Chapter 13
Internet of Things

Overview The connection of *physical things* to the Internet makes it possible to access remote sensor data and to control the physical world from a distance. The mash-up of captured data with data retrieved from other sources, e.g., with data that is contained in the Web, gives rise to new synergistic services that go beyond the services that can be provided by an isolated embedded system. The *Internet of Things* is based on this vision. A *smart object*, which is the building block of the Internet of Things, is just another name for an embedded system that is connected to the Internet. There is another technology that points in the same direction – the *RFID technology*. The RFID technology, an extension of the ubiquitous optical bar codes that are found on many every-day products, requires the attachment of a smart low-cost electronic ID-tag to a product such that the identity of a product can be decoded from a distance. By putting more intelligence into the ID tag, the *tagged thing* becomes a *smart object*. The novelty of the Internet-of-Things (IoT) is not in any new disruptive technology, but in the pervasive deployment of *smart objects*.

At the beginning of this chapter, the vision of the IoT is introduced. The next section elaborates on the forces that drive the development of the IoT. We distinguish between *technology push* and *technology pull* forces. The *technology push forces* see in the IoT the possibility of vast new markets for novel ICT products and services, while the *technology pull forces* see the potential of the IoT to increase the productivity in many sectors of the economy, to provide new services, e.g., for an aging society, and to promote a new lifestyle. Section 13.3 focuses on the technology issues that have to be addressed in order to bring the IoT to a mass market. Section 13.4 discusses the RFID technology, which can be seen as a forerunner of the IoT. The topic of wireless sensor networks, where *self-organizing smart objects* build ad-hoc networks and collect data from the environment, is covered in Sect. 13.5. The pervasive deployment of smart objects that collect data and control the physical environment from a distance poses a severe challenge to the security and safety of the world and the privacy of our lives.

H. Kopetz, *Real-Time Systems: Design Principles for Distributed Embedded Applications*, 307
Real-Time Systems Series, DOI 10.1007/978-1-4419-8237-7_13,

13.1 The Vision of an Internet-of-Things

Over the past 50 years, the Internet has exponentially grown from a small research network, comprising only a few nodes, to a worldwide pervasive network that services more than a billion users. The further miniaturization and cost reduction of electronic devices makes it possible to expand the Internet into a new dimension: to *smart objects*, i.e., everyday physical things that are enhanced by a small electronic device to provide local intelligence and connectivity to the cyberspace established by the Internet. The small electronic device, a *computational component* that is attached to a *physical thing,* bridges the gap between the physical world and the information world. A *smart object* is thus a *cyber-physical system* or an *embedded system*, consisting of a *thing* (the physical entity) and a *component* (the computer) that processes the sensor data and supports a wireless communication link to the Internet.

> **Example:** Consider a *smart refrigerator* that keeps track of the availability and expiry date of food items and autonomously places an order to the next grocery shop if the supply of a food item is below a given limit.

The novelty of the IoT is not in the functional capability of a *smart object* – already today many embedded systems are connected to the Internet – but in the expected size of billions or even trillions of *smart objects* that bring about novel technical and societal issues that are related to size. Some examples of these issues are: authentic identification of a *smart object*, autonomic management and self-organization of networks of smart objects, diagnostics and maintenance, context awareness and goal-oriented behavior, and intrusion of the privacy. Special attention must be given to *smart objects* that can act – more or less autonomously – in the physical world and can *physically* endanger people and their environment.

The advent of low-power wireless communication enables the communication with a *smart object* without the need of a physical connection. Mobile *smart objects* can move around in the physical space while maintaining their identity. The wide availability of signals from the global positioning system (GPS) makes it possible to make a smart object *location and time-aware* and offer services that are tuned to the current context of use.

We can envision an *autonomic smart* object that has access to a domain specific knowledge base – similar to the *conceptual landscape* introduced in Sect. 2.2 – and is empowered with reasoning capabilities to orient itself in the selected application domain. Based on the capability level of a smart object, [Kor10] distinguish between *activity aware*, *policy aware, and process* aware smart objects.

> **Example:** A *pay-per-use smart tool* is an activity aware smart object that collects data about the time and intensity of its use and transmits the data autonomously to the billing department. A *policy-aware smart tool* will know about its use cases and will ensure that it is not used outside the contracted use cases. A *process-aware smart tool* will reason about its environment and guide the user how to optimally apply the tool in the given scenario.

