I

INTRODUCTION TO MOBILE AD HOC NETWORKS

The first wireless communication network between computers was created in 1970 by Norman Abramson at the University of Hawaii, the AlohaNet [11]. It was composed of seven computers distributed over four islands that were able to communicate with a central node on Oahu using radio communication. Additionally, the most well-known random-access protocol, ALOHA, was also developed and presented at that time [12]. The ALOHA channel is used nowadays in all major mobile networks (2G and 3G), as well as in almost all two-way satellite data networks [58].

Thanks to the reduction in the cost and size of the hardware needed, the wireless technology widely extends in our everyday life. The huge number of devices that provide wireless technology nowadays, as well as the increasing number of people that not only carry a device with wireless capabilities but actually use it, make the field of wireless technology a key topic in research.

The current mobile wireless networks consist of wireless nodes that are connected to a central base station. When a device moves to a different

Evolutionary Algorithms for Mobile Ad Hoc Networks, First Edition. Bernabé Dorronsoro, Patricia Ruiz, Grégoire Danoy, Yoann Pigné, and Pascal Bouvry.

geographical area, it must connect to a different base station in order to continue with the service. This means that two nodes located in the same region cannot communicate unless there is a base station associated to that area. Researchers envisioned a possibility for communicating devices where the fixed infrastructure was not available, that is, remote or disaster areas. This kind of network is called an ad hoc network.

The term *ad hoc* has been extensively used during the last decade. According to the *American Heritage Dictionary of the English Language*, it has two different meanings: (1) form for or concerned with one specific purpose and (2) improvised and often impromptu. These two definitions of the term *ad hoc* describe the purpose of a new kind of network that emerged with the wireless technology.

Definition 1 Ad hoc Network. *It is a decentralized and self-configuring network spontaneously created between neighboring devices with communication capabilities, without relying on any existing infrastructure.*

In an ad hoc network, all devices may also act as routers and forward packets to enable communication between nodes that are not in range. Two nodes are said to be in range when they are able to receive and properly decode packets sent by the other node.

Some examples where the deployment of an ad hoc network can be used and actually can be very useful are relief in disaster areas, battlefield deployment, sensing areas, social events (like a concert), and the like. In those cases, devices can create a temporary network for a specific purpose, that is, an ad hoc network. When devices are mobile, they are called mobile ad hoc networks.

Ad hoc networks suffer from the typical drawbacks of wireless networks such as interference, time-varying channels, low reliability, limited transmission range, and so forth. Additionally, ad hoc networks have specific characteristics that make their deployment very challenging. Next, we describe the main ones:

1. Decentralization: nodes locally execute the algorithms and take all decisions by themselves:
2. Self-organization: nodes must be able to create, join, and manage an ad hoc network by their own means.
3. Limited network resources: the medium is shared between all devices in range.
4. Energy limitations: devices rely on battery.
5. Dynamism: nodes move, appear and disappear from the network.

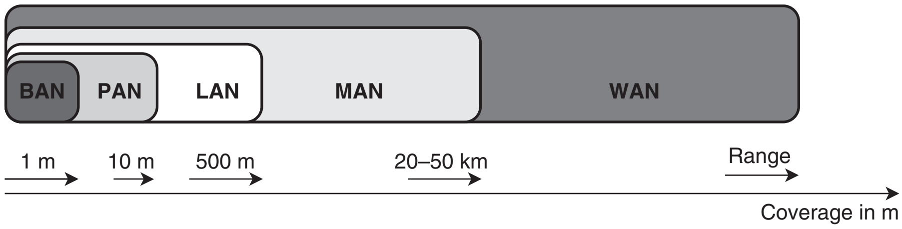

Figure 1.1. Classification of ad hoc networks in terms of the coverage area.

6. Heterogeneity: any kind of device with wireless capabilities may be able to join the network.
7. Scalability: nodes can join or leave the network at any time, therefore the number of nodes composing it is unpredictable.
8. Multihop: in order to communicate two remote nodes, devices have to also act as routers forwarding packets not intended for themselves.
9. Security: the lack of central authority, the changing topology, and the vulnerability of the channel makes difficult guaranteeing secure communications.

Chlamtac et al. [20] presented a classification of ad hoc networks in terms of the coverage of the devices (see Fig. 1.1). They can be differentiated into five different classes, explained below.

- Body area network (BAN) is a communication network (usually wireless) composed of small wearable nodes (earphones, microphones) that provides connectivity between those devices. It is also extended to small sensor nodes implanted in the human body that collect information about the patient’s health and send it to an external unit. The range needed is just to cover the human body (i.e., 1–2 m).
- Personal area network (PAN) enables the communication of mobile devices carried by individuals, like smart phones, PDAs, and the like to other devices. The range varies with the technology used, from 10 to 100 m.
- Local area network (LAN) interconnects computer nodes with peripheral equipment at high data transfer in a predefined area such as an office, school, or laboratory. The communication range is restricted to a building or a set of buildings, between 100 and 500 m.
- Metropolitan area network (MAN) spans a city or a large campus. It usually interconnects different LANs. The size is variable, covering up to tens of kilometers.

- Wide area network (WAN) covers a large geographical area. It can relay data between different LANs or over long distances.

Both MAN and WAN still need much more work to become a reality in a near future. There are many challenges that are not solved yet like communication beyond line of sight, identification of devices, routing algorithms, and the like that keep researchers working on the topic [35, 38, 39, 68].

Apart from this classification, the ad hoc networking field has three well-defined research lines: (1) mobile ad hoc networks, (2) vehicular ad hoc networks, and (3) sensor networks. The first one is defined as an ad hoc network where devices do move and includes all personal devices like smart phones, PDAs, laptops, and gaming devices. When devices move at high speeds, without energy restrictions and the network is able to use road side units for communicating, we are talking about vehicular ad hoc networks. Finally, in sensor networks devices are generally meant to acquire data from the environment and report it to a central node or gateway. The next sections give a more detailed view of these three types of ad hoc networks.

1.1 MOBILE AD HOC NETWORKS

Mobile ad hoc networks, also called MANETs, are ad hoc networks where the devices that make up the network are mobile. Khan [43] extended the previously mentioned AlohaNet including repeaters, authentication, and coexistence with other possible systems in the same band. This new system was called the packet radio network, PRNET [43]. The PRNET project of the Defense Advanced Research Projects Agency, DARPA, started in 1973 and evolved through the years (1973–1987) to be a robust, reliable, operational experimental network. The MANETs were first defined in PRNET project. In Jubin and Tornow [41], a detailed description of PRNET is presented and in [40] PRNET is defined as a mobile ad hoc network.

