Chapter 4

Seamless IoT mobile sensing through Wi-Fi mesh networking

Antonio Cilfone[1], Luca Davoli[1], Laura Belli[1], and Gianluigi Ferrari[1]

The research activity in the field of wireless mesh networks (WMNs) has been extremely active in the past years, leading to the design and implementation of different protocols and architectures. Moreover, due to their flexibility, WMNs have often been considered for Internet of things (IoT) applications, in order to provide seamless connectivity in scenarios where traditional infrastructure-based connectivity is not available (e.g., rural or industrial areas). In this chapter, an IoT-oriented mesh infrastructure for WMNs, based on the Better Approach To Mobile Ad-Hoc Networks (B.A.T.M.A.N.) protocol, is presented, with the aim to support mobility of nodes and also to allow the integration of non-mesh IoT nodes, enabling them to access the network and transmit data collected from the environment in a "transparent" way.

4.1 Introduction

In the context of networking, an important role is played by WMNs, in which the nodes can dynamically connect to each other through multi-hop communications. This enables the mobility of the nodes composing the backbone of the WMN itself [1]. Moreover, due to the absence of a static infrastructure, the network topology can evolve: for instance, nodes can be dynamically added, removed, or displaced, still guaranteeing connectivity. Therefore, the network deployment phase is faster and less expensive than that of centralized or infrastructure-based networks. This makes WMNs very attractive for IoT scenarios [2, 3].

The above characteristics highlight how WMNs are one of the more flexible and scalable networks approached for smart scenarios in large areas (e.g., smart agriculture

[1]Department of Engineering and Architecture, University of Parma, Parco Area delle Scienze, Parma, Italy

monitoring [4, 5]). In fact, over the past years, the potential of WMNs has continuously grown, becoming a reality in several scenarios. Thanks to the ease of deployment and scalability, several mesh networks, based on various radio technologies (besides Wi-Fi), have found applications in military, industrial, public safety, surveillance, and distributed sensing scenarios [6–10]. In general, WMNs are attractive when the geographic area that needs to be covered is not easily accessible and/or traditional connectivity strategies are not economically convenient or practically feasible [11].

In this chapter, we describe a WMN where the backbone is composed of different wireless mesh nodes based on IEEE 802.11 standard and on Raspberry Pi (RPi) 3 model B [12] nodes. The network allows external (non-mesh) nodes to join and also supports mobility for both mesh and non-mesh network nodes. The proposed infrastructure, due to its flexibility, can be used in several IoT scenarios to collect data through the use of mobile nodes—equipped with sensors and/or actuators—that move in the monitored area and access the network to transmit collected information or to execute received commands. Each mobile node, implemented using an RPi 3 model B, is not part of the mesh network but uses the mesh backbone as a client and is unaware of the internal organization of the WMN itself. Relying on the approach proposed in [13], the nodes composing the backbone of the WMN have two different IEEE 802.11 interfaces in order to separate the backbone tier from the network access tier. Moreover, the B.A.T.M.A.N. version IV routing algorithm [14], which is natively available in the Linux kernel, has been chosen to route the traffic inside the backbone network. This algorithm has been developed by the German Freifunk community to overcome the limitation of the optimized link state routing protocol [15] and is specifically designed to fit WMN scenarios.

The rest of this chapter is organized as follows. In Section 4.2, a background describing the most relevant protocols and standards adopted in building mesh networks is provided. Section 4.3 is devoted to the detailed description of the proposed WMN implementation and a preliminary experimental setup. Finally, in Section 4.4 we draw our conclusions, highlighting possible applications, in the field of IoT, of the proposed architecture.

4.2 Background

4.2.1 IEEE 802.11s basics

The demand for larger wireless infrastructures has led, in the past decade, to the development of an amendment of the IEEE 802.11 standard [16] specifically designed for Wi-Fi mesh networking, denoted as IEEE 802.11 seconds [17], which introduces new frame forwarding and routing capabilities at the MAC layer, together with new inter-networking and security techniques, in order to support mesh capabilities. The IEEE 802.11 seconds standard does not change L1 (PHY layer) of IEEE 802.11 but just modifies L2 (MAC layer). The most important novelty introduced is that the traffic routing is performed at L2 instead of L3

(network layer) so that nodes in the network can have direct knowledge of their "radio neighborhood."

