fragmentation in savings [50]

Figure 5-13 | Savings [50]

as shown in Figures 5-11 and 5-12 where the comfort sensor is one of the key elements.

Further, this has been assessed on five pilot sites representing different climatic zones, sector, constructive age, heating energy, hot water energy and owner type. The savings went from 25 % for residential up to 56 % for the school, proving the relevance of the above assumptions, see Figure 5-13.

5.4.4 WSNs are key for improving the energy efficient performances of existing buildings

For achieving multi-applicative control at the zone level, it is necessary to closely monitor the environment (light, temperature, relative humidity, CO_2) as well as the activity of the occupants (presence detection, alarms). If we keep in mind that just a few percent of new buildings are built every year, the challenge is to deploy active control

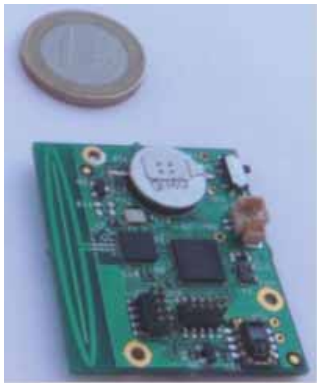


Figure 5-14 | Autonomous sensor electronics [50]

Figure 5-15 | Schneider Electric sensor prototypes [50]

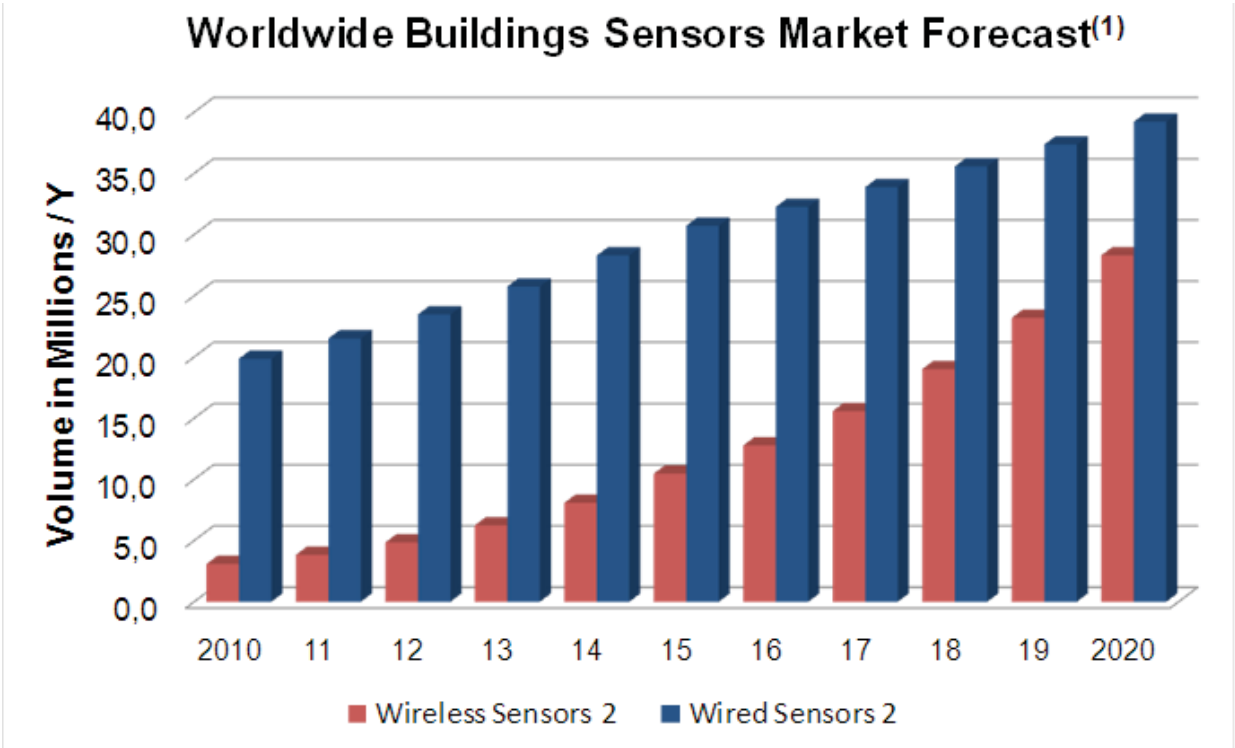


Figure 5-16 | Worldwide buildings sensors market forecast [52]

at the zone level in millions of existing buildings. The only way to achieve this is to use wireless, and even battery-less sensors for avoiding having hundreds of millions of batteries to manage and maintain.

The feasibility of a multi-physics wireless autonomous sensor has been demonstrated. The results were presented in Munich at the Energy Harvesting and Storage Conference in June 2011.

Powered by a photovoltaic (PV) cell, the prototype was able to measure temperature, relative humidity and light intensity, and to transmit it every 10 minutes on an 802.15.4 radio, using ZigBee® Green Power protocol. The average power consumption was 5 µW, enabling to have such a sensor operating continuously under less than 100 lux 8 hours/day.

From a study made by IMS Research in October 2011 [52], it is expected that sensors will have a continuous growth in the building market, with wireless sensors growing at a much faster pace.

From a communication protocol perspective, the ZigBee® Alliance has adopted the Green Power feature set as part of the ZigBee standard in 2012 [53]. It enables to integrate in a ZigBee® meshed network wireless sensors with very limited energy available like when powered by energy harvesting. This makes it a very attractive solution for control in a building.

WSNs are a key enabler for deploying multi-applicative control in buildings at the zone level, and they contribute significantly to improve energy efficiency by taking into account the building within its environment, while taking care of the comfort and the activity of the occupants.

5.5 Additional application benefits of WSN

5.5.1 Improve energy efficiency

As is indicated in the 2010 IEC White Paper, *Coping with the Energy Challenge – The IEC's Role from 2010 to 2030*: "but of the theoretical energy in the fuel, two-thirds is today lost in generation and another 9 % in transmission/distribution, so that of the primary energy consumed only about 30 % is available as electricity at the point of use." However, IoT can help to solve this problem. As an effective means to acquire information, it can implement real-time monitoring over the operation of energy conversion, and make timely analysis and processing of the large amount of data. In addition, it can also make speedy responses to abnormal status and guarantee the system security as it can enable a valid management of the whole process (from generation to transportation and usage) of the energy system in fine grain and dynamic mode.