Initially, MANETs were mainly developed for military applications, specially for creating communication networks on the battlefield. In the middle of 1991, when the first standard was defined (IEEE 802.11 [69]), and the first commercial radio technologies appeared, the great potential of ad hoc networks outside the military domain was envisioned. Apart from the military scenarios, all the previously mentioned applications for ad hoc networks (if we consider moving devices) are considered in this section. However, there are many applications like emergency services, multiuser gaming, e-commerce, information services, mobile office, that extend the cellular network.

Advances in the technology made possible Internet connection in portable devices. Mobile phones evolved to smart phones with large screens, cameras,

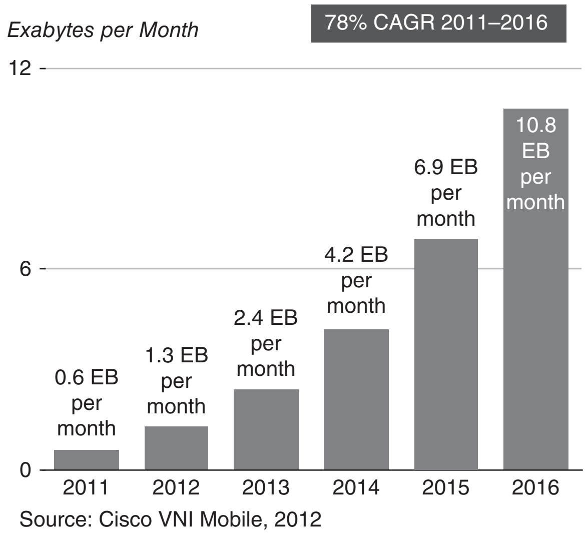

Figure 1.2. Cisco forecasts of mobile data traffic up to 2016.

GPS, bluetooth, high-speed data access, and a friendly operating system. At the end of 2013, the number of mobile devices will exceed the world’s population, and by 2017 there will be 1.4 mobile devices per capita [52]. Moreover, as many people (not only industry) focused on developing applications for those smart phones, social networks such as Facebook or Twitter appeared. The former has, on average, 1.11 billion monthly active users as of March 2013 [64]. The latter has 140 million active users and 340 million Tweets a day [65] just after 6 years. No one could have predicted the amazing growth of social networking. Actually, those applications are not only used in computers but also in smart phones and tablets, increasing the mobile data traffic. It is expected that in 2016 the mobile data traffic will be more than eight times higher than in 2012, and only 0.3% of this traffic will be due to VoIP (voice over IP) [52]. Figure 1.2 shows the growth of mobile data, envisioning a 78% increase in the compound annual growth rate (CAGR) from 2011 to 2016.

With such numbers, the cellular network will be soon saturated. To alleviate this problem, part of the mobile data traffic can be delivered by a complementary network. This mechanism is known as *3G Offloading*. There are studies that present mobile ad hoc networks as this complementary network [14, 56].

Some of the main characteristics of mobile ad hoc networks that make their design challenging are mentioned below:

1. The lack of any infrastructure forces the node to perform network setup, management, self-healing, neighbor discovery, and the like.

2. Every node must have routing capabilities for communicating nodes out of range.
3. Energy constraints depend on batteries.
4. Network resource restrictions, as in wireless network, are shared (limited bandwidth, collisions, etc.).
5. Network partitioning is due to the limited transmission range and the mobility of devices:
6. Dynamic topology of the links is time varying because of the mobility of the nodes and appearance and disappearance of devices.

Although vehicular ad hoc networks and mobile sensor networks can be seen as a subclass of mobile ad hoc networks, the nodes composing the network are completely different. Therefore, the technologies used for each of the previously mentioned types of ad hoc networks are different. The main idea of mobile ad hoc networks is connecting any device in range (considering WLAN). The most common technology that gives service for computer communication in WLAN is Wi-Fi, which is already included in most of the commercial devices, making it the most suitable technology for mobile ad hoc networks.

Wi-Fi is a technology defined by the Wi-Fi Alliance [7] that allows wireless communication based on the IEEE 802.11 standards. The first IEEE 802.11 standard was published in 1997 [69], and there have been two updates, one in 2007 and another in 2012. It uses two frequency bands, 2.4 and 5 GHz. There exists a big variety of amendments to each of the standards that focus on different characteristics in wireless communication. Some examples are IEEE 802.11n, which allows MIMO antenna (multiple-input multiple-output), the IEEE 802.11s for mesh networking, and IEEE 802.11aa for video transport stream. For a complete view of the amendments and the time line, please refer to [69].

The most commonly used standards are IEEE 802.11b (1999) and IEEE802.11g (2003), which are amendments to the original standard IEEE 802.11-1997. They both work on the 2.4-GHz band, the latter being more recent with higher data rate but still fully compatible with IEEE 802.11b hardware. The IEEE 802.11n (2009) is an amendment to the IEEE 802.11-2007, which includes MIMO antenna, a significant increase in the throughput (from 54 to 600 Mbits/s), and operates in both frequency bands. These amendments are the most used versions of the IEEE 802.11 standard that provide wireless capabilities for everyday devices. Due to its reduced cost and its fast arrival on the market the IEEE 802.11b was widely adopted, making the adoption of IEEE 802.11g, which was fully compatible, very easy and fast.

1.2 VEHICULAR AD HOC NETWORKS

Vehicular ad hoc networks, hereinafter VANETs, are ad hoc networks where the devices making up the network are vehicles. In VANETs, apart from the nodes, there can also be base stations or fixed infrastructure called roadside units.

VANETs should not be confused with intelligent transportation systems (ITS). ITS cope with all kind of communications inside the vehicle, between cars or with the roadside unit, but are not limited to road transport. It also includes rail, water, and air transport. Thus, VANET is a component of ITS.

The idea of a network composed of base stations and vehicles is not new. The literature reveals that much effort has been applied to vehicular networks. Already in 1952, Friedberg discussed how to place a mobile antenna on a vehicle in order to communicate with the driver [29]. Researchers were not the only ones interested. So were companies. In 1966, General Motors Research Laboratory was already designing a real-time system for traffic safety. It was able to send voice messages alerting devices about road dangers ahead. Later, they were also considering systems that would not only make driving safer but more convenient and more enjoyable as well [33]. At that time, they were already proposing a two-way communication system, able to obtain road information but also enable drivers to ask for assistance. The system also provides (1) audio signs for receiving emergency messages and road conditions in the vehicle, (2) visual signs reproducing roadside traffic signs, and (3) navigation assistance of a preselected route. An extensive review of studies related to motorist information is presented in [50].