In an IEEE 802.11 seconds mesh network, also named as mesh basic service set (MBSS), there are different logical components. Besides a sufficient number of "mesh stations" (mesh STAs), there are other mesh points (MPs) with augmented functionalities. While one type of enhanced MPs, denoted as mesh Access Points (MAPs), acts as APs for classical IEEE 802.11 stations, there exist other components, denoted as mesh portal points (MPPs), performing as gateways (GWs) toward an external (typically wired) network. Therefore, each entity composing the mesh network relies on a specific ISO/OSI stack implementation. Moreover, only mesh STAs have mesh functionalities (e.g., formation of the MBSS, path selection, and forwarding); thus, a mesh STA is not a member of an independent BSS (IBSS) or an infrastructure BSS, with mesh STAs not directly communicating with non-mesh STAs. In order to enable communication between mesh BSS and other BSSs, in fact, a mesh node can communicate with non-mesh nodes through the distribution system using the *mesh gate*, which is the logical component that enables the integration between mesh BSS and infrastructure BSS. In order to enable also the communication between the mesh BSS and non-IEEE 802.11 local area networks (LANs), such as wired LANs, another logical component is used, namely the *portal*. In the following, we assume that non-mesh nodes can communicate with mesh STAs through the MAPs.

4.2.2 IEEE 802.11s routing algorithm

One of the key aspects of a WMN is the traffic organization process handled by the specific routing protocol chosen for the WMN itself. The goal of that routing protocol is to discover and manage the best routes connecting pairs (or, more generally, groups) of nodes, according to one or more link- or route-based metrics (e.g., hop number, link quality, throughput). Moreover, inside a mesh network, all the devices should use the same path metric and routing protocol and, to this end, IEEE 802.11 seconds defines a default behavior for both, which, however, can be replaced by other custom solutions. The default metric, called "airtime metric," indicates the total cost of a link by taking into account some parameters (such as data rate, overhead, or frame error rate) measured by transmitting a 1 kbyte frame. The default routing algorithm is the hybrid wireless mesh protocol [18], based on the Ad-hoc On-demand Distance Vector protocol [19] combined with a proactive tree-based solution, in which a mesh station (typically acting as MPP) propagates routing messages to all mesh stations in order to establish and maintain the links.

4.2.3 B.A.T.M.A.N.

B.A.T.M.A.N. advanced (batman-adv in the following) is a proactive L2 routing protocol for WMNs and, namely, the "wireless" version of the B.A.T.M.A.N. protocol (originally designed for wired networks), which also supports roaming of mobile nodes [20]. More in detail, it keeps the information about the existence of nodes in the mesh network that are accessible via single-hop or multi-hop communication

links. The batman-adv approach consists in allowing each node to determine, for each destination in the mesh network, its best next-hop, which can be identified as a GW to communicate with the destination node without requiring the knowledge of the complete route. In this way, there is no need for transmitting and keeping information about the whole topology at each node, as each node performs routing independently of the other ones. Therefore, each node needs to keep updated for each destination, the best next-hop; this significantly reduces the amount of control traffic and makes synchronization faster. Therefore, such behavior is similar to that specified by the software-defined networking (SDN) paradigm [21, 22], in detail looking at the data plane, where network nodes do not need to take care of the whole network topology—to be known only by the SDN controller(s) at the control plane and on which all the traffic-related decisions (e.g., based on Traffic Engineering strategies [23, 24]) will be taken.

In the version used in this chapter, B.A.T.M.A.N. IV [25], in order to perform the discovery of its neighbors, every B.A.T.M.A.N.-based node periodically broadcasts an OriGinator message (OGM), corresponding to a 12 byte UDP payload (for a total packet size equal to 52 bytes, including IP and UDP headers). The OGM has relevant information, such as a sequence number which is used to (i) distinguish new OGMs, (ii) guarantee that OGMs are not counted twice, and (iii) discover if a neighbor is a GW toward Internet or not. At the same time, by sending OGMs, each node informs its link-local neighbors about its existence [14].

Having to maintain B.A.T.M.A.N. as light as possible, each B.A.T.M.A.N.-based packet is encapsulated into a single UDP packet and consists of an OGM and zero or more attached Host Network Announcement (HNA) messages—HNA is a message type used to announce a GW to a network. The formats of the OGM and the HNA message are shown in Figure 4.1a and b, respectively.