5.5.2 Contribute to environmental monitoring

Environment pollution, sudden natural and ecological disasters and man-made damages are still the major environmental problems that need to be resolved at present. Early detection, alarming and initiation of emergency measures are key steps to avoid great environment disasters. IoT, featuring a powerful sensing ability and wide coverage of detecting area, can make a real-time and all-around monitoring over the environment. In this sense, with a data fusion and intelligent recognition technology, it can increase the alarming efficiency. As a result, it is reasonable to predict that IoT will play a key role in the warning and forecast of flood, forest fire and water pollution, etc.

5.5.3 Enhance social services

IoT offers a way for different elements in social services to relate and connect with each other through the internet: man, equipment, and social service resources. Thanks to IoT, on one hand, the service providers can obtain information about people's demands and provide them tailored and high-quality services; while on the other hand, people can have a better understanding of

themselves and the environment around them. It is safe to predict that IoT will change people's lifestyles in some aspects. For example, IoT-based smart health care and smart home systems will bring more convenience and comfort to people's lives.

Section 6

Standards of WSNs and systems

6.1 General

Standardization is a major prerequisite to achieve interoperability, not only between products of different vendors, but also between different solutions, applications and domains. The latter are of special interest to IoT and WSN as common access to devices, sensors and actors from various application domains leading to new cross domain applications is the major intent of IoT.

Interoperability has to be considered at different layers from component, to communication, information, function and business layer. The component layer basically reflects the devices like sensors and actuators, but also gateways and servers which run the applications. The communication layer is responsible for the data exchange between the components while the information layer represents the actual data. The function layer is concerned with the functionality which can be software applications, but also hardware solutions. At the business layer the business interactions are described. From the WSN and IoT approach to provide information exchange between “things” and applications covering various application domains, common communication and information layer standards are of main interests, but also generic functions might be used by different application areas. At the component layer we will find various types of devices, but still standards defining for example form factors and connectors for modules (e.g. wireless modules, control processing unit (CPU) boards) can make sense.

As a prerequisite for the successful standardization use cases and requirements have to be collected and architecture standards are needed to structure the overall system and identify the relevant functions, information flows and interfaces.

As WSN will be used in the wider context of IoT, also IoT standards and standardization activities are considered. This concerns especially the higher communication protocol, information and function layer.

Note that the list of standards and standardization activities below is not exhaustive.

6.2 Present status

IEEE 802.5.14 is the most relevant communication standard for the WSN. It defines the physical and link layer for short-range wireless transmission with low power consumption, low complexity and low cost. It uses the ISM frequency bands at 800/900 MHz and 2.4 GHz. IEEE 802.15.4 is the foundation for other standards like ZigBee®, WirelessHart, WIA-PA and ISA.100.11a which define regional or market specific versions. The base standard was published in 2003 and revisions in 2006 and 2011. Various amendments have been added to cover additional physical layer protocols, regional frequency bands and specific application areas. Current work is covering additional frequency bands (e.g. TV white space, regional bands), ultra-low power operation and specific applications like train control.

Bluetooth is also a wireless short range protocol defined by the Bluetooth Special Interest Group. With Bluetooth 4.0 they have included a low energy protocol variant for low power applications.

RFID is not only used in the WSN context, but is of general interest to IoT. ISO/IEC JTC 1/SC 31

is one of the major standardization drivers with its ISO/IEC 18000 series of standards defining diverse RFID technologies. Other bodies like ISO, EPCglobal and DASH7 have either contributed to or used these standards.

While the lower communication layers are often specific for a certain application approach like WSN, the network and higher communication layer should preferably use common protocols in order to allow interoperability across networks. Still specific requirements of certain technologies, such as low power consumption and small computational footprints in the case of WSNs, have to be taken into account. The IP protocol suite is today the *de facto* standard for these layers. While previously domain specific standards have defined their own protocol stack they all move today to IP. In the case of WSN and IoT IPv6 is the preferred solution. The IPv6 standards set (network to application layer) from Internet Engineering Task Force (IETF) (RFC 2460 and others) is available and stable. In order to support low power constrained devices and networks, especially considering IEEE 802.15.4, IETF is working on specific extensions and protocols. The 6LoWPAN working group defines the mapping of IPv6 on IEEE 802.15.4 (e.g. RFC 6282). The roll working group considers routing over low power and lossy networks (e.g. RFC 6550). The constrained application protocol (CoAP) working group defines an application protocol for constrained devices and networks. This is an alternative to the HTTP protocol used for RESTful web services taking into account the specially requirements of constrained devices and networks.

The ZigBee® specifications enhance the IEEE 802.15.4 standard by adding network and security layers and an application framework. They cover various application areas like home and building automation, health care, energy and light management and telecom services. The original Zigbee® specifications define their own network and application layer protocols, while the latest Zigbee® IP specification builds on IPv6 and CoAP.

For the actual data exchange between applications various approaches exist, often using a service oriented architecture (SOA). Examples are OPC-UA which is an IEC standard and SOAP, WSDL and REST defined by World Wide Web Consortium (W3C). XML as defined by W3C is the commonly used encoding format. In the context of WSN it has to be considered how far these protocols fit to constrained devices and networks. The Open Geospatial Consortium (OGC) has defined a set of open standards for integration, interoperability and exploitation of web-connected sensors and sensor-based systems (sensor web enablement).

For the management of devices and networks the SNMP protocol defined by IETF is widely used. NETCONF is a new approach for network management in IETF. Currently activities have started to cover management of constrained devices and networks explicitly in IETF. Other devices management protocols considered for IoT are TR-69 from Broadband Forum (BBF) and Open Mobile Alliance (OMA) Device Management.

Semantic representation of the information is an important issue in WSN and IoT in order to ease knowledge sharing and auto-configuration of systems and applications. W3C is defining the base protocols like RDF, RDFS and OWL in its semantic web activities. Again the specific requirements of constrained networks and devices have to be taken into account. Furthermore semantic sensor network ontology has been defined. For querying geographically distributed information OGC has defined GeoSPARQL.