The PROMETHEUS Eureka program (1985–1993) was intended for developing an intelligent co-pilot that helps the driver but did not create an autonomous car. More than 60 participants from 5 different countries where involved and almost all the car manufactures. The project was divided into different subprograms: PRO-CAR, PRO-NET, and PRO-ROAD. The PRO-NET system depends on the communication links between vehicles [30]. In 1988, in the framework of the project they proposed vehicle-to-vehicle communication that would increase driving security [25]. In 1989, the Commission of the European Community launched the DRIVE program. The objectives were similar to the ones proposed in PROMETHEUS: improve road safety, traffic and transport conditions, and reduce environmental pollution; but while PROMETHEUS focuses on assisting the driver, DRIVE focuses on the infrastructure. A review of both projects and their differences can be found in [30].

Anwar et al. [16] proposed the use of packet radio networks for car-to-car communication in densely populated cities. They are considering mobile radio networks (MRN) where there are no central stations. Thus, they are actually talking about a mobile ad hoc network. They created a scenario with one- and two-way roads, traffic lights, buildings, collisions, and shadowing. In the same conference, Davoli et al. [27]. presented an architecture and a protocol for car-to-infrastructure communication using the packet radio network. But as mentioned in [34], the term VANET was first coined by Kenneth B. Laberteaux, who also conducted and promoted the first VANET workshop in 2004 as general co-chair [45].

Vehicular ad hoc networks can be considered as a subset of mobile ad hoc networks, but they have specific characteristics that distinguish them from typical mobile ad hoc networks and that make their design challenging. For example:

1. Constantly changing topology because devices move at very high speeds, typically varying from 0 to 180 km/h. The changing topology impacts network partitioning not only because of the high speeds of vehicles but also because when vehicles move from urban to rural areas the density of devices is lower.
2. Variable network density mostly depends on the time and the area. At rush hours the traffic is high and it is usually low in rural areas.
3. As a consequence of the high speed and the limited transmission range, the link availability is low (less than 1 minute), not only for devices moving in opposite directions but also cars driving in the same directions.
4. Unlike mobile or sensor ad hoc networks, vehicular ad hoc networks are not energy constrained.
5. Vehicles do not move at random, they move along lanes following routes. Additionally, a specific device might have predictable routes: Everyday, a driver goes from home to work and back again, at approximately the same time.
6. There exist two different operation modes: (1) car-to-car communication and (2) car-to-infrastructure communication.

In 1999, the U.S. Federal Communication Commission allocated 75 MHz of the dedicated short-range communication (DSRC) spectrum at 5.9 GHz to be used exclusively for vehicle-to-vehicle and infrastructure-to-vehicle communications [23]. DSRC technology allows high-speed communication between vehicles and the roadside or between vehicles that might be separated up to 1000 m. There exist differences in the frequency allocation between North America and Europe, but the intention is to be able to use the same antenna and transmitter/receiver. Different organizations like the

Institute of Electrical and Electronic Engineers (IEEE), International Standard Organization (ISO), or Car-to-Car Communication Consortium/GeoNet are working on developing an architecture for VANETs. There is no agreement between the different organizations on which of the different proposals is more convenient for vehicular networks. Thus, each of them is working on their own system: WAVE by IEEE, CALM by ISO, and C2CNet by C2C Communication Consortium. A general overview on the three schemes is given next.

1.2.1 Wireless Access in Vehicular Environment (WAVE)

The IEEE 1609 family of standards for wireless access in vehicular environments (WAVE) defines the architecture, communications model, management structure, security mechanisms and physical access for high-speed (up to 27 Mb/s) short-range (up to 1000 m) low-latency wireless communications in the vehicular environment. The primary architectural components defined by these standards are the on-board unit (OBU), road-side unit (RSU) and WAVE interface [55].

IEEE 1609 is composed of different standards tackling different layers that are already published, that is, IEEE1609.1 is the resource manager, IEEE 1609.2 copes with security services, IEEE 1609.3 with network services, and IEEE 1609.4 is for channel switching. However, part of this family of standards is still under development as IEEE 1609.0 the architecture, IEEE 1609.5 the communication manager, IEEE 1609.6 remote management service, IEEE 1609.11 for secure electronic payment, or IEEE 1609.12 identifier allocations, at the time of this writing.

In 2003, IEEE and American Society for Testing and Materials (ASTM) adopted a first version of the DSRC PHY [18], which was based on IEEE 802.11a. In 2004, in creating the 802.11p amendment within the IEEE 802.11 Working Group they agreed to add wireless access in vehicular environments (WAVE). The 802.11p [10] is built on its predecessor ASTM E2213, and it defines the required enhancements to IEEE 802.11 for supporting ITS applications.

Additionally, Society of Automotive Engineers (SAE) international standards J2735 [66] and SAE J2945.1 [57] (still under development) define a set of message formats for vehicular applications and the rules (like rate or power constraints), respectively. Those standards operate with applications using DSRC/WAVE, but they have been designed to potentially be also used with other wireless communication technologies.

Depending on the application requirements DSRC/WAVE can operate using the traditional internet protocols Internet Protocol Version 6 (IPv6), User Datagram Protocol (UDP), and Transmission Control Protocol (TCP) defined by Internet Engineering Task Force (IETF), or using WAVE Short Messages Protocol (WSMP) defined in IEEE 1609.3. The non-IP WSMP aims at exchanging nonrouted data as safety messages.

The architecture proposed by IEEE has the IEEE 1609.x family as the core standard, the IEEE 802.11p at the physical and MAC layers, and the SAE J2735 and SAE J2945.1 at the top of the protocol stack. A detailed explanation of the architecture of the IEEE standard for DSRC can be found in [44].

1.2.2 Communication Access for Land Mobiles (CALM)

ISO TC204 WG16 is developing a family of international standards based on the CALM (communication access for land mobiles) concept. This family of standards specifies a common architecture, network protocols, and communication interface definitions for wired and wireless communications using various access technologies including cellular second generation, cellular third generation, satellite, infrared, 5-GHz microwave, 60-GHz millimeter-wave, and mobile wireless broadband. These and other access technologies that can be incorporated are designed to provide broadcast, unicast, and multicast communications between mobile stations, between mobile and fixed stations, and between fixed stations in the intelligent transport systems (ITS) sector [62].