According to the IoT vision, a *smart planet* will evolve, where many of the everyday things around us have an identity in cyberspace, acquire intelligence, and mash-up information from diverse sources. On the *smart planet,* the world economy and support systems will operate more smoothly and efficiently. But the life of the average citizen will also be affected by changing the relation of power between those that have access to the acquired information and can control the information and those that do not.

13.2 Drivers for an IoT

Which are the forces that drive the development of the Internet of Things? They are on both sides of the technology landscape: *technology push forces* and *technology pull forces*. The technology push forces see in the IoT a vast new market for the deployment of current and future information and communication technologies (ICT). The IoT will help to utilize existing and new factories, provide new employment opportunities in the ICT sector, and contribute to the further development of the ICT technologies in general.

In this section, the focus is mainly on *technology pull forces*. Which areas of our economy, society, and life in general will benefit from the wide deployment of the IoT? The following analysis is not exhaustive – we are only highlighting some sectors where, according to our present understanding, the wide deployment of the IoT technology will have a major impact.

13.2.1 Uniformity of Access

The Internet has achieved the worldwide interoperability of heterogeneous end-systems over a wide variety of communication channels. The IoT should extend this interoperability to the universe of heterogeneous *smart objects*. From the point of view of reduction of the cognitive complexity (see Chap. 2), the IoT can make a very significant contribution: the establishment of a *uniform access pattern* to things in the physical world.

13.2.2 Logistics

The first commercial application of a forerunner of the IoT, the RFID (Radio Frequency Identification – see Sect. 13.4) technology, is in the area of logistics. With the decision of some major corporations to base their supply-chain management on RFID technology, the development of low-cost RFID tags and RFID

readers has moved forward significantly. There are many quantitative advantages in using RFID technology in supply-chain management: the movement of goods can be tracked in real-time, shelf space can be managed more effectively, inventory control is improved, and above all, the amount of human involvement in the supply chain management is reduced considerably.

13.2.3 Energy Savings

Already today, embedded systems contribute to energy savings in many different sectors of our economy and our life. The increased fuel efficiency of automotive engines, the improved energy-efficiency of household appliances, and the reduced loss in energy conversion are just some examples of the impact of this technology on energy savings. The low cost and wide distribution of IoT devices opens many new opportunities for energy savings: individual climate and lighting control in residential buildings, reduced energy loss in transmission by the installation of *smart grids*, and better coordination of energy supply and energy demand by the installation of smart meters. The *dematerialization of parts of our life* such as the replacement of physical meetings by virtual meetings and the delivery of information goods such as the daily paper, music, and videos by the Internet, lead to substantial energy savings.

13.2.4 Physical Security and Safety

A significant technology pull for the IoT technology comes from the domains of physical security and safety. Automated IoT based access control systems to buildings and homes and IoT-based surveillance of public places will enhance the overall physical security. Smart passports and IoT based identifications (e.g., a smart key to access a hotel room or a smart ski lift ticket) simplify admission controls checks and increase the physical security, while reducing human involvement in these checks. Car-to-car and car-to-infrastructure communication will alert the driver of dangerous traffic scenarios, such as an icy road or an accident, and reduce the number of accidents.

IoT technology can help to detect counterfeit goods and suspected unapproved spare parts that are becoming a safety risk in some application domains such as the airline or automotive industry.

On the other side, safety and security applications intrude into the privacy of our lives. It is up to policy makers to draw the fine line between the rights of a person to individual privacy and the desire of the public to live in a safe environment. It is up to the scientists and engineers to provide the technology so that the political decisions can be flawlessly implemented.

13.2.5 Industrial

In addition to streamlining the supply chain and the administration of goods by the application of RFID technology, the IoT can play a significant role in reducing maintenance and diagnostic cost. The computerized observation and monitoring of industrial equipment does not only reduce maintenance cost because an anomaly can be detected before it leads to a failure, but also improves the safety in the plant (see also Sect. 11.6).

A smart object can also monitor its own operation and call for preventive or spontaneous maintenance in case a part wears out or a physical fault is diagnosed. Automated fault-diagnosis and simple maintenance are absolutely essential prerequisites for the wide deployment of the IoT technology in the domain of ambient intelligence.