As the default path metric, B.A.T.M.A.N. uses the transmission quality (TQ) metric, based on expected transmission count [26], to find a trade-off between a short (in terms of hops) route and a (potentially) long route with good links. During

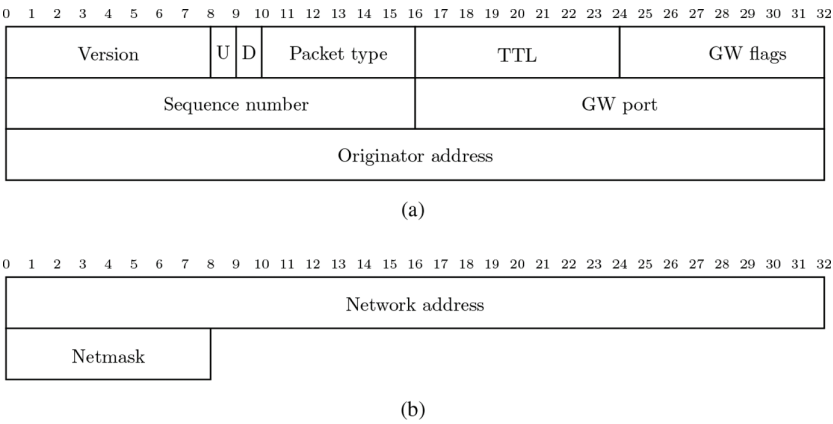

Figure 4.1 Packet formats: (a) OGM message and (b) HNA message

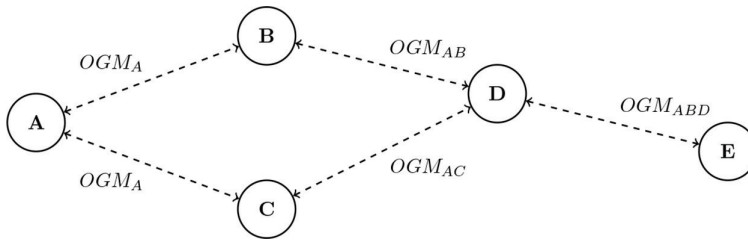

Figure 4.2 OGM rebroadcasting process

OGMs' broadcasting, a node also counts the OGMs received from a given neighbor: this value is denoted as receive quality (RQ) and its calculation takes place considering a sliding window of 64 bits (which leads to 2^{64} possible entries). The sliding window keeps track of the last received sequence numbers of OGMs and the current received from each node in the network. The in-window sequence numbers are those that fit in the window below the current sequence number. If an out-of-range sequence number is received, it is set as the current sequence number and the sliding window is moved accordingly. Sequence numbers that are no longer in the sliding window are deleted. Neighbors rebroadcast received OGMs so that nodes more than one hop away get information about the existence of far nodes, as shown in Figure 4.2. In order to avoid overcrowding the network, each node resends only OGMs received from its neighbor with the best TQ metric.

In particular, a B.A.T.M.A.N.-enabled node evaluates the TQ metric of a generic neighbor *i* as the fraction of its OGMs that are correctly received by this neighbor as follows:

$$\mathrm{TQ} = \frac{\mathrm{EQ}}{\mathrm{RQ}} \tag{4.1}$$

where echo quality (EQ) corresponds to the number of received broadcasts of its own messages within the sliding window. Finally, the best hop is determined by applying penalties for asymmetric links and taking into account the number of hops needed to reach the destination node.

4.3 Mesh network implementation

Our goal is to carry out an experimental evaluation of a WMN which (i) relies on a mesh backbone composed of B.A.T.M.A.N.-based nodes, (ii) allows the integration of non-B.A.T.M.A.N.-enabled devices as external clients that communicate with both mesh and non-mesh nodes, and (iii) allows the mobility of these external clients. In the proposed IoT-like architecture, the mobile nodes are non-B.A.T.M.A.N. devices—in detail, based on RPi boards—equipped with sensors or actuators and aiming at collecting data or executing commands using the WMN infrastructure to send and receive information. Moreover, the MPP and MAPs are implemented using an RPi 3 board, which embeds a Quad Core @ 1.2 GHz Linux-based Single-Board Computer with 1 GB RAM and on-board IEEE 802.11b/g/n interface.

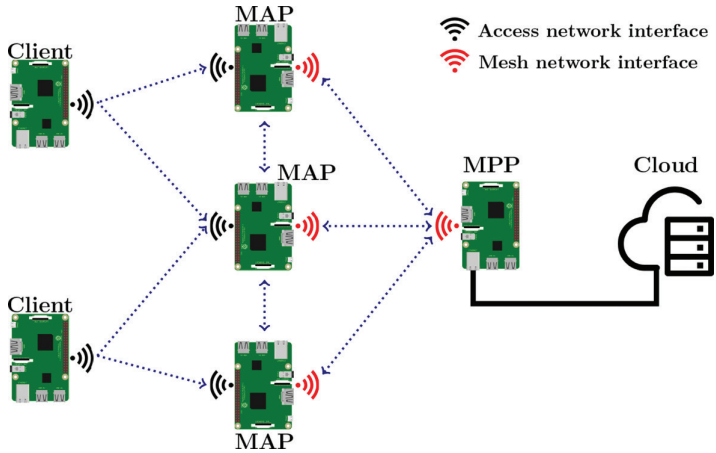

Figure 4.3 Multi-hop mesh network architecture

Focusing on the network topology, the overall IoT architecture is composed of two network tiers: the B.A.T.M.A.N.-based mesh backbone network, composed of four MAPs and one MPP; and a set of non-B.A.T.M.A.N.-based (namely, mesh-unaware) client nodes which can be used to collect data of interest from the deployment environment.