The CALM standards are communication-centric that block out the application layer from the communication protocols. The idea behind it is that the CALM system will communicate using the most suitable communication technology depending on the application needs, the availability of the different technologies, the channel conditions, and the like. It is a heterogeneous system where devices have different interfaces and are able to support handover between the different technologies supported in CALM (cellular, infrared, DSRC, satellite, etc.). This is known as media-independent handover.

As of 2013, the set of CALM standards is still under development, but some research projects like COOPERS [4] or CVIS [8], already consider this technology. The CALM architecture (ISO 21217) is composed of six parts: *applications*, *management*, *security*, *facilities*, *networking, and transport*, and *access*. As it is based on a modification and an extension of the layered Open Systems Interconnection (OSI) model [72], there exists a correspondence between the OSI layers and some of the previously mentioned parts. The first two layers of the OSI model are included in access; layers three and four correspond with networking and transport; and facilities contain the remaining layers of the OSI model. For a more detailed explanation of the model refer to [63].

In CALM, the car is not only considered as one single device but more as a whole in-vehicle network with a variety of embedded and interconnected devices. The architecture must be able to cope with multiple technologies simultaneously and also with network mobility (NEMO). As vehicles move, the gateways to the Internet change, but the Internet connectivity to the in-vehicle network must be uninterrupted.

Similarly to WAVE, CALM operates using the IPv6 networking protocol, but for time-critical safety messages a specific non-IP protocol called FAST is used (ISO 29281). FAST supports vehicle–vehicle and vehicle–roadside communications with a very light header.

1.2.3 C2C Network

C2C Network (C2CNet) is a communication layer defined by the Car-2-Car Communication Consortium [3] specifically for car-to-car communication. As it was first defined in [24], the C2C Communication layers' architecture differentiates between three different type of applications: active safety, traffic efficiency, and infotainment. The first one relies on IEEE 802.11p and does not make use of the TCP/IP protocol. It uses a specific C2C network and C2C Transport for vehicular communications. The traffic efficiency applications can use both the IPv6 or the C2C Network over the conventional wireless LAN technologies based on IEEE 802.11 a/b/g/n. For the last kind of applications the TCP/IP (or UDP) will be used on top of other wireless technologies like General Packet Radio Service (GPRS) or Universal Mobile Telecommunications System (UMTS).

The C2C-CC system does not force all vehicles to be equipped with all the previously mentioned technologies, but at least the on-board unit must be able to communicate using the IEEE 802.11p radio technology for safety applications.

The C2C Network layer [54] is located between the network and the link layer. It supports geographical addressing and routing. The C2C header contains geographical locations. It does not use IP addresses, but IPv6 packets can be transmitted by encapsulating the IPv6 packet into a C2CNet packet (IPv4 will also be supported). That was defined in the GeoNet project [1] "IPv6 over C2CNet."

At the time of this writing, these three architectures are still under development. Therefore, the final architecture will possibly differ from the brief overview given here. Moreover, the final decision about which standard to adopt may depend on car manufactures and authorities considering various technical, business, and political aspects. A more detailed comparison between the three architectures is presented in [49].

1.3 SENSOR NETWORKS

Nowadays, sensor networks are widely used in practice for managing traffic lights, environmental conditions, system failures, security systems, and the like. But one of the main areas of sensor networks is in the field of medicine, and it is most probably one of the oldest sensor applications. Already in the early 1950s, doctors were using sensors for monitoring patients like electrocardiographs, blood pressure recorders, electroencephalograph, and so forth. In 1956, Davis and Baldwin [26] proposed an intercommunication system for all members of the operating team, as well as for stimulating a patient during the surgical treatment of epilepsy. Moreover, they were exploring the possibility of a wireless system at that time.

Indeed, in 1957 Mackay and Jacobson [48] described a small unit (0.9 × 2.8 cm) that could be easily swallowed that was able to simultaneously transmit pressure and temperature signals for 2 weeks. A survey on the techniques available at that time can be found in [47].

The advances in microelectrical-mechanical systems (MEMS) technology made possible low-cost and small-size wireless sensor nodes. A sensor network is an ad hoc network composed of a large number of devices geographically distributed, able to monitor different environmental or physical conditions (the data of interest). Each node usually gets the raw sensed data, processes it locally, and sends it to the node responsible for the data aggregation, the sink or gateway (see Fig. 1.3). The user is able to access the gathered data from the gateway. There are many different configurations of sensor networks. It is possible to have a network with a single sink, where all the devices send the collected data to the sink and it uses the information locally. There could also be a gateway that connects the sink to other networks like the Internet, so that the user can access the data gathered (in this case, the gateway can also act as a sink). For scalability reasons, having more than one sink is desirable. Wireless sensor networks (WSN) can be programmed as self-organizing, according to different network topologies (star, linear, clustered, mesh, etc.) based on the specific application requirements. Akyildiz et al. [13] present an extensive survey on sensor networks.

Sensor networks have been widely used. Initially, they were mostly limited to military applications (surveillance, intrusion detection, targeting systems, etc.). Chong and Kumar [21] explained the history of sensor networks, the technology, and the challenges. An example of the early military use is the deployment of the seismic intrusion sensors in the Vietnam war around the camp as part of the intrusion warning system [46]. Nowadays, thanks to the reduction in cost and size, they are being applied in many different fields like in health for monitoring patients, for environmental measurements like temperature, pollution, pressure, or humidity, for monitoring disaster

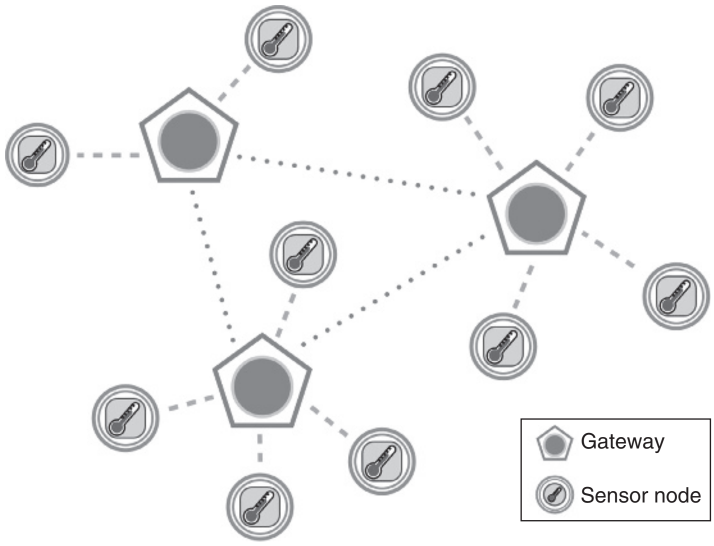

Figure 1.3. Example of a sensor network.

areas, in commercial for managing inventory, intelligent buildings, vehicle monitoring, animal monitoring, or machine monitoring.