The European Telecommunications Standards Institute (ETSI) TC SmartM2M has started from use cases and requirements for several application areas to develop M2M communication architecture and the related interfaces between devices, gateways, network notes and applications with a focus on offering M2M services. This work is introduced into OneM2M.

ISO/IEC JTC 1/SWG 7 (sensor networks) has developed the ISO/IEC 29182 services for a sensor

network reference architecture and services and interfaces for collaborative information processing. They are working on sensor network interfaces for generic applications and smart grid systems. ISO/IEC JTC 1/SWG 7 (IoT) was started analysis market requirements and standardization gaps for IoT.

ITU has setup a M2M focus group to study the IoT standardization landscape and identify common requirements. Its initial focus is on the health sector. A joint coordination activity (JCA-IoT) shall coordinate the ITU-T work on IoT, including network aspects of identification functionality and ubiquitous sensor networks (USNs). In addition ITU has varies more or less related activities for example on next generation networks including USN, security and identification (naming and numbering).

IEEE has in addition to the 802.15.4 also activities on smart transducers (1451 series) and for ubiquitous green community control (1888 series).

Information models, sometimes with semantic representation and even ontology are already available for different application areas like for smart grid from IEC TC 57, industry automation from IEC TC 65 and ISO TC 184 and building automation from ISO TC 205 and ISO/IEC JTC 1/SC 25.

Important in the IoT context are also product data standards as defined for example by IEC SC 3D, identification standards as defined by ISO and ITU and location standards as defined for example by ISO/IEC JTC 1/SC 31 and OGC.

And last but not least security and privacy standards are important for WSN and IoT.

Table 6-1 | WSN/IoT standardization activities (not exhaustive)

Organization	Group	Relationship with WSN/IoT	Standards	Ongoing work
IEEE	802	Physical and link layer protocol for short range wireless network	802.15.4-2011 (including amendments a, c and d), 802.15.4e-2012, 802.15.4f.2012, 802.15.4g-2012, 802.15.4k-2013, 802.15.4j-2013	TV white space, rail communication
IETF		IP protocol suite (network to application layer)	e.g. RFC 2460 (IPv6), RFC 2616 (HTTP), RFC 768 (UDP), 1180 (TCP), RFC 5246 (TLS), RFC 4301 (IPsec)	

Organization	Group	Relationship with WSN/IoT	Standards	Ongoing work
IETF	roll	Routing for low power and lossy networks	RFC 5548, RFC 5673, RFC 5826, RFC 5867, RFC 6206, RFC 6550, RFC 6551, RFC 6552, RFC 6719, RFC 6997, RFC 6998	Multicast routing, security threats, applicability statements for different applications
IETF	core	Application protocol for constrained devices/networks	RFC 6690, draft-ietf-core-coap-18 (waiting for publishing as RFC)	Group communication, HTTP mapping, resources, device management
IETF	6LoWPAN	IPv6 mapping for constrained wireless networks (i.e. IEEE 802.15.4)	RFC 4919, RFC 4944, RFC 6282, RFC 6568, RFC 6606, RFC 6775	IPsec header compression, DECT low power mapping
Zigbee® Alliance			2007 Specification, IP Specification, RF4CE Specification, Building Automation, Remote Control, Smart Energy, Smart Energy Profile 2, Health Care, Home Automation, Light Link, Telecom Services, Gateway	Retail services
ISO/IEC JTC 1	SC 31	RFID, NFC	ISO/IEC 14443, ISO/IEC 15693, ISO/IEC 15961, ISO/IEC 15962, ISO/IEC 18000, ISO/IEC 18092, ISO/IEC 21481, ISO/IEC 24791, ISO/IEC 29160	

Organization	Group	Relationship with WSN/IoT	Standards	Ongoing work
EPCglobal		RFID (Electronic Product Code)	EPCglobal Tag Data, Tag Data Translation, EPCglobal HF air interface protocol, EPCglobal UHF "Gen2" air interface protocol, EPC Information Services (EPCIS)	
ISO	TC 104	RFID (container tracking)	ISO18185	
DASH7		RFID	ISO/IEC 18000-7	DASH7 Alliance Protocol
W3C		Application communication, Web Services	XML, SOAP, WSDL, REST	
IEC	TC 65	Application communication	IEC 62541 (OPC-UA)	
IETF	opsawg	Device and network management	RFC 1155, RFC 1157, RFC1213, RFC3411-3418 (SNMPv3)	Management for constrained devices
IETF	netconf	Device and network management	RFC 4741-4744	Security
BBF	BroadbandHome	Device management	TR-69	
OMA	DM WG	Device management	DM 1.3	Version 2.0, constrained devices (Lightweight DM)
W3C		Semantic representation	RDF, RDFS, RIF, OWL, SPARQL, EXI, SSN ontology	Binary RDF, Object Memory Modeling (OMM), RDF stream processing

Organization	Group	Relationship with WSN/IoT	Standards	Ongoing work
OGC	Sensor Web Enablement DWG	Application communication, web services	Overview and High Level Architecture, Application communication, Web Services, Sensor Model Language, Transducer Model Language, Sensor Observations Service, Sensor Planning Service, Sensor Alert Service, Web Notification Services	
OGC	GeoSPARQL SWG	Semantic representation	GeoSPARQL	
ETSI (OneM2M)	TC SmartM2M	M2M communication, architecture, use cases, requirements, interfaces	TS 102689, TS 102690, TS 102921, TS 103092, TS 103093, TS 103104, TR 101584, TR 102691, TR 102725, TR 102732, TR 102857, TR 102898, TR 102935, TR 103167	Interworking, security, smart cities, smart appliances, semantics
ISO/IEC JTC 1	SWG 7	Sensor network, architecture, application interfaces	ISO/IEC 29182, ISO/IEC 20005	Smart grid interfaces (ISO/IEC 30101), generic application interfaces (ISO/IEC 30128)