13.2.6 Medical

The wide deployment of IoT technology in the medical domain is anticipated. Health monitoring (heart rate, blood pressure, etc.) or precise control of drug delivery by a smart implant are just two potential applications. Body area networks that are part of the clothing can monitor the behavior of impaired persons and send out alarm messages if an emergency is developing. Smart labels on drugs can help a patient to take the right medication at the right time and enforce drug compliance.

Example: A heart pacemaker can transmit important data via a Bluetooth link to a mobile phone that is carried in the shirt pocket. The mobile phone can analyze the data and call a doctor in case an emergency develops.

13.2.7 Life Style

The IoT can lead to a change in life-style. A smart phone can function as a browser for smart objects and augment the reality we see with background information retrieved from a diversity of context dependant databases.

13.3 Technical Issues of the IoT

13.3.1 Internet Integration

Depending on the computational capabilities and the available energy, a smart object can be integrated into the Internet either directly or indirectly via a *base station* that is connected to the Internet. The indirect integration will be chosen

when the smart object has a very limited power budget. Application specific power-optimized protocols are used to connect the smart object to a near-by *base station*. The base station that is not power constrained can act as a standard web server that provides gateway access to the reachable smart objects.

> **Example:** In an RFID system, the RFID reader acts as a base station that can read the local RFID tags. The reader can be connected to the Internet. In *Sensor Networks*, one or more *base stations* collect data from the sensor nodes and forward the data to the Internet.

Recently, a number of major companies have formed an alliance to develop technical solutions and standards to enable the direct integration of low-power smart objects into the Internet. The Internet Engineering Task Force (IETF) has initiated a working group (named *6LowPan*) on *IPv6 over Low Power Wireless Area Networks* to find an energy-efficient solution for the integration of the IPv6 standard with the IEEE 802.15.4 wireless near field communication standard.

Guaranteeing the safety and information security of IoT-based systems is considered to be a difficult task. Many smart objects will be protected from general Internet access by a tight firewall to avoid that an adversary can acquire control of a smart object. The important topic of safety and security in the IoT is further addressed in the final section of this chapter.

13.3.2 Naming and Identification

The vision of the IoT (that all of the billions of smart objects can communicate via the Internet) requires a well-thought-out *naming architecture* in order to be able to identify a smart object and to establish an access path to the object.

Every name requires a *named context* where the name can be resolved. The recursive specification of naming context leads to a *hierarchical name structure* – the naming convention adhered to in the Internet. If we want a name to be universally interpretable without reference to a specific naming context, we need a single context with a universally accepted name space. This is the approach taken by the RFID community, which intends to assign an *Electronic Product Code (EPC)* to every physical smart object (see also Sect. 13.4.2). This is more ambitious than the forerunner, the optical bar code, which assigns a unique identifier only to a class of objects.

Isolated Objects. The following three different object names have to be distinguished when we refer to the simple case of an isolated object:

- *Unique object identifier (UID)* refers to the physical identity of a specific object. The Electronic Product Code (EPC) of the RFID community is such a UID.
- *Object type name* refers to a class of objects that ideally have the same properties. It is the name that is encoded in the well-established *optical bar code*.
- *Object role name*. In a given use context, an object plays a specific role that is denoted by the *object role name*. At different times, the same object can play

different roles. An object can play a number or roles and a role can be played by a number of objects.

Example: The assumption that all objects that have the same *object type name* are identical does not always hold. Consider the case of an *unapproved spare part* that has the same visible properties and is of the same type as an *approved spare part*, but is a *cheaper copy* of the approved part.

Example: An *office key* is an *object role name* for a physical object type that unlocks the door of an office. Any instance of the *object type* is an *office key*. When the lock in the office door is changed, a different object type assumes the role of the *office key*. A particular office key can also unlock the laboratory. It then plays two roles, the role of an *office key* and the role of a *laboratory key*. A *master key* can open any office – there are thus two different keys that play the same role.

Composite Objects. Whenever a number of objects are integrated to form a composite object, a *new whole*, i.e., new object is created that has an emerging identity that goes beyond the identities of the constituent objects. The composite object resembles a *new concept* (see Sect. 2.2.1) that requires a *new name*.

Example: *George Washington's axe* is the subject of a story of unknown origin in which the famous artifact is *still George Washington's axe* (a composite object) despite having had both its head replaced twice and its handle replaced three times [Wik10].