The size of the node can vary depending on the application. Kahn et al. [42], propose a prototype called Smart Dust, so small that it could be suspended in the air for hours or even days (the volume is a few cubic millimeters). Regarding mobility, the nodes are typically fixed. However, in applications like data acquisition of twisters where the sensor nodes go inside the tornado, mobility is a key feature for capturing information.

Now, we focus on ad hoc WSNs and briefly explain them. In this kind of network (ad hoc networks in general), the network topology is not known a priori, thus, it must be constructed in real time. Moreover, due to new deployments of sensors or node failures, the topology must be updated periodically. In these networks, where nodes only communicate with neighbors, distributed algorithms are attractive because they are robust to topology changes. Chong and Kumar [21], claimed that decentralized algorithms are preferred to centralized ones (even if they can collect data from multiple sensor nodes) because the latter are less robust, less reliable, and have higher communication cost.

There are specific and challenging key features when designing a wireless sensor network that must be taken into account. Here, we mention some desired characteristics:

1. *Energy:* The tiny size and the constant sensing activity of the devices make energy consumption the critical factor in its design [28]. Some

decisions must be taken in order to balance the performance of the sensor network and the resource utilization. For example, gathering sensed data from a higher number of nodes will give more accurate results, but more communication resources are needed (i.e., energy).

2. *Low Latency:* Depending on the application, the data gathered can be already out of date in high latency networks. The delay the raw sensed data experiences from its acquisition until its utilization can be crucial depending on the application (e.g., patient monitoring).
3. *Scalability:* The number of nodes deployed in an area can vary from tens to thousands of sensors. Thus, algorithms used must be able to provide the desired performance regardless of the size of the network.
4. *Reliability:* Sensor nodes can fail due to the battery lifetime or because of extreme environmental conditions. Therefore, the algorithms designed must be resilient to failures and the network self-healing.
5. *Deployment:* Optimal distribution of the sensor over a spatial area is necessary.

There are some important differences between mobile ad hoc networks and sensor networks and also between their applications, which makes no straightforward reuse of algorithms and protocols of MANETs in sensor networks. The suitability of those algorithms must be checked before their actual implementation. We now mention some of those differences:

- In ad hoc networks the terminals are smart with high capacity, while in sensor they are simple, and the capacity rate in most of the applications is very low (few bytes).
- Unlike in ad hoc networks, in sensors not all the nodes act as routers.
- Although energy is considered a key feature, capacity is the most relevant characteristic that must be taken into consideration when designing an ad hoc network; while in sensor networks the energy is the most important restriction that must be always considered in their design [19].

In sensors, communications protocols must be designed that consider the energy restrictions. Indeed, the energy consumption needed for transmitting data is much bigger than the one needed for processing the data. However, the signal processing must not be neglected from the energy consumption as processing data sometimes can take much longer than transmitting the data and, therefore, consumes more than the transceiver in idle mode. Additionally, when the sleep mode is assumed in sensors, suitable synchronization is needed in order to have efficient communication between nodes.

As each sensor must sense, process, and communicate using a limited amount of energy, a cross-layer design that takes into consideration all these requirements (communication protocols, signal, and data processing) will provide some benefits.

Unlike MANETs or VANETs, sensors are being used in some real-world applications. Thus, there exist many different technologies for sensors depending on the necessities of the targeted application. Next, we introduce some of the most well-known technologies and standards that are available at the time of this writing.

1.3.1 IEEE 1451

The National Institute of Standards and Technology (NIST) [6] is developing a family of smart transducer interface standards IEEE 1451 *that describes a set of open, common, network-independent communication interfaces for connecting transducers (sensors or actuators) to microprocessors, instrumentation systems, and control/field networks. The key feature of these standards is the definition of Transducer Electronic Data Sheets (TEDS). TEDS is a memory device attached to the transducer, that stores transducer identification, calibration, correction data, measurement range, and manufacture-related information. The goal of 1451 is to allow the access of transducer data through a common set of interfaces whether the transducers are connected to systems or networks via a wired or wireless means* [51].

IEEE 1451 allows the sensors to have capabilities for self-identification, self-description, self-diagnosis, self-calibration, location awareness, time awareness, data processing, reasoning, data fusion, alert notification, standard-based data formats, and communication protocols [60]. It also provides plug-and-play capability. The definition of TEDS is the key feature that can be seen as an identification card that contains specific data of the transducer (including manufacturer information) allowing the sensor to connect to different networks.

1.3.2 IEEE 802.15.4

In 2003, the original standard of the IEEE for low-rate personal area networks (LR-PAN), IEEE 802.15.4, was approved. Unlike IEEE 1451, it only defines the two bottom layers of the OSI model considering very low power consumption, low complexity, and low cost. After this standard, the improved version was approved in 2006 (IEEE 802.15.4b), and in 2007 location capabilities were added in IEEE 802.15.4a. In order to make it compatible with the bands available in China and Japan, in 2009, 802.15.4c and 802.15.4d were approved. Recently, in 2011, IEEE 802.15.4 was extended, the ambiguities removed, and improvements included [70].

The network can have two different topologies: (1) star and (2) peer-to-peer. Moreover, two types of devices are defined: (1) full-function device (FFD) and (2) reduced-function device (RFD). The FFD has all network functionalities, while the RFD has low resources and is capable of very simple applications. There must exist at least one FFD for coordinating the network (PAN coordinator). In the star topology nodes can only communicate with the PAN coordinator, while in the peer-to-peer configuration any two nodes in range can connect, and they are able to self-organize, which is the basis for an ad hoc sensor network.

IEEE 802.15.4 serves as the low layers of many different specifications like ZigBee, 6LoWPAN, Wireless HART, ISA-SP100, and MiWi. We will now briefly consider some of these.

1.3.3 ZigBee

ZigBee is a standard-based network protocol created by the ZigBee Alliance [2]. It is based on the 802.15.4 standard and defines layer 3 and above in the OSI model. It was designed with for purpose of creating a network with low rate and low power capabilities that still covers a long area and that gives extra features like security. In ZigBee there are two possible access modes: beacon and nonbeacon. If the beaconing is not enabled, any node can transmit data whenever the channel is free. When beacons are enabled, the PAN coordinator assigns a time slot to every device for transmitting and sends beacon signals to synchronize all devices under its control.