4.3.1 Proposed mesh backbone network

The backbone network, as shown in Figure 4.3, is composed of an MPP and one or more MAPs, all implemented on top of RPi boards. The MPP, acting as a GW, is the only node with a direct connection to the Internet (through an Ethernet cable) and has a single wireless interface, denoted as bat0, which is reserved to execute B.A.T.M.A.N. and to build the backbone network among all MAPs.

MAPs, instead, are "completely wireless" nodes equipped with the built-in IEEE 802.11 interface and an external IEEE 802.11 dongle—in other words, they have two IEEE 802.11 interfaces. Moreover, since a key goal of the proposed architecture is the support of the roaming functionality of a mobile node among the backbone nodes, the MPP is the only node running a DHCP server, whose aim is to distribute IP addresses to mesh-unaware nodes, *regardless* of their connection point. More in detail, the IP addresses' distribution is carried out through the presence of some specific daemons, namely *DHCP relays*, running on the access interface of the MAPs. In this way, when a new client joins the network and asks for an IP address, the request is forwarded to the MPP, which releases a new IP address and sends it back to the requester. In Table 4.1, the network configurations of a B.A.T.M.A.N. MPP and a generic MAP are shown, with reference to IP classes in which they are reachable and the services that will run on their network interfaces.

In order to enable connectivity to external mobile clients, each MAP node runs (i) a hostapd daemon on its wlan1 interface, turning this network interface

Table 4.1 Backbone mesh network configuration

	Interface	Network	IP Class	Services
MPP	eth0	LAN	192.168.1.0/24	
	bat0	Mesh	192.168.3.0/24	DHCP server, batctl
MAP	bat0	Mesh	192.168.4.0/24	DHCP relay, batctl
	wlan1	Access	192.168.2.1	hostapd

into an AP and an authentication server, and (ii) a DHCP relay, operating through the dhcp-helper daemon, which is used to dynamically assign IP addresses to external clients. Furthermore, the DHCP requests are forwarded from wlan1 to the bat0 interface and, once the request reaches bat0, it is finally sent to the DHCP server following the proper multi-hop route foreseen by the B.A.T.M.A.N. protocol. More in detail:

- the DHCP client broadcasts the packets in the subnet 192.168.2.0/24 generated through the *hostapd* daemon;
- the DHCP relay agent receives the broadcast and transmits it to the DHCP server(s) using a unicast transmission, thus being able to route the DHCP request to other DHCP servers not strictly in the same local network;
- the DHCP relay agent stores its own IP address in the giaddr field of the DHCP packet, as shown in Figure 4.4, and specifies, through the option82 field [27], that the request is coming from the subnet 192.168.2.0/24 in such a way that the DHCP server can lease the proper address.

As previously introduced, in the proposed B.A.T.M.A.N.-based mesh network, external nodes, potentially mobile, can use the mesh backbone as external clients,