Organization	Group	Relationship with WSN/IoT	Standards	Ongoing work
ITU-T	Focus Group M2M	M2M architecture, requirements, application interfaces, e-health		Requirements, architecture framework, APIs, protocols, e-health Standardization activities and gap analysis, e-health M2M eco system, e-health use cases
ISA		Physical and link layer protocol for short range wireless network	ISA100.11.a	
IEEE	P1451	Smart transducers	IEEE 1451 (ISO/IEC/IEEE 21451)	
IEEE	P1888	Community control	IEEE 1888	
ITU-T	SG16	Ubiquitous sensor network middleware, applications, identification	F.771, F.744, H.621, H.642	IoT applications, tag-based identification
IEC	TC 57	Information models, smart grid	IEC 61850, IEC 61968, IEC 61970	Web services mapping, renewable integration, customer interface, market interface
IEC	TC 65	Information models, industry automation	IEC 6242, IEC 62714, IEC 62794,	
ISO	TC 184	Information models, industry automation	ISO 13584, ISO 15926	

Organization	Group	Relationship with WSN/IoT	Standards	Ongoing work
ISO/IEC JTC 1	SC 25	Information models, building automation	ISO/IEC 14543	
ISO	TC 205	Information models, building automation	ISO 16484	
IEC	SC 3D	Product data	IEC 61360	
ISO	TC 184	Product data	ISO 13584	
ecl@ss		Product data	ecl@ss 7.0	
IEC	TC 65	Wireless sensor network	IEC 62591, IEC 62601, IEC 62734	
ISO	TC 46	Identifiers	ISO 27729, ISO 26324, ISO 3297, ISO 2108, ISO 10957	
ISO/IEC JTC 1	SC 31	Location	ISO/IEC 24730, ISO/IEC 24769	
ISO/IEC JTC 1	SC 31	Identifiers	ISO/IEC 15459	
ITU-T	SG2	Identifiers	E.101, Y.2213	
ITU-T	SG13	Ubiquitous sensor network	Y. 2221	
ITU-T	SG17	Security	X.1171, X.1311, X.1312, X.1313	
OGC	SWE	Location	OpenGIS location services	
3GPP	SA1, SA2, SA3	Service and system		MTC optimization, MTC communication
3GPP	G2, R1, R2, R3	Radio access networks		Enhancement tech. of wireless access MTC

Organization	Group	Relationship with WSN/IoT	Standards	Ongoing work
3GPP	CT1, CT3l, CT4	Communication networks		Evaluate the influence of 3GPP protocols
3GPP2	TSG-SX	M2M communication		Study for M2M communication for CDMA2000 networks
CCSA	TC10/WG3	M2M communication		M2M communication, next generation network
CCSA	TC5/WG7	Typical M2M application		
ITU-T	JCA-NID	Identification system		Network character of identification system (including RFID)

6.3 Standardization needs and outlook

WSN and even more IoT are not single technologies, but represent complex systems using various technologies from physical communication layers to application programmes. Furthermore, they are used in many application areas and different environments. This can also result in a complex standardization environment. As discussed above we have already a large set of existing standards and ongoing standardization activities. However they often cover only certain aspects and application areas of the overall system or focus on specific use cases.

As IoT and WSN are base technology areas for ongoing and emerging standardization areas by the IEC like smart grid, industry 4.0 and smart cities, it is important for IEC to have a good understanding of them, the standardization environment and the specific needs for the IEC applications areas in order to steer standardization in the necessary direction and identify and fill the standardization gaps. This has to be done in close cooperation with other relevant standardization bodies.

Starting from the use cases of the specific application areas (i.e. smart grid, industry 4.0, smart cities) the requirements and an architectural framework have to be defined that fit the needs of IEC. Based on that it can be identified which existing standards can be reused and which gaps have to be filled.

6.4 Challenges and future standardization needs

WSN is an emerging technology which involves different layers and aspects of information technology. So its standardization has its unique complexity:

§ Disunity: communication, coordination and unified planning are absent from different standard organizations and between each other.

§ Incompatibility: since WSN involves different aspects of information technology, its standards are complex and diverse. Yet different standards developed by different standard organizations are not compatible.

§ Lack of harmonization: some WSN applications have already begun to implement successively. Though different standard organizations have carried out the work from different perspective and with different depth, most of the work is still in its initial stage and is not market ready.

§ Divergence: since the applications are out of sync and the standard development is delayed, the application constructions are not in conformity with standard development, which affects the reusability and intercommunity of the applications and impede the development of industrialization.

To resolve the above problems, it is recommended that WSN standardization should enhance the communication and coordination among different standard organizations, make unified planning, optimize resource allocation and reduce repetition of work.

Section 7

Conclusions and recommendations

WSN and even more so, IoT, are not single technologies but instead represent complex systems using various technologies from physical communication layers to application programmes and are used in many application areas and different environments. This diversity has resulted in a complex standardization environment. As discussed in this White Paper there is already a large set of existing applications, challenges and ongoing standardization activities for WSNs. This can create opportunities for industry, research organizations and standardization bodies due to the unique characteristics of WSNs. This makes them attractive in current and future infrastructure applications.

As IoT and WSN are based on technology areas strongly covered by the IEC, like smart grid, industry 4.0 and smart cities, it is important for the IEC to have a good understanding of the applications, the standardization environment, and the specific needs of WSN for the IEC stakeholders. In order to steer standardization in the right direction, and to identify and fill the standardization gaps, close cooperation within and outside the IEC (i.e. other relevant standardization bodies) is required.

7.1 General recommendations

7.1.1 Large-scale WSNs

As the number of nodes in large-scale WSNs increase, the density of the network is also increased and the possibility of link failure becomes more frequent. The IEC recommends that further research should consider other network performance criteria such as the quality of service (QoS) issues for the real-time applications, and node mobility in some special environments.

7.1.2 Research on system architecture and integration technology suitable for ultra-large sensing and dynamic changes

The IEC recommends that industry and research institutes develop systems architecture and integration technology for WSN. The system architecture based on Service Oriented Architecture Protocol (SOAP) combined with integration technology, e.g. OPC-UA, semantic representation and processing, is needed in order to realize free exchange of information in a variety of heterogeneous network environments.

7.1.3 Develop common model to ensure security

Because more and more nodes are deployed, and performance is generally impacted with the addition of security services in WSNs, especially in infrastructure, the IEC recommends relative research organizations to combine their efforts to develop a common model to ensure security for each layer, and to make the layers work in collaboration with each other.

7.1.4 High-concurrent access technology of WSNs

The IEC recommends significant effort to be put into developing and operating with the high-concurrent access technology in addition to current access technologies, despite their novelty in the historical context. The high-concurrent access technology

can further improve the efficiency of scarce wireless spectrum, and support larger networks.