A composite object that provides an emergent service requires its own UID that is hardly related to the UIDs of its constituent parts. The different names, *UID*, *object type name*, and *object role name* must be introduced at the level of composite objects as well. Since a composite object can be an *atomic unit* at the next level of integration, the name space must be built up recursively.

Which one of the object names, introduced in the above paragraphs, should be the access points for the communication with the Internet? It will be difficult to manage the *communication complexity* if all objects that are contained in *multilevel composite objects* can be accessed *anytime* at *anyplace*.

It is evident that the introduction of a flat name space for all smart objects of the universe, as stipulated by the EPC is only a starting point. More research on the proper design of name-space architectures in the IoT is needed.

13.3.3 Near Field Communication

The IoT requires, in addition to the established WLANs (Wireless Local Area Networks), short-range energy-efficient WPANs (Wireless Personal Area Networks) in order to enable the energy-efficient wireless access to *smart objects* over a small distance. The IEEE 802.15 standard working group develops standards for WPAN networks. Among the networks that are conforming to the 802.15 standards are the *Bluetooth* network and the *ZigBEE* network.

Originally, *Bluetooth* has been introduced as a wireless alternative to the RS232 wire-bound communication channel [Bar07]. Bluetooth, standardized in IEEE

802.15.1, defines a complete WPAN architecture, including a security layer. At the physical level, it achieves a data rate of up to 3 Mbit/s over a distance of 1 m (Class 3 – maximum transmission power of 1 mW) to 100 m (Class 1 – maximum transmission power 100 mW) using the transmission technology of frequency *hopping*. Bluetooth allows multiple devices to communicate over a single adapter.

The *ZigBee* alliance is a group of companies that develops a secure WPAN that is intended to be simpler, more energy efficient, and less expensive than Bluetooth [Bar07]. *ZigBee* uses high-level communication protocols based on the IEEE 802.15.4 standard for low-power digital radios. ZigBee devices are requested to have a battery live of more than a year.

The NFC (Near Field Communication) standard [Fin03], an extension of the ISO/IEC 14443 proximity-card standard, is a short-range high frequency wireless communication technology which enables the exchange of data between devices over a distance of $<$20 cm. The technology is compatible with both existing smartcards and readers, as well as with other NFC devices, and is thereby compatible with the existing contactless infrastructure already in use for public transportation and payment. NFC is primarily aimed for use in mobile phones.

13.3.4 IoT Device Capabilities versus Cloud Computing

Smart objects that have access to the Internet can take advantage of services that are offered by the *cloud* (large data centers that provide their services through the Internet). The division of work between a smart object and the cloud will be determined, to a considerable degree, by privacy and energy considerations [Kum10]. If the energy required to execute a task locally is larger than the energy required to send the task parameters to a server in the cloud, then the task is a candidate for remote processing. However, there are other aspects that influence the decision about work distribution: autonomy of the smart object, response time, reliability, and security.

13.3.5 Autonomic Components

The large number of smart objects that are expected to populate our environment requires an autonomic system management without the need of frequent human interactions. This autonomic management must cover *network service discovery*, *system configuration and optimization*, *diagnosis of failures and recovery after failures*, and *system adaptation and evolution*. There is a need for a *multi-level autonomic management*, starting with the fine-grained management of components up to the coarse grained management of massive assemblies of components or large systems.

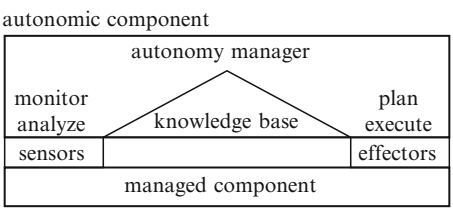

Fig. 13.1 Model of an autonomic component (Adapted from [Hue08])

Figure 13.1 shows the generic MAPE-K (Monitoring, Analyzing, Planning, Execution with a Knowledgebase) architecture of an *autonomic component* [Hue08]. An *autonomic component* consists of two *independent fault-containment units* (FCU), a *managed component* and an *autonomy manager*. The *managed component* can be a single component, a cluster of components, or a part of a larger system. The *autonomy manager* consists of a monitor that observes and analyzes information about the behavior of the managed component, a planning module that develops and evaluates alternative plans to achieve the stated goals, and finally an interface to the managed object that allows the autonomy manager to influence the behavior of the *managed component*. The autonomy manager maintains a *knowledge base* with static and dynamic entries. The *static entries* are provided *a priori*, i.e., at design time. They set up the goals, beliefs, and generic structure of the knowledge base, while the dynamic entries are filled in during operation to capture the acquired information about concrete situational parameters. The *multicast communication primitive* makes it possible for the autonomy manager to observe the behavior of the managed component and its interactions with the environment without any *probe effect*.