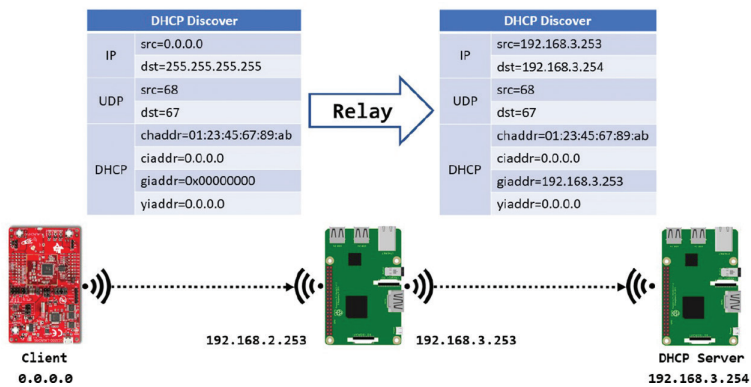

Figure 4.4 DHCP relay message exchange

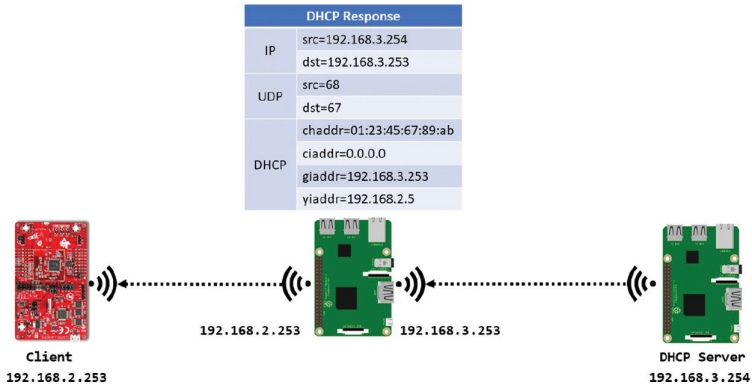

Figure 4.5 DHCP response

in order to reach the Internet or communicate with other nodes. In the proposed architecture, these nodes have to simply connect to the Wi-Fi network generated through the wlan1 interface of the nearest MAP. Due to the presence of DHCP management functionalities, external B.A.T.M.A.N.-unaware clients are able to connect in a seamless way, without performing any additional configuration or installing specific software.

The main fields of the DHCP messages are the following:

- chaddr, containing the MAC address of the client requesting the IP address;
- ciaddr, containing the IP address of the client, which is 0.0.0.0 in the case that the client has no IP address;
- giaddr, containing the IP address of the GW, namely the DHCP agent relaying requests from the client;
- yiaddr, containing the IP address leased for the client.

The most relevant fields are chaddr and giaddr, which are used to forward the DHCP requests and the DHCP responses in a proper way. In particular, a MAP uses the chaddr to understand which client is the destination of the DHCP response containing the leased IP address. The DHCP server uses the giaddr to determine the subnet from which the DHCP relay agent received the broadcast, then allocates an IP address to this subnet. When the DHCP server replies to the client, it sends the reply to the giaddr address, again using a unicast transmission, as shown in Figure 4.5. The message is then routed to the correct node, eventually following a multi-hop route. Then, the DHCP relay agent retransmits the response to the local network.

In order to properly route the traffic arriving from external non-mesh clients, as well as to allow them to connect to the Internet, the following routing rules have been defined for MPP and MAPs.

With regard to the MPP:

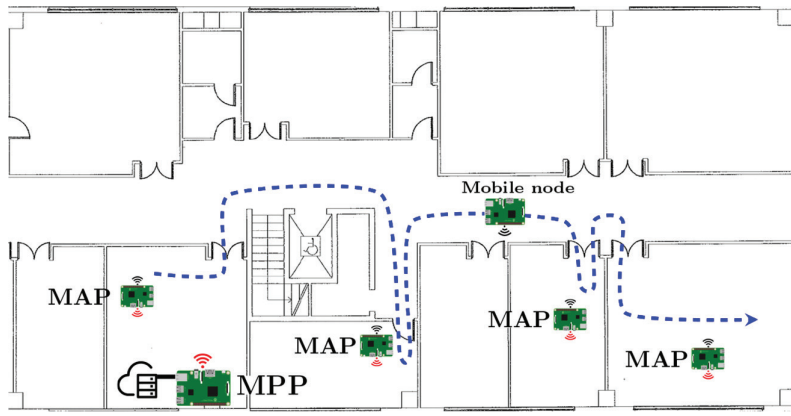

Figure 4.6 *Experimental setup scenario. The B.A.T.M.A.N. interfaces are represented in red color, while regular wireless interfaces are represented in black.*

- the traffic outgoing to the wired network (through eth0) is NATted, flowing outside the wireless network with only one public IP address, namely the IP address of the eth0 interface statically assigned by the network administrator;
- the traffic coming from bat0 is sent to eth0;
- the traffic coming from eth0 is sent to bat0 only for already established traffic flows.

With regard to the MAPs:

- the traffic outgoing to the backbone with source address 192.168.2.0/24 is sent through bat0 and is NATted in order to flow outside with only one IP address, namely the IP address of the bat0 interface of the considered MAP;
- all the traffic coming from wlan1 to bat0 is accepted;
- the traffic coming from bat0 and with destination address 192.168.2.0/24 is accepted only for already established traffic flows;

In order to test the performance of the proposed IoT mesh architecture, some connection tests have been performed in an indoor environment, as shown in Figure 4.6. More in detail, the experimental setup includes six double-interface Wi-Fi nodes, deployed in different rooms of the building and configured as follows:

- one MPP node connected to the Internet through the eth0 and a B.A.T.M.A.N. interface, to communicate with the mesh backbone;
- four MAP nodes, each one located in a different room;
- one mobile node moving on a path that enters and exits from all the 4 covered rooms.