7.2 Recommendations addressed to the IEC and its committees

7.2.1 Basic standards needed that are suitable for architecture of WSNs

The MSB recommends the SMB to develop relative standards for a unified architecture of WSNs. Starting from the use cases of the specific application areas that fit the needs of IEC (i.e. smart grid, industry 4.0, smart cities), the requirements and an architectural framework need to be defined. Based on the analysis, only then can we identify which existing standards can be reused and which gaps have to be filled.

7.2.2 Technical contribution to the WSN for factory automation

The MSB recommends the SMB to take an active part in the development of WSNs for factory automation with high-concurrent access requirements. IEC TC 65 is positioned in this field.

7.2.3 Rapid progress in WSN standards for factory automation

The MSB recommends the SMB to implement the WSN standards for factory automation, paying particular attention to the harmonization of already existing national or regional standards.

7.2.4 Synergy with industry associations on WSNs for factory automation

The MSB recommends the SMB to encourage TCs to follow WSN developments at the global industry level. Many industry associations are active in this area and produce studies and position papers which contribute certain views of the problems. Standardization efforts should take account of these efforts.

7.2.5 Systems certification standards

The MSB recommends the CAB to consider future standardization needs to promote and support modular certification for WSNs. Since complex systems usually come with very complex system behaviours, certification of large-scale systems is anything but straightforward. However, modular systems come with the promise of modular certification. In such a system, most of the certification process focuses on individual system modules, and only a minor, remaining certification is conducted on the integrated system itself. In other words, the system “inherits” the certification of its modules.

Annex A

Access technologies

A.1 Developing trend of access technologies

According to the current specific requirements for WSN applications, the development of access technology has already made significant progresses. The representative access technologies that are more systematic and remarkable are Bluetooth 4.0 oriented towards medical WSN, IEEE 802.15.4e oriented towards industrial WSN, and WLAN IEEE 802.11™ in the view of IoT.

A.1.1 Bluetooth 4.0

Considering the characteristics and requirements of medical and some other IoT applications, especially the requirements of low power, Bluetooth SIG published the latest Bluetooth standard of Bluetooth 4.0 in 2012.

Oriented towards the highly integrated and compacted devices, Bluetooth 4.0 adopts a lightweight access technology to provide ultra-low-power standby mode operation, which ensures extremely low power consumption in both operating and standby modes. Even a button battery can support the uninterruptible work of a Bluetooth 4.0 device for several years. The following table compares the parameters of Bluetooth 4.0 and traditional Bluetooth technology.

Table A-1 | Comparisons between Bluetooth 4.0 and traditional Bluetooth technology [54]

Technical specification	Classic Bluetooth technology	Bluetooth low energy technology
Distance/Range	100 m (330 ft)	50 m (160 ft)
Over the air data rate	1 Mbit/s to 3 Mbit/s	1 Mbit/s
Application throughput	0.7 Mbit/s to 2.1 Mbit/s	0.27 Mbit/s
Active slaves	7	Not defined; implementation dependent
Security	56/128-bit and application layer user defined	128-bit AES with Counter Mode CBC-MAC and application layer user defined
Robustness	Adaptive fast frequency hopping, FEC, fast ACK	Adaptive frequency hopping, Lazy Acknowledgement, 24-bit CRC, 32-bit Message Integrity Check

Latency (from a non-connected state)	Typically 100 ms	6 ms
Total time to send data (detect battery life)	100 ms	3 ms, <3 ms
Voice capable	Yes	No
Network topology	Scatternet	Star-bus
Power consumption	1 as the reference	0.01 to 0.5 (depending on use case)
Peak current consumption	<30 mA	<15 mA

A.1.2 IEEE 802.15.4e

The characteristic of WSN is quite similar to the low-speed WPAN, and thus most WSNs take IEEE 802.15.4 as the underlying communication standard. Moreover, ZigBee® [55], WirelessHART [56], ISA100.11a [57] and WIA-PA [58] are all built upon on the standard of IEEE 802.15.4. Therefore, for the high reliability, hard real-time requirements of industrial IoT applications, IEEE 802.15.4 working group put forward IEEE 802.15.4e in 2012.

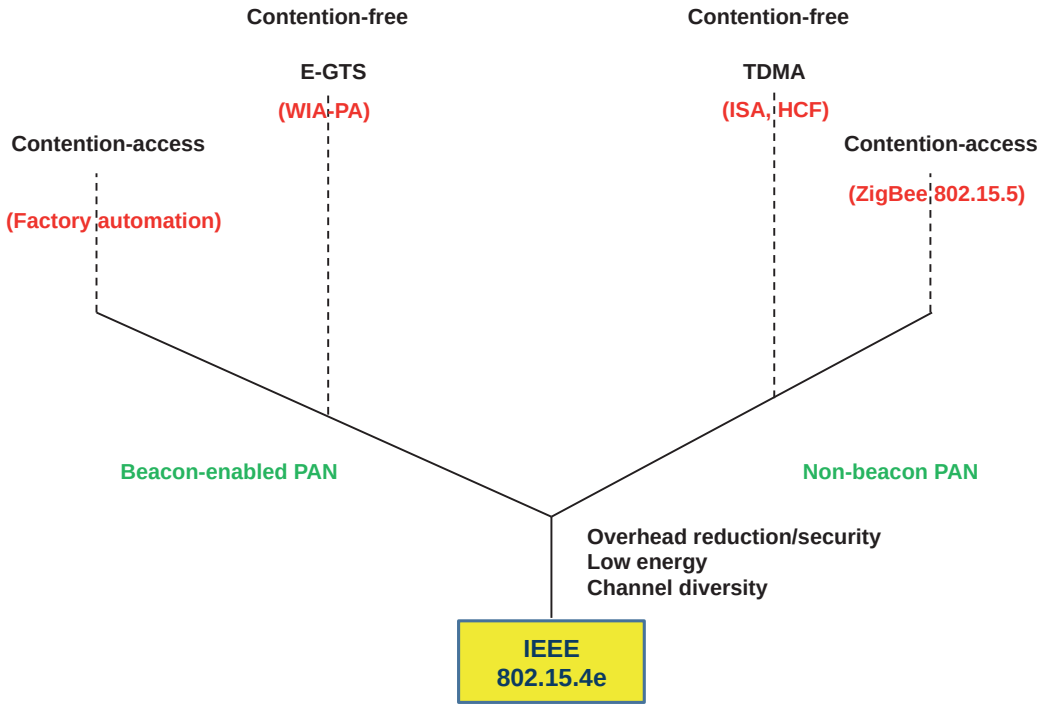


Figure A1-1 | Access technology architecture of IEEE 802.15.4e [59]