Three different topologies are considered in ZigBee: (1) star, (2) cluster tree, and (3) mesh. The cluster tree topology is similar to the star, but there exists the possibility that other nodes rather than the PAN coordinator are able to communicate with each other. Unlike in the first two, in the mesh network any node can communicate with any other in range. Beaconing is not allowed in this latter topology.

The ZigBee Alliance offers two specification: ZigBee and ZigBee RF4CE. The former is intended for mesh networks offering all the features of ZigBee such as self-configuring, self-healing, and so forth. Additionally, two feature sets are available: ZigBee and ZigBee PRO (being low power consumption and a large network of thousands of devices). The latter aims at providing simple device-to-device topology, thus reducing the cost and the complexity. For a more detailed description of the ZigBee technology refer to [15, 31].

1.3.4 6LoWPAN

The idea of having all devices IP-enabled connected to the Internet and all the Internet services monitoring and controlling those devices is called Internet of Things and was first mentioned in 1999 [17]. It envisions trillions of nodes working under the Internet protocol IPv6. The problem arose when dealing with low power, low bandwidth, or battery-dependent devices, what is called the wireless embedded Internet.

The IPv6 [low-power wireless personal area networks (6LoWPAN)] working group of IETF defines a set of standards for adapting IPv6 to those resource-limited devices. In Shelby and Bormann [59], we find a formal definition: *6LoWPAN standards enable the efficient use of IPv6 over low-power, low-rate wireless networks on simple embedded devices through an adaptation layer and the optimization of related protocols*.

The IPv6 header is compressed and some functionalities are simplified, so that IPv6 packets can be transmitted over an IEEE 802.15.4 network. In this case, the topology considered is a mesh.

At the time of this writing several proposals were available. A more detailed explanation of them can be found in Yibo et al. [71].

1.3.5 Bluetooth

In 1994, engineers at Ericsson invented Bluetooth, founding the Bluetooth Special Interest Group (SIG) [61] in 1998 to expand and promote the concept. But it was not until 1999 when the first specification was published.

The main idea of Bluetooth is to enable wireless information transfer between electronic devices via short-range ad hoc radio connections in a wireless personal area network. It allowed the design of low-power, small-size, low-cost radios that can be embedded in existing portable devices. In [32] the Bluetooth radio system and its ad hoc capabilities are presented.

Bluetooth works in master–slave mode, where the master is able to communicate with up to seven devices at the same time. The ad hoc network formed by the master device and the slaves connected using Bluetooth technology make up a called a piconet.

From its creation, different versions of Bluetooth were released. At the time of writing this, the last published version is Bluetooth v4.0, which includes *classic* Bluetooth technology, Bluetooth low-energy technology, and Bluetooth high-speed technology, which can be used combined or separately [67].

In their early stages, although being similar technologies focusing on short-range wireless communication, Bluetooth and ZigBee were aiming at different objectives. ZigBee had lower power consumption and was able to support larger networks, while Bluetooth had higher bit rates, what clearly differentiated the application fields for each of them. While Bluetooth was used for mobile devices and peripherals, ZigBee focused on home automation and medical sensors. Lately, Bluetooth v4.0 includes Bluetooth low energy (BLE), aimed also at very low power applications.

1.3.6 Wireless Industrial Automation System

Both ISA100 or ISA-100.11a [9, 36] and WirelessHART [22] are specific for the process automation and manufacturing industries.

WirelessHART, the first specification for wireless field instruments, was released by the Highway Addressable Remote Transducer (HART) Communication Foundation (HCF) [5] in 2007.

ISA-100.11a was started by the International Society of Automation (ISA) [37] in 2008, and it was intended to provide reliable and secure wireless operation for noncritical monitoring, alerting, supervisory control, open-loop control, and closed-loop control applications.

There are many differences between the two standards. In WirelessHART, all field devices and adapters are routers capable of forwarding packets to and from other devices in the network, enabling a mesh network topology. In the case of ISA100.11a, a node can have router capabilities or not, which means that not all devices are able to allow a new node to join the network. On the one hand, in WirelessHART there are a few optional parameters making it less flexible than ISA100.11a, which has a complex specification with many parameters. On the other hand, the lack of flexibility makes easier the interoperability between different devices in WirelessHART. Additionally, as WirelessHART is an extension of the HART protocol, it is limited to this communication protocol. However, ISA100.11a is able to tunnel many different protocols, even supporting IPv6 using 6LoWPAN. For a more detailed comparison between both protocols refer to [53].

1.4 CONCLUSION

As previously mentioned in this chapter, the design and implementation of ad hoc networks is complex. There are many challenging aspects in ad hoc networks, some of them are specific for VANETs or sensors, but many others are common for any ad hoc network like changing topology, limited resources, network partitioned, energy constraints, scalability, and the like.

It was not mentioned before, but the design of algorithms for this kind of networks is based on simulations. Creating a real mobile ad hoc network for testing purposes is very unrealistic. For handling every device a person is needed (as devices do move), which makes it unlikely to be able to test a network with a high number of devices. Moreover, in order to reproduce the experiments, the same mobility patterns at exactly the same time as well as the same conditions must be given. Therefore, it is necessary to rely on simulations. The accuracy of the simulations directly impacts on the real performance of the designed protocol.

In this book, we try to overcome some of the problems of ad hoc networks that were mentioned above using metaheuristics. In Chapter 6, the optimization of the network resources used by a broadcasting algorithm is presented. The optimal configuration of an energy-efficient broadcast protocol restricting the communication latency is studied in Chapter 7. Chapter 8 reveals some hints for overcoming network partitioning. And finally, a mechanism for creating realistic simulations is explained in Chapter 9.