The described deployment has been chosen to experimentally verify the roaming activity of the mobile node, which can thus connect to the network in a seamless and transparent way (as well as it happens, on high layers, to IoT nodes joining Web of Things contexts [28]) and be completely unaware of the mesh network infrastructure existing "behind the surface" of the publicly available Wi-Fi network.

4.4 Conclusions and application scenarios

In this chapter, we have proposed a WMN architecture based on the B.A.T.M.A.N. protocol, supporting the integration of non-B.A.T.M.A.N. external mobile clients for seamless IoT mobile sensing. In detail, the proposed mesh backbone allows external mesh-unaware clients to connect and send their collected data toward Wi-Fi clients in a transparent way, thus allowing to extend the normal Wi-Fi coverage with a multi-hop approach. To this end, the first experimental results obtained with a preliminary setup (composed of six IoT nodes) in an indoor environment seem to be promising, highlighting the flexibility of the proposed approach. Therefore, this mesh-oriented architecture seems to be suitable for several IoT applications, where traditional connectivity strategies are not employable or not economically suitable.

Looking at alternative scenarios in which such a mesh-oriented architecture may fit and be useful for extending the coverage from indoor to outdoor contexts, one example can involve the smart agriculture and rural areas-monitoring scenarios. To this end, IoT-like technologies and paradigms are nowadays rising a certain interest from different "players" in this field (e.g., technology developers, system integrators, and farmers) and is used for real-time data collection and actuation, as shown in Figure 4.7. Therefore, farmers can make conscious decisions on the basis of data sensed from their agricultural fields (e.g., soil temperature and humidity, wind speed, soil moisture, pH value [29]). Then, due to their geographical extension and the presence of natural obstacles, in rural areas, the deployment of a WMN can be the best solution to provide connectivity. Moreover, in order to reduce infrastructure costs, the use of mobile nodes (such use drones [30], as shown in Figure 4.8) to periodically perform environmental data collection campaigns and surveillance activities in the monitored area, joining the mesh network as a mobile external client, can represent another example fitting the characteristics of these networks. Finally, other possible mobile nodes can be represented by tractors, animals, or other entities that need to be monitored.

Another relevant scenario that can take advantage of the proposed architecture involves smart industries and smart infrastructures. In particular, our approach can be

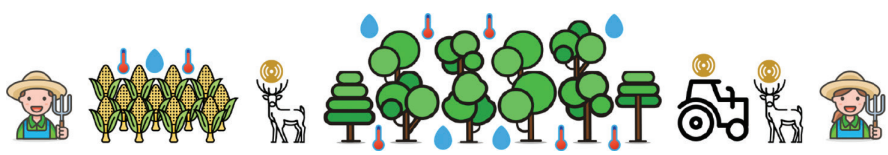

Figure 4.7 Smart agriculture application scenario

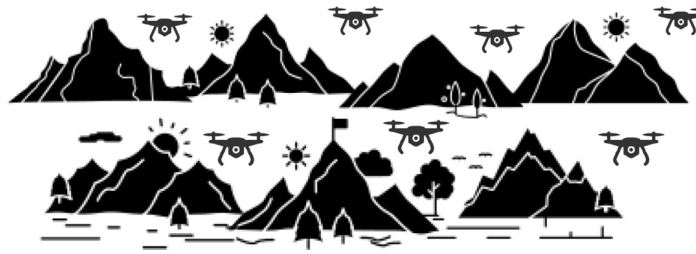

Figure 4.8 Application scenario involving flying drones communicating and collecting data from the environment

beneficial for all those large industrial environments where, due to their geographical peripheral position, as well as the presence of obstacles, it is not possible to rely on cellular networks or standard Wi-Fi connectivity, as well as on the adoption of alternative long-range low data-rate wireless protocols (e.g., LoRa and LoRaWAN). Therefore, as shown in Figure 4.9, the possibility to deploy the proposed WMN network can allow a data collection in different manufacturing areas, through both fixed nodes (e.g., sensors linked to machines) and mobile nodes (e.g., industrial vehicles moving inside the manufacturing plants and environments). Finally, the dataset built from these monitoring campaigns can then be used to perform high-level activities based on these data, such as predictive maintenance, failure prevention, quality control, and so on.

Finally, on the basis of the heterogeneity of the illustrative reference scenarios and contexts, it would be interesting to analyze how such mesh-oriented environments would evolve in the presence of a large amount of involved (mesh-aware and non-mesh) devices (e.g., through network emulators [31–33]), as well as analyzing the data generated by them (to be processed locally or outsourced to external entities through Edge and Cloud Computing paradigms [34, 35]).