In its simplest form, the autonomy manager recognizes objects and object changes (events) and assigns them to known concepts (see Sect. 2.2.1). It then selects an action based on *event-condition-action* rules. If more than one action is applicable, it uses utility functions to select the action with the highest utility value for achieving the desired goals. In a more advanced form, the autonomy manager is based on a cognitive architecture that supports some form of advanced reasoning and can improve its decision by evaluating past decisions and by the incorporation of learning [Lan09].

13.4 RFID Technology

The easy and fast identification of *things* is required in many situations, e.g., in stores, warehouses, supermarkets etc. For this purpose, an optical barcode is attached to an object. Reading an optical barcode requires the careful positioning of the object by a human such that a direct line-of-sight between the barcode and the barcode reader is established.

13.4.1 Overview

In order to be able to automate the process of object identification and eliminate the human link, *electronic tags* (called RFID tags) that can be read from a small distance by an *RFID reader* have been developed. An RFID reader does not require a direct line-of-sight to the RFID tag. The RFID tag stores the unique Electronic Product Code (EPC) of the attached object. Since an RFID tag has to be attached to every object, the cost of an RFID tag is a major issue. Due to the standardization of the RFID technology by the International Standard Organization (ISO) and the massive deployment of RFID technology, the cost of an RFID tag has been reduced significantly over the last few years.

The RFID reader can act as a gateway to the Internet and transmit the object identity, together with the read-time and the object location (i.e., the location of the reader) to a remote computer system that manages a large database. It is thus possible to track objects in real-time.

Example: An *electronic ski pass* is an RFID tag that is queried by the reader that is built into the admission gate to a ski lift. Based on the object identifier, a picture of the person that owns the ski pass is displayed to the operator and the gate is opened automatically if the operator does not intervene.

13.4.2 The Electronic Product Code

Whereas an optical barcode denotes a product class (all boxes of the same product have the same barcode), the EPC of an RFID tag denotes an object instance (every box has a unique identifier). It is the intent of the EPC to assign a *unique identifier (UID)* to every identifiable *thing* on the globe, i.e., a unique name to each *smart object* of the IoT.

The EPC is managed by the international organization *EPC global*. In order to cope with the huge number of things the EPC must identify, the EPC contains a number of fields. A small header field determines the structure of the remaining fields. A typical EPC has a length of 96 bits and contains the following fields:

- Header (8 bits): defines the type and the length of all subsequent fields.
- EPC Manager (28 bits): specifies the entity (most often the manufacturer) that assigns the object class and serial number in the remaining two fields.
- Object Class (24 bits): specifies a class of objects (similar to the optical bar code).
- Object Identification Number (36 bits): contains the serial number within the object class.

The EPC is unique product identification, but does not reveal anything about the properties of the product. Two *things* that have the same properties, but are designed by two different manufacturers, will have completely different EPCs.

Normally, the unique EPC is used as a key to find the product record in a *product database*. The product record contains all required information about the attributes of the product.

13.4.3 RFID Tags

A RFID Tag contains as its most important data element the EPC of the associated *physical thing*. A number of different RFID tags have been developed and standardized. Basically, they fall into two main categories: *passive RFID tags* and *active RFID tags*.

Passive RFID Tags. Passive tags do not have their own power supply. They get the power needed for their operation from energy harvested out of the electric field that is beamed on them by the RFID reader. The energy required to operate a passive tag of the latest generation is below 30 μW and the cost of such a tag is below 5 ¢. Passive tags contain in addition to a standardized EPC (Electronic Product Code) as a unique identification number selected other information items about product attributes. Due to the low level of the available power and the cost pressure on the production of RFID tags, the communication protocols of passive RFID tags do not conform to the standard Internet protocols. Specially designed communication protocols between the RFID tag and the RFID reader that consider the constraints of passive RFID tags have been standardized by the ISO (e.g., ISO 18000-6C also known as the EPC global Gen 2) and are supported by a number of manufacturers. The parameters of a typical low-cost passive RFID tag are given in Table 13.1.