REFERENCES

1. *Geonet handbook.* GeoNet Deliverable D8.3. Available at `http://www.transport-research.info/Upload/Documents/201210/20121024_111737_62231_GeoNet-D.8.3-v1.0.pdf`. Accessed February 2014.
2. Zigbee Alliance. Available at `www.zigbee.org`. Accessed September 2012.
3. CAR 2 CAR Communication Consortium. Available at `http://www.car-to-car.org/`. Accessed July 2013.
4. COOPERS project (2006–2011). Available at `http://www.coopers-ip.eu/index.php?id=2`. Accessed July 2013.
5. HART Communication Foundation. Available at `http://www.hartcomm.org/hcf/aboutorg/aboutorg.html`. Accessed July 2013.
6. National Institute of Standards and Technology (NIST). Available at `http://www.nist.gov/`. Accessed July 2013.
7. Wi-Fi Alliance. Available at `http://www.wi-fi.org/`. Accessed July 2013.
8. CVIS project (2006–2010). Available at `http://www.cvisproject.org`. Accessed July 2013.
9. ISA 100.11a 2011 standard. Wireless systems for industrial automation: Process control and related applications, ISA-100, 2011.
10. IEEE 802.11p published standard. IEEE Standard for Information Technology—Local and metropolitan area networks—Specific requirements—Part 11: Wireless LAN medium access control (MAC) and physical layer (PHY) Specifications Amendment 6: Wireless Access in Vehicular Environments.

IEEE Std 802.11p-2010 (Amendment to IEEE Std 802.11-2007 as amended by IEEE Std 802.11k-2008, IEEE Std 802.11r-2008, IEEE Std 802.11y-2008, IEEE Std 802.11n-2009, and IEEE Std 802.11w-2009), pp. 1–51, 2010.

11. N. Abramson. The ALOHA system: Another alternative for computer communications. In *Proceedings of the November 17–19, 1970, Fall Joint Computer Conference*, pp. 281–285. ACM, New York, 1970.
12. N. Abramson. Development of the ALOHANET. *IEEE Transactions on Information Theory*, 31(2):119–123, 1985.
13. I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci. A survey on sensor networks. *IEEE Communications Magazine*, 40(8):102–114, 2002.
14. L. Al-Kanj and Z. Dawy. Offloading wireless cellular networks via energy-constrained local ad hoc networks. In *IEEE Global Telecommunications Conference (GLOBECOM)*, pp. 1–6, 2011.
15. ZigBee Alliance. Specifications. Available at `http://www.zigbee.org/Specifications.aspx`. Accessed July 2013.
16. T. Anwar, C. Jones, D. Schreib, and G. Strauch. Mobile PR-network in a densely populated urban environment. In *Proceedings of the Global Telecommunications Conference, 1990, and Exhibition. 'Communications: Connecting the Future' (GLOBECOM)*, pp. 1574–1578, 1990.
17. K. Ashton. That 'Internet of things' thing. *RFID Journal*, 22:97–114, 2009.
18. ASTM. ASTM E2213—03(2010) Standard specification for telecommunications and information exchange between roadside and vehicle systems—5 ghz band dedicated short range communications (DSRC) medium access control (MAC) and physical layer (PHY) specifications (2003). Available at `http://www.astm.org/Standards/E2213.htm`. Accessed July 2013.
19. S. Basagni, M. Conti, S. Giordano, and I. Stojmenovic. *Mobile Ad Hoc Networking*. Wiley, San Francisco, 2004.
20. I. Chlamtac, M. Conti, and J.-N. Liu. Mobile ad hoc networking: Imperatives and challenges. *Ad Hoc Networks*, 1:13–64, 2003.
21. C-Y. Chong and S. P. Kumar. Sensor networks: Evolution, opportunities, and challenges. *Proceedings of the IEEE*, 91(8):1247–1256, 2003.
22. HART field communication protocol specification, revision 7.0, September 2007. Available at http://www.hartcomm.org. Accessed February 2014.
23. Federal Communications Commission. FCC News. Available at `http://transition.fcc.gov/Bureaus/Engineering\_Technology/News\_Releases/1999/nret9006.html` (1999). Accessed July 2013.
24. CAR 2 CAR communication consortium manifesto, version 1.1. Overview of the C2C-CC system, 2007. Available at http://elib.dlr.de/48380/1/C2C-CC_manifesto_v1.1.pdf. Accessed February 2014.
25. W. Dabbous and C. Huitema. PROMETHEUS: Vehicle to vehicle communications. Technical report, Research report. INRIA-Renault Collaboration, INRIA, France, 1988.

26. M. M. Davis and M. Baldwin. An intercommunication system for the surgical operating room. In *1956 IRE National Convention*, pp. 24–28. New York, 1956.
27. F. Davoli, A. Giordano, and S. Zappatore. Architecture and protocol design for a car-to-infrastructure packet radio network. In *Proceedings of the Global Telecommunications Conference, 1990, and Exhibition. "Communications: Connecting the Future" (GLOBECOM)*. IEEE, Vol. 3, pp. 1579–1585, 1990.
28. V. Dyo and C. Mascolo. Adaptive distributed indexing for spatial queries in sensor networks. In *Proceedings of the 16th International Workshop on Databases and Expert Systems Applications*, pp. 1103–1107, 2005.
29. M. R. Friedberg. Mobile antennas for vehicular communications. *Transactions of the IRE Professional Group on Vehicular Communications*, 1(1):100–104, 1952.
30. W. J. Gillan. PROMETHEUS and DRIVE: Their implications for traffic managers. In *Proceedings of the Vehicle Navigation and Information Systems Conference, 1989. Conference Record*, pp. 237–243, 1989.
31. D. Gislason, Ed. *Zigbee Wireless Networking*. Elsevier, 2008.
32. J. C. Haartsen. The Bluetooth radio system. *IEEE Personal Communications*, 7(1):28–36, 2000.
33. E. A. Hanysz, C. E. Quinn, J. E. Stevens, and W. G. Trabold. DAIR—A new concept in highway communications for added safety and driving convenience. In *Proceedings of the 17th IEEE Vehicular Technology Conference*, Vol. 17, pp. 108–120, 1966.
34. H. Hartenstein and K. Laberteaux, Ed. *VANET Vehicular Applications and Inter-Networking Technologies*. Wiley, Hoboken, 2009.
35. J.-P. Hubaux, J.-Y. Le Boudec, S. Giordano, and M. Hamdi. The Terminode project: Towards mobile ad-hoc WANs. In *Proceedings of the IEEE International Workshop on Mobile Multimedia Communications*, pp. 124–128. San Diego, 1999.
36. International Society of Automation. ISA100 wireless standard. Available at `http://www.isa100wci.org/`. Accessed July 2013.
37. ISA. International Society of Automation. Available at `http://www.isa.org/`. Accessed July 2013.
38. J. G. Jetcheva, Y.-C. Hu, S. PalChaudhuri, A. K. Saha, and D. B. Johnson. Design and evaluation of a metropolitan area multitier wireless ad hoc network architecture. In *Proceedings of the IEEE Workshop on Mobile Computing Systems and Applications*, pp. 32–43, 2003.
39. E. E. Johnson, T. Zibin, M. Balakrishnan, Z. Huiyan, and S. Sreepuram. Routing in HF ad-hoc WANs. In *Proceedings of the IEEE Military Communications Conference (MILCOM)*, Vol. 2, pp. 1040–1046, 2004.
40. D. B. Johnsort. Routing in ad hoc networks of mobile hosts. In *Proceedings of the First Workshop on Mobile Computing Systems and Applications*, pp. 158–163, 1994.