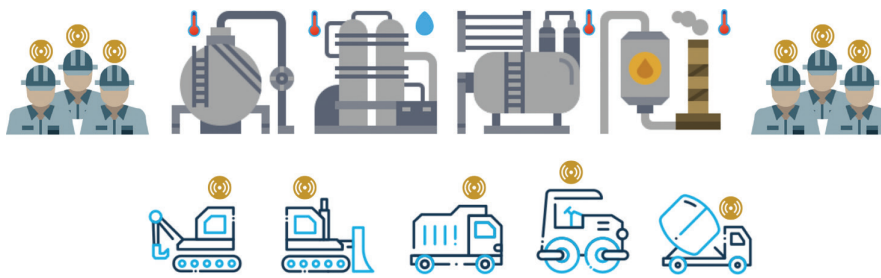

Figure 4.9 Smart industry application scenario

Acknowledgments

This work received funding from the European Union's Horizon 2020 research and innovation program ECSEL Joint Undertaking (JU) under grant agreements: No. 783221, AFarCloud project—"Aggregate Farming in the Cloud;" No. 876038, InSecTT project—"Intelligent Secure Trustable Things;" No. 876019, ADACORSA project—"Airborne Data Collection on Resilient System Architectures." The work of Luca Davoli was also partially funded by the University of Parma, under "Iniziative di Sostegno alla Ricerca di Ateneo" program, "Multi-interface IoT sYstems for Multi-layer Information Processing" (MIoTYMIP) project. The JU received support from the European Union's Horizon 2020 research and innovation program and the nations involved in the mentioned projects. The work reflects only the authors' views; the European Commission is not responsible for any use that may be made of the information it contains.

References

[1] Zhang Y., Luo J., Hu H. *Wireless Mesh Networking: Architectures, Protocols and Standards*. Boca Raton: Auerbach Publications; 2007.

[2] Liu Y., Tong K.F., Qiu X., Liu Y., Ding X. 'Wireless mesh networks in IoT networks'. 2017 International Workshop on Electromagnetics: Applications and Student Innovation Competition; 2017. pp. 183–5.

[3] Belli L., Cirani S., Davoli L. 'Design and deployment of an IoT application-oriented testbed'. *Computer*. 2015;48(9):32–40.

[4] Aliev K., Moazzam M., Narejo S., Pasero E., Pulatov A. 'Internet of plants application for smart agriculture'. *International Journal of Advanced Computer Science and Applications*. 2018;9(4).

[5] Codeluppi G., Cilfone A., Davoli L., Ferrari G. 'VegIoT garden: a modular IoT management platform for urban vegetable gardens'. 2019 IEEE International Workshop on Metrology for Agriculture and Forestry (MetroAgriFor); 2019. pp. 121–6.

[6] Moore J.P.T., Bagale J.N., Kheirkhahzadeh A.D., Komisarczuk P. 'Fingerprinting seismic activity across an Internet of things'. 2012 5th International Conference on New Technologies, Mobility and Security (NTMS); 2012. pp. 1–6.

[7] Han K., Zhang D., Bo J., Zhang Z. 'Hydrological monitoring system design and implementation based on IOT'. *Physics Procedia*. 2012;33:449–54.

[8] Belli L., Davoli L., Medioli A., Marchini P.L., Ferrari G. 'Toward industry 4.0 with IoT: optimizing business processes in an evolving manufacturing factory'. *Frontiers in ICT*. 2019;6:17.

[9] Andrés G.R.C. 'CleanWiFi: the wireless network for air quality monitoring, community internet access and environmental education in smart cities'. 2016 ITU Kaleidoscope: ICTs for a Sustainable World (ITU WT); 2016. pp. 1–6.

[10] Kandhalu A., Rowe A., Rajkumar R., Huang C., Yeh C.-C. 'Real-time video surveillance over IEEE 802.11 mesh networks'. 15th IEEE Real-Time and Embedded Technology and Applications Symposium; 2009. pp. 205–14.

[11] Cilfone A., Davoli L., Belli L., Ferrari G. 'Wireless mesh networking: an IoT-oriented perspective survey on relevant technologies'. *Future Internet*. 2019;11(4):99.

[12] Raspberry Pi 3 Model B [online]. 2021. Available from https://www.raspberrypi.org/products/raspberry-pi-3-model-b/ [Accessed 25 Jun 2021].

[13] Davoli L., Cilfone A., Belli L., Ferrari G. 'Design and experimental performance analysis of a B.A.T.M.A.N.-based double Wi-Fi interface mesh network'. *Future Generation Computer Systems*. 2019;92(3):593–603.