Active RFID Tags. Active tags have their own on-board power supply, e.g., a battery that gives them the capability to support many more services than passive tags. The lifetime of an active tag is limited by the lifetime of the battery, typically in the order of a year. Active tags can transmit and receive over a longer distance than passive tags, typically in the order of hundreds of meters, can have sensors to monitor their environment (e.g., temperature, pressure) and sometimes support standard Internet communication protocols. In some sense, an active RFID tag resembles a small embedded system. The ISO standard 18000-7 specifies

Table 13.1 Parameters of a typical low-cost passive RFID tag (Adapted from [Jue05])

Storage	128–512 bits of read-only storage
Memory	32–128 bits of volatile read-write memory
Gate count	1,000–10,000 gates
Operating frequency	868–956 MHz (UHF)
Clock cycles per read	10,000 clock cycles
Scanning range	3 m
Performance	100 read operations per second
Tag power source	Passively powered by reader via RF signal
Power consumption	10 μW

the protocol and the parameters for the communication with an active tag in the 433 MHz range. The reduction of the power consumption of an active RFID Tag in the *sleep* mode is a topic of current research.

13.4.4 RFID Readers

The RFID reader is a gateway component between the world of RFID tags and the Internet. These two worlds are characterized by different architectural styles, naming conventions, and communication protocols. On the Internet side, an RFID reader looks like a standard web server that adheres to all Internet standards. On the RFID side, the RFID reader respects the RFID communication protocol standards. The RFID reader has to resolve all property mismatches.

13.4.5 RFID Security

Whenever we connect a computer to the Internet, sensitive security issues arise [Lan97] that must be addressed. Standard security techniques are based on the deployment of cryptographic methods, like *encryption*, *random number generation*, and *hashing* as outlined in Sect. 6.2. The execution of cryptographic methods requires energy and silicon real estate, which are not sufficiently available in all smart objects, such as low-cost RFID tags. The often-heard argument that computationally constrained RFID tagged objects will disappear in the near future as the microelectronic devices become cheaper overlooks the price pressure on simple RFID tags. If low-cost RFID tags are placed on billions of retail products, even a 1-¢ increase in the cost of a tag for the provision of cryptographic capabilities will be shunned.

The information security threats in the IoT can be classified into three groups: (1) the threats that compromise the *authenticity* of information, (2) the threats to *privacy* caused by a pervasive deployment of IoT products, and (3) *denial of service* threats. We assume that the vast majority of IoT devices are connected to the cyberspace by a wireless connection. A wireless connection always presents a serious vulnerability since it opens the door to an unnoticed observation of the traffic by an adversary.

Authentication. It is a basic assumption in the IoT that the *electronic device*, e.g., a RFID tag, represents a unique *physical thing* in cyberspace and that this link between the electronic device and the physical thing which has been established by a *trusted authority* can be relied upon. This belief in *tag authenticity* can be shaken easily. Scanning and replicating an unprotected tag is relatively easy, since a tag is nothing else than a string of bits that can be copied without difficulty.

Attaching another *physical thing* – e.g., a *faked product* – to an authentic tag can break the link between the *physical thing* and the *tag* – the representative of the physical thing in cyberspace. This kind of attack has to be addressed in the level of *physical design of a smart object* and cannot be dealt with by cyberspace security methods.

The known techniques to ensure the authenticity of the *thing* behind a low cost RFID tag are quite limited. A tag is a bit-string that can be read by any commodity reader and can be copied to produce a *cloned tag*. Even a digital signature could not prevent *cloning of tags*. *Men in the middle attacks*, where an attacker mimics a correct tag, might break the established link between the *reader* and the *tag*. Accessing the product database can detect the existence of *cloned tags* by discovering that the uniqueness property of the EPC has been violated, but it cannot eliminate cloning.

Example: Accessing the product database can identify a counterfeit piece of art that carries a cloned tag and finding out that the genuine object is at a location that is different from the tag reader.