41. J. Jubin and J. D. Tornow. The DARPA Packet Radio Network Protocols. *Proceedings of the IEEE*, 75:21–32, 1987.
42. J. M. Kahn, R. H. Katz, and K. S. J. Pister. Next century challenges: Mobile networking for "Smart Dust." In *Proceedings of the 5th Annual ACM/IEEE International Conference on Mobile Computing and Networking*, pp. 271–278. ACM, New York, 1999.
43. R. Kahn. The organization of computer resources into a packet radio network. *IEEE Transactions on Communications*, 25:177–186, 1977.
44. J. B. Kenney. Dedicated short-range communications (DSRC) standards in the United States. *Proceedings of the IEEE*, 99(7):1162–1182, 2011.
45. K. P. Laberteaux, R. Sengupta, C.-N. Chuah, and D. Jiang, Eds. *Proceedings of the First International Workshop on Vehicular Ad Hoc Networks, Philadelphia, PA, USA*. ACM, New York, 2004.
46. J. R. Lundien and H. Nikodem. A mathematical model for predicting microseismic signals in terrain materials. Technical Report M-73-4. U.S. Army Engineer Waterways Experiment Station, 1973.
47. R. S. Mackay. Radio telemetering from within the human body. *IRE Transactions on Medical Electronics*, ME-6(2):100–105, 1959.
48. R. S. Mackay and B. Jacobson. Endoradiosonde. *Nature*, 179:1239–1940, 1957.
49. S. A. Mohammad, A. Rasheed, and A. Qayyum. VANET architectures and protocol stacks: A survey. In T. Strang, C. R. Garcia, A. Festag, A. Vinel, and R. Mehmood, Eds., *Proceedings of the Third International Conference on Communication Technologies for Vehicles*, Nets4Cars/Nets4Trains'11, pp. 95–105. Springer-Verlag, Berlin, 2011.
50. J. M. Mounce. Human factors requirements for real-time motorist information displays. Technical Report DOT-11-8505. Texas Transportation Institute, Texas A&M University, College Station, Texas, 1978.
51. National Institute of Standards and Technology (NIST). IEEE 1451 family of standards. Available at `http://www.nist.gov/el/isd/ieee/ieee1451.cfm`. Accessed July 2013.
52. Visual networking index. Cisco forecast. Available at `http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/white\paper\c11-520862.html`. Accessed July 2013.
53. S. Petersen and S. Carlsen. WirelessHart versus ISA100.11a: The format war hits the factory floor. *IEEE Industrial Electronics Magazine*, 5:23–34, 2011.
54. Geonet Project. D 1.2 final geonet architecture design, 2010.
55. Research and Innovative Technology Administration (Rita). Intelligent Transportation Systems. IEEE 1609—Family of Standards for Wireless Access in Vehicular Environments (WAVE) (Sept. 2009). Available at `http://www.standards.its.dot.gov/fact_sheet.asp?f=80`. Accessed July 2013.

56. N. Ristanovic, J-Y. Le Boudec, A. Chaintreau, and V. Erramilli. Energy efficient offloading of 3G networks. In *Proceedings of the Eighth IEEE International Conference on Mobile Ad-Hoc and Sensor Systems (MASS)*, pp. 202–211, 2011.
57. DSRC Committee. SAE Draft Std. J2945.1, Revision 2.2, SAE International. Draft DSRC minimum performance requirements—Basic safety messages for vehicle safety applications, 2011.
58. M. Schwartz and N. Abramson. The AlohaNet—Surfing for wireless data [history of communications]. *IEEE Communications Magazine*, 47(12): 21–25, 2009.
59. Z. Shelby and C. Bormann. *6LoWPAN: The Wireless Embedded Internet*. Wiley, Hoboken, 2009.
60. E. Y. Song and K. Lee. Understanding IEEE 1451—Networked smart transducer interface standard—What is a smart transducer? *IEEE Instrumentation Measurement Magazine*, 11(2):11–17, 2008.
61. Special Interest Group (SIG). Bluetooth. Available at `https://www.bluetooth.org/apps/content/`. Accessed July 2013.
62. ITS Standards. CALM Standards for ITS (Nov. 2009). Available at `http://its-standards.info/Feeds/21217Intro.html`. Accessed July 2013.
63. ITS Standards. Communications in Cooperative Intelligent Transport Systems—CALM for C-ITS. Available at `http://calm.its-standards.info/`. Accessed July 2013.
64. Facebook statistics. Available at `http://newsroom.fb.com/content/default.aspx?NewsAreaId=22`. Accessed July 2013.
65. Twitter statistics. Available at `http://blog.twitter.com/2012/03/twitter-turns-six.html`. Accessed July 2013.
66. SAE Std. J2735. SAE International. Dedicated short-range communications (DSRC) message set dictionaty (2009). Available at `http://standards.sae.org/j2735_200911`. Accessed July 2013.
67. Bluetooth v4.0. Core specification. Available at `http://developer.bluetooth.org/KnowledgeCenter/TechnologyOverview/Pages/v4.aspx`. Accessed July 2013.
68. C. Wewetzer, M. Caliskan, and A. Luebke. The feasibility of a search engine for metropolitan vehicular ad-hoc networks. In *Proceedings of the IEEE Globecom Workshops*, pp. 1–8, 2007.
69. IEEE 802.11 Working Group. IEEE 802.11 timelines (1991). Available at `http://www.ieee802.org/11/Reports/802.11_Timelines.htm`. Accessed July 2013.
70. IEEE 802.15 Working Group. 802.15.4-2011—IEEE standard for local and metropolitan area networks—Part 15.4: Low-Rate wireless personal area networks (LR-WPANss), 2011.

71. C. Yibo, K-M. Hou, H. Zhou, H-L. Shi, X. Liu, X. Diao, H. Ding, J-J. Li, and C. de Vaulx. 6LoWPAN Stacks: A survey. In *Proceedings of the 7th International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM)*, pp. 1–4, 2011.
72. H. Zimmermann. OSI reference model. *IEEE Transactions on Communications*, 28(4):425, 1980.