Oriented towards industrial applications, IEEE 802.15.4e extends IEEE 802.15.4 by having four access methods, including non-competitive expansion GTS method based on Beacon supporting the process automation-oriented WIA-PA, non-beacon non-competitive TDMA method supporting the process automation-oriented WirelessHART and ISA100.11a, competitive access based on Beacon method supporting factory automation applications, and Non-beacon competitive access method supporting Zigbee® and IEEE 802.15.5 [60].

A.1.3 WLAN IEEE 802.11™

The main advantages of WLAN IEEE 802.11™ in the view of IoT are

- § the easy integration of WLAN clients and devices into the internet,
- § its broad acceptance as wireless communication technology in offices, homes, and industry,
- § its support of mobile devices, and
- § low power consumption levels acceptable for industrial applications and sensor networks.

Wireless LANs based on the standard IEEE 802.11™ [17] are the favourite choice for wireless data communication in offices, at conferences and meetings, in homes, but also in industrial wireless communication. WLAN IEEE 802.11 networks provide an easy integration into the internet through its network-oriented, ethernet-like specification and through their stable, commercially successful and widely deployed eco system.

The predominant network topologies for IEEE 802.11™ WLANs are mobile WLAN clients connected to access points of the WLAN network.

Figure A1-2 | GainSpan GS1011M low-power Wi-Fi module [61]

Other network topologies are also possible, especially wireless mesh networks (IEEE 802.11s [62]) WLAN IEEE 802.11™ which provides data rates of 56 Mb/s with IEEE 802.11a/g, of 150 Mb/s and more with IEEE 802.11n, and of up to 1 Gb/s with IEEE 802.11ac.

Moreover, WLANs are also reaching into industrial wireless communication and sensor networks. Companies such as GainSpan offer so-called low-power Wi-Fi clients (see Figure A1-2). The low power consumption is achieved by energy-efficient hardware and a consequent usage of power save capabilities of the IEEE 802.11™ specification. A certification through the Wi-Fi Alliance is planned. More amendments to IEEE 802.11™ that are relevant to IoT and WSNs are underway. For instance, additional PHY layers for the sub-GHz band in IEEE 802.11ah and for the 60 GHz band in IEEE 802.11ad/aj.

References

[1] ASHTON, K. *That 'Internet of Things' Thing. In the real world, things matter more than ideas*. RFID Journal, 22 June 2009. Available from: http://www.rfidjournal.com/articles/view?4986

[2] BRÖRING, A. et al. *New generation sensor web enablement*. Sensors, 11, 2011, pp. 26522699. ISSN 1424-8220. Available from: doi:10.3390/s110302652

[3] SENSEI. *Integrating the physical with the digital world of the network of the future*. Available from: http://www.sensei-project.eu/

[4] CHONG, C.-Y. and KUMAR, S. P. *Sensor networks: Evolution, opportunities, and challenges*. Proceedings of the IEEE 91(8), 2003, pp. 1247-1256.

[5] KUMAR, S. and SHEPHERD, D. *Sensit: Sensor information technology for the warfighter*. Proceedings of the 4th International Conference on Information Fusion (FUSION'01), 2001, pp. 3-9.

[6] COY, P. and GROSS, N. et al. *21 Ideas for the 21st Century*. Business Week Online, 1999, pp. 78-167. Available from: http://www.businessweek.com/1999/99_35/2121_content.htm

[7] NI, L.M. *China's national research project on wireless sensor networks*. Proceedings of the 2008 IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC'08), 2008, p. 19.

[8] HATLER, M., GURGANIOUS, D. and CHI, C. *Industrial wireless sensor networks. A market dynamics report*. ON World, 2012.

[9] Figure courtesy of Silicon Labs and RTC Magazine: http://rtcmagazine.com/files/images/4151/RTC1212_SilLabs_fig1_medium.jpg

[10] Yole Development SA. *MEMS technology: World's smallest barometric pressure sensor*. Micro News, 2009,78:1.

[11] KAHN, J. M., KATZ, R. H. and PISTER, K. S. J. *Mobile Networking for Smart Dust*. ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom 99), Seattle, WA, August 17-19, 1999.

[12] ANG, R.J., TAN, Y.K. and PANDA, S.K. *Energy harvesting for autonomous wind sensor in remote area*. 33rd Annual IEEE Conference of Industrial Electronics Society (IECON'07), Taipei, Taiwan, 2007.

[13] TANG, L. and GUY C. *Radio frequency energy harvesting in wireless sensor networks*. International conference on communications and mobile computing, 2009, pp. 644648.

[14] Courtesy of Shenyang Institute of Automation, Shenyang, China, 2014.

[15] FP7 EXALTED consortium, *D3.3 – Final report on LTE-M algorithms and procedures*, project report, July 2012. Available from: http://www.ict-exalted.eu/fileadmin/documents/EXALTED_WP3_D3.3_v1.0.pdf

[16] IEEE 802.15.4e-2012, *IEEE Standard for local and metropolitan area networks – Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs) Amendment 1: MAC sublayer*.

[17] IEEE Std 802.11™-2012, *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, IEEE Computer Society, March 2012.