Tamper-proof tags that physically break when they are detached from the *thing* they have been attached to by the trusted authority are one solution to the problem of physical tag stealing. In order to be able to ascertain the authenticity of valuable things *physical one-way functions* (POWF) have been proposed [Pap02]. An example for a POWF is a transparent optical device with a random three-dimensional microstructure that is attached to the thing in a tamper-proof manner. Since the randomness of the structure cannot be controlled during the manufacturing process, it is impossible to produce two POWF that are alike. When read by a laser under a specific angle, a POWF response is a bit stream that is characteristic for this unique POWF. Depending on the reading angle, different characteristic bit streams can be retrieved. These bit streams can be stored in the product database. It is difficult for an adversary to clone a POWF, because it is a *thing with random characteristic physical properties* that cannot be represented by a mathematical function. A POWF is not a *construct of cyberspace* that can be copied or reconstructed.

Privacy. The main privacy concern in the RFID world is the *clandestine reading* of a tag by an unauthorized reader. Since low-cost RFID tags are unprotected and can be read by commodity readers, clandestine tag tracking by unauthorized readers discloses valuable information to an adversary. If the adversary uses a sensitive reader with a high-power antenna output (*rogue reading*), he can significantly extend the nominal read range. The information about EPC codes and other attributes that are contained in the tag can be linked with the identity of the person carrying the tag in order to construct a personal profile. Since a low-cost tag does not have the cryptographic capability to authenticate the reader, it will disclose its information whenever it is queried. Clandestine tag reading can be prevented by permanently killing the tag as soon as the tag enters the consumer domain, i.e., at the point-of-sale. Tag killing enforces consumer privacy effectively. However, if tags support the functionality of tag killing, a *vulnerability* with respect to availability is established.

Example: By analyzing the tagged medication a person is carrying, an adversary could infer information about the health condition of the person.

Example: If – as has been proposed – money bills contain an RFID tag, an adversary with a hidden reader could determine unnoticeably the amount of money a person is carrying in her/his briefcase.

Example: In a commercial setting, an adversary with a hidden reader could periodically monitor the inventory of goods in a competing supermarket.

Another privacy enforcement technique does not *prevent*, but *detects* clandestine reading. A consumer can carry a special *monitoring tag* that alerts the carrier whenever a clandestine reading attack is detected. The monitoring tag transforms a *clandestine reading action* to an *open reading action* and thus exposes the hidden adversary.

Denial of Service. A *denial of service attack* tries to make a computer system unavailable to its users. In any wireless communication scenario, such as an RFID system or a sensor network, an adversary can jam the ether with high-power signals of the appropriate frequency in order to interfere with the communication of the targeted devices. In the Internet, an adversary can send a coordinated burst of service requests to a site to overload the site such that legitimate service requests cannot be handled any more (see also Sect. 6.2.2 on botnets).

Some RFID tags support – as a privacy enhancement mechanism – the functionality to put a tag into a sleep mode or to permanently kill a tag. An adversary can use this functionality to interfere with the proper operation of the service.

Example: At an automated supermarket checkout an RFID reader determines the purchased goods by reading the RFID tags of the items in the shopping cart. If an adversary disables some tags, the respective items will not be recognized and don't appear on the bill.

13.5 Wireless Sensor Networks

Recent progress in the field of Micro-Electro-Mechanical Systems (MEMS), low-power microelectronics, and low-power communication has made it possible to build small integrated *smart objects,* called *sensor nodes*, that contain a sensor, a microcontroller and a wireless communication controller. A sensor node can acquire a variety of physical, chemical, or biological signals to measure properties of its environment. Sensor nodes are resource constrained. They are powered either by a small battery or by energy harvested from its environment, have limited computational power, a small memory, and constrained communication capabilities.

In order to monitor and observe a phenomenon, a number (from few tens to millions) of sensor nodes are deployed, either systematically or randomly, in a *sensor field* to form an ad hoc self-organizing network – a wireless sensor network (WSN). The WSN collects data about the targeted phenomenon and transmits the data via an ad-hoc multi-hop communication channel to one or more base stations that can be connected to the Internet.

After a *sensor node* is deployed in a *sensor field*, it is left on its own and relies on its self-organizing capabilities. At first, it must detect its neighbors and establish communication. In the second phase, it must learn about the arrangement in which the nodes are connected to each other, *the topology of nodes*, and build up ad-hoc multi-hop communication channels to a base station. In case of the failure of an active node, it must reconfigure the network.

Wireless sensor networks can be used in many different applications such as remote environment monitoring, surveillance, medical applications, ambient intelligence, and in military applications. The utility of a wireless sensor network is in the *collective emergent intelligence* of all active sensor nodes, not the contribution of any particular node.