[18] UIMER, C. *Wireless Sensor Networks*. Georgia Institute of Technology, 2000. Available from: www.craigulmer.com/portfolio/unlocked/000919_sensorsimii/wireless_sensor_networks.ppt

[19] PISTER, K. and DOHERTY, L. *TSMP: Time synchronized mesh protocol*. [C]. Proceedings of the IASTED International Symposium, Distributed Sensor Networks (DSN 2008), 2008, pp. 391398. Available from: http://robotics.eecs.berkeley.edu/~pister/publications/2008/TSMP%20DSN08.pdf

[20] SHELBY, Z. and BORMANN C. *6LoWPAN: The wireless embedded Internet*. New York, NY, USA: John Wiley & Sons Ltd, 2009. Available from: http://elektro.upi.edu/pustaka.elektro/Wireless%20Sensor%20Network/6LoWPAN.pdf

[21] Sensinode. Available from: www.sensinode.com\\EN\\products\\software.html

[22] *6LoWPAN Sub1GHz Evaluation kit*. Texas Instruments. Available from: www.ti.com/tool/CC-6lOWPAN-DK-868

[23] HUI, J., CULLER, D. and CHAKRABARTI, S. *6LoWPAN: Incorporating IEEE 802.15.4 into IP architecture*. IPSO, Industrial Ethernet Book Issue 59, 1997. Available from: http://www.iebmedia.com/index.php?id=7176&parentid=63&themeid=255&hft=59&showdetail=true&bb=1&PHPSESSID=a3tc6d9vhs5ab6svu8ahcb4c10

[24] BLILAT, A., BOUAYAD, A., CHAOUI, N. and EL GHAZI, M. *Wireless sensor network: Security challenges*. Network Security and Systems (JNS2), 2012 National Days of. IEEE, 2012, pp. 6872. Available from: http://novintarjome.com/wp-content/uploads/2014/05/Wireless-Sensor-Network.pdf

[25] JAIN, A., KANT, K. and TRIPATHY, M. R. *Security solutions for wireless sensor networks*[C]. Proceedings of the 2012 Second International Conference on Advanced Computing and Communication Technologies (ACCT '12). IEEE Computer Society, 2012, pp. 430433.

[26] WANG, Y., ATTEBURY, G. and RAMAMURTHY, B. *A survey of security issues in wireless sensor networks* IEEE Communications Surveys and Tutorials 8, 2006, pp. 223.

[27] ALZAID, H. *Security map for WSN*. 2009. Available from:http://www.wsn-security.info/Security_Map.htm

[28] MARTIN, T., HSIAO, M., HA, D. and KRISHNASWAMI, J. *Denial-of-service attacks on battery-powered mobile computers*. Second IEEE International Conference on Pervasive Computing and Communications (PerCom'04), IEEE, 2004, pp. 309318. Available from: http://www.ece.vt.edu/tlmartin/power-secure/percom_martin_camera-final.pdf

[29] FALK, R. and HOF, H.-J. *Fighting insomnia, a secure wake-up scheme for wireless sensor networks*. Third International Conference on Emerging Security Information, Systems and Technologies (SECURWARE'09), Athens/Glyfada, Greece, 18-23 June 2009, pp. 191196.

[30] LE X. H., SANKAR, R., KHALID, M., and SUNGYOUNG, L. *Public key cryptography-based security scheme for wireless sensor networks in healthcare*. Proceedings of the 4th International Conference on Ubiquitous Information Management and Communication (ICUIMC '10). ACM, 2010.

[31] SZCZECHOWIAK, P., KARGL, A., COLLIER, M. and SCOTT, M. *On the application of pairing based cryptography to wireless sensor networks*. Proceedings of the second ACM conference on Wireless network security. ACM, 2009: 1-12.

[32] Libelium, *Encryption libraries for waspmote sensor networks*. Available from: http://www.libelium.com/products/waspmote/encryption/

[33] KALITA, H. K. and KAR, A. *Key management in secure self-organized wireless sensor network: a new approach*. Proceedings of the International Conference and Workshop on Emerging Trends in Technology (ICWET '11). ACM, 2011, pp. 865870.

[34] FALK, R. and HOF, H.-J. *Security design for industrial sensor networks*. Information Technology, Vol. 52, No. 6, Oldenbourg, 2010, pp. 331-339.

[35] AL-KARAKI, J. N. and KAMAL, A. E. *Routing techniques in wireless sensor networks: a survey*. Wireless communications, IEEE, Vol. 11, No. 6, 2004, pp. 628.

[36] WOOD, A. D., FANG, L. and STANKOVIC, J. A. *SIGF: a family of configurable, secure routing protocols for wireless sensor networks*. Proceedings of the fourth ACM workshop on Security of ad hoc and sensor networks. ACM, 2006: 35-48.

[37] SEN, J. *A survey on wireless sensor network security*. International Journal of Communication Networks and Information Security (IJCNIS), Vol. 1, No. 2, 2009, pp. 5578. Available from: http://arxiv.org/ftp/arxiv/papers/1011/1011.1529.pdf

[38] JHA, M. K. and SHARMA, T. P. *Secure data aggregation in wireless sensor network: a survey*. International Journal of Engineering Science and Technology (IJEST), Vol. 5, No. 3, 2011.

[39] SCHMITT, C. *Cooperation between all components in the established wireless sensor network*. Technische Universität München, 2009. Available from: https://corinna-schmitt.de/doku.php?id=wsn_research

[40] ROZANSKI, N. and WOODS, E. *Software systems architecture: Working with stakeholders using viewpoints and perspectives.* Addison-Wesley Professional, 2nd edition, 2011.

[41] DUNLAP, J. *From billing & technology convergence to ecosystem convergence: Why M2M matters to your business*. Pipeline: Technology for Service Providers, Vol. 8, No. 7, 2011, pp. 13. Available from: http://pipelinepub.com/1211/OSS_BSS/pdf/7230_PipelineDecember2011_A5.pdf

[42] FELDMAN, S. *Unified information access: Creating information synergy*. IDC, 2012. Available from: http://www.infonortics.com/sdv-12-post/feldman.pdf

[43] MYRDA, P. T. and KOELLNER, K. *NASPInet-The internet for synchrophasors*. 43rd Hawaii International Conference on System Sciences (HICSS), IEEE, 2010, pp. 16.

[44] HEBELER, J. et al. *Semantic Web Programming*. John Wiley & Sons, Inc., 2009.

[45] WOOD A. D. and J.A. Stankovic. 2002. "Denial of Service in Sensor Networks." IEEE Computer,35 (10), 54-62.

[46] PATHAN, A. S. K., LEE, H. W. and HONG, C. S. *Security in wireless sensor networks: issues and challenges*. The 8th International Conference on Advanced Communication Technology (ICACT 2006). IEEE, 2006, Vol. 2, 6 pp.-1048. Available from: http://arxiv.org/ftp/arxiv/papers/0712/0712.4169.pdf

[47] Courtesy of State Grid Corporation of China, 2014.

[48] Courtesy of SAP.

[49] *Industry group leader report*, “Sustainability Scores”. RobecoSAM AG, 2013. Available from: http://www.sustainability-indices.com/images/Industry_Group_Leader_DJSI2014_Wipro-Ltd.pdf

[50] Courtesy of Schneider Electric.

[51] http://www2.schneider-electric.com/sites/corporate/en/press/press-kit/homes-project.page

[52] Courtesy of IMS Research.

[53] ZigBee 2012, *ZigBee specification overview*. Available from: http://www.zigbee.org/Specifications/ZigBee/GreenPower.aspx

[54] Bluetooth Low Energy. Wikipedia: The Free Encyclopedia. 31 July 2014 at 05:16. Available from: http://en.wikipedia.org/wiki/Bluetooth_low_energy

[55] ZigBee Alliance. http://zigbee.org/Home.aspx

[56] IEC 62591, *Industrial communication networks Wireless communication network and communication profiles WirelessHART™*.

[57] IEC/PAS 62734, *Industrial communication networks – Fieldbus specifications – Wireless systems for industrial automation: process control and related applications.*

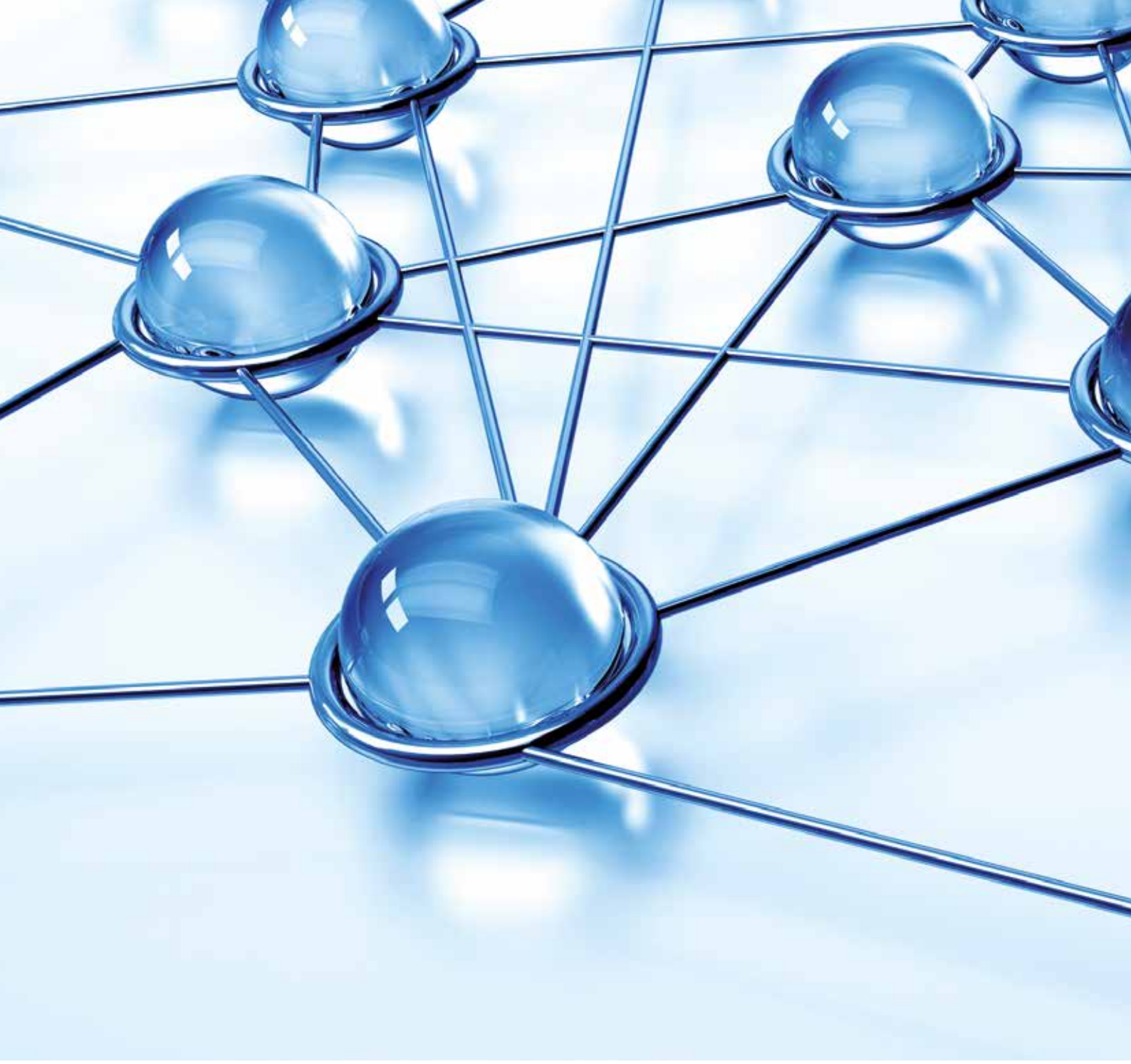
[58] IEC 62601, *Industrial communication networks – Fieldbus specifications – WIA-PA communication network and communication profile.*

[59] IEEE Std 802.15.4e-2012, *Local and metropolitan area networks – Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs) Amendment 1: MAC sublayer*. April 2012.

[60] IEEE P802.15 Working Group for Wireless Personal Area Networks (WPANs). IEEE 802.15.5 WPAN Mesh Networks. http://grouper.ieee.org/groups/802/15/pub/Meeting_Plan.html. May 2005.

[61] GainSpan, *Low Power Wi-Fi Modules and Embedded Software*, Product Photography, Available from: http://www.gainspan.com/news/media_kit

[62] IEEE Std 802.11s-2011, *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications, Amendment 10: Mesh Networking*, IEEE Computer Society, September 2011.



ISBN 978-2-8322-1834-1

CHF 50.-

International Electrotechnical Commission

3 rue de Varembé
PO Box 131
CH-1211 Geneva 20
Switzerland

T +41 22 919 0211
info@iec.ch
www.iec.ch

IEC WP IoT:WSN:2014-11(en)