A sensor network is operational as long as a minimum number of nodes is active and the connectivity of the active nodes to one of the base stations is maintained. In battery-powered sensor networks, the lifetime of the network depends on the energy capacity of the batteries and the power-consumption of a node. When a sensor node has depleted its energy supply, it will cease to function and cannot forward messages to its neighbors any more. Energy conservation is thus of utmost importance in sensor networks. The design of the nodes, the communication protocols, and the design of the system and application software for sensor networks are primarily determined by this quest for energy efficiency and low cost.

Recently, attempts are made to use the RFID infrastructure for the interconnection of autonomous low-cost RFID-based sensor nodes [Bha10]. These sensor nodes operate without a battery and harvest the energy either from the environment or the electromagnetic radiation emitted by the RFID reader. This technology has the potential to produce long-lasting, low-cost ubiquitous sensor nodes that may revolutionize many embedded applications.

Points to Remember

- According to the IoT vision, a *smart planet* will evolve, where many of the everyday things around us have an identity in cyberspace, acquire intelligence, and mash-up information from diverse sources.
- The *Electronic Product Code (EPC)* is a unique identifier for the naming of every physical smart object on the planet. This is more ambitious than the forerunner, the optical bar code, which assigns a unique identifier only to a class of objects. The EPC is managed by the international organization *EPC global*.
- A composite object requires its own UID that is only loosely related to the UIDs of its constituent parts. The different names, *UID*, *object type name*, and *object role name* must be introduced at the level of composite objects as well. Since a composite object can be an *atomic unit* at the next level of integration, the name space must be built up recursively.

- The division of work between a smart object and the cloud will be determined, to a considerable degree, by energy considerations. If the energy required to execute a task locally is larger than the energy required to send the task parameters to a server in the cloud, the task is a candidate for remote processing.
- The autonomic management of smart objects must cover *network service discovery*, *system configuration and optimization*, *diagnosis of failures and recovery after failures*, and *system adaptation and evolution*.
- An RFID reader can act as a gateway to the Internet and transmit the object identity, together with the read-time and the object location (i.e., the location of the reader) to a remote computer system that manages a large database.
- The information security threats in the IoT can be classified into three groups: (1) the threats that compromise the *authenticity* of information, (2) the threats to *privacy* caused by a pervasive deployment of IoT products, and (3) *denial of service* threats.
- In order to avoid clandestine reading, a tag must authenticate the reader.
- It is difficult for an adversary to clone *physical one-way functions* (POWF), because it is a *thing with random characteristic physical properties* that cannot be represented by a mathematical function. A POWF is not a *construct of cyberspace* that can be copied or reconstructed.
- After a *sensor node* is deployed in a *sensor field*, it is left on its own and relies on its self-organizing capabilities. At first, it must detect its neighbors and establish communication. In the second phase it must learn about the arrangement in which the nodes are connected to each other, *the topology of nodes*, and build up ad-hoc multi-hop communication channels to a base station. In case of the failure of an active node, it must reconfigure the network.

Bibliographic Notes

In 2009, the European Union has published a Strategic Research Roadmap for the Internet of Things [Ver09] that discusses the vision of the IoT and relevant research issues up to the year 2020 and beyond. The excellent *RFID handbook* [Fin03] is a valuable reference for the RFID technology. The September 2010 special issue of the Proceedings of the IEEE [Gad10] is devoted to RFID technology.

Review Questions and Problems

13.1 What is the vision of the *Internet of Things* and which are the most pressing technical issues that must be resolved?
13.2 What are the drivers for the *Internet of Things*?
13.3 What is a *smart object*?
13.4 Discuss the naming of smart objects! What is a *UID*, a *type name*, a *role name*, or a *name of a composite object*?

13.5 Discuss the different standards for near-field communication!
13.6 What is the relation between the IoT and cloud *computing*?
13.7 Describe the MAPE-K model of an autonomic component!
13.8 What are the functions of an RFID reader?
13.9 What are typical parameters for low-costs RFID tags?
13.10 What is the electronic product code (EPC) and what is its relation to the ubiquitous optical bar code?
13.11 What is a *physical one-way function* (POWF)? Where is it needed?
13.12 What are the three main security threats in the RFID field?
13.13 How is a sensor node deployed in a sensor field?
13.14 Describe the self-organizing capabilities of a sensor node!