[14] Neumann A., Aichele C., Lindner M., Wunderlich S. *Better approach to mobile ad-hoc networking (B.A.T.M.A.N.). Internet engineering task Force (IETF) [online]*. 2008. Available from https://datatracker.ietf.org/doc/html/draft-openmesh-b-a-t-m-a-n [Accessed 25 Feb 2022].

[15] Clausen T., Jacquet P. *Optimized link state routing protocol (OLSR). Internet engineering task force (IETF) [online]*. 2003.. Available from https://tools.ietf.org/rfc/rfc3626 [Accessed 25 Feb 2022].

[16] 'IEEE standard for information technology–telecommunications and information exchange between systems local and metropolitan area networks–specific requirements part 11: wireless LAN medium access control (MAC) and physical layer (PHY) specifications'. *IEEE Std 80211-2012*. 2012:1–2793.

[17] 'IEEE standard for information technology–telecommunications and information exchange between systems–local and metropolitan area networks–specific requirements part 11: wireless LAN medium access control (MAC) and physical layer (PHY) specifications Amendment 10: mesh networking'. *IEEE Std 80211s-2011*; 2011. pp. 1–372.

[18] Bari S.M.S., Anwar F., Masud M.H. 'Performance study of hybrid wireless mesh protocol (HWMP) for IEEE 802.11s WLAN mesh networks'. 2012 International Conference on Computer and Communication Engineering (ICCCE); 2012. pp. 712–16.

[19] Perkins C., Belding-Royer E., Das S. *Ad hoc on-demand distance vector (AODV) routing. Internet engineering task force (IETF) [online]*. 2003. Available from https://tools.ietf.org/rfc/rfc3561.

[20] Quartulli A., Lo Cigno R. *Client announcement and fast* roaming in a layer-2 mesh network [online]. DISI-11-472. University of Trento: Department of Information Engineering and Computer Science; 2011. Available from http://eprints.biblio.unitn.it/2269/1/report.pdf [Accessed 25 Feb 2022].

[21] Davoli L., Veltri L., Ventre P.L., Siracusano G., Salsano S. 'Traffic engineering with segment routing: SDN-based architectural design and open source implementation'. 2015 Fourth European Workshop on Software Defined Networks (EWSDN); IEEE; 2015. pp. 111–12.

[22] Seppänen K., Kilpi J., Suihko T. '*Integrating WMN based mobile backhaul with SDN control*' in Giaffreda R., Cagáňová D., Li Y., Riggio R., Voisard A.

(eds.). *Internet of Things. IoT Infrastructures*. Cham: Springer International Publishing; 2015. pp. 222–33.

[23] Huang H., Li P., Guo S., Zhuang W. 'Software-defined wireless mesh networks: architecture and traffic orchestration'. *IEEE Network*. 2015;29(4):24–30.

[24] Salsano S., Veltri L., Davoli L., Ventre P.L., Siracusano G. 'PMSR–poor man's segment routing, a minimalistic approach to segment routing and a traffic engineering use case'. 2016 IEEE/IFIP Network Operations and Management Symposium (NOMS); 2016. pp. 598–604.

[25] Better Approach To Mobile Ad-hoc Networking (B.A.T.M.A.N.) IV [online]. 2021. Available from https://www.open-mesh.org/projects/batman-adv/wiki/BATMAN_IV [Accessed 25 Jun 2021].

[26] De Couto D.S.J., Aguayo D., Bicket J., Morris R. 'A high-throughput path metric for multi-hop wireless routing'. Proceedings of the 9th Annual International Conference on Mobile Computing and Networking. MobiCom '03; New York, NY, USA: ACM; 2003. pp. 134–46.

[27] Droms R.E., Lemon T. *The DHCP Handbook*. 2nd ed. Pearson Education; 2002.

[28] Davoli L., Belli L., Cilfone A., Ferrari G. 'Integration of Wi-Fi mobile nodes in a web of things testbed'. *ICT Express*. 2016;2(3):96–9. Special Issue on ICT Convergence in the Internet of Things (IoT).

[29] Codeluppi G., Cilfone A., Davoli L., Ferrari G. 'LoRaFarM: a LoRaWAN-based smart farming modular IoT architecture'. *Sensors*. 2020;20(7):2028.

[30] Davoli L., Pagliari E., Ferrari G. 'Hybrid LoRa-IEEE 802.11s opportunistic mesh networking for flexible UAV swarming'. *Drones*. 2021;5(2):26.

[31] Beuran R., Nguyen L.T., Miyachi T., *et al.* 'QOMB: a wireless network emulation testbed'. IEEE Global Telecommunications Conference; Honolulu, HI, USA, 30 Nov; 2009. pp. 1–6.

[32] Davoli L., Protskaya Y., Veltri L. 'NEMO: a flexible Java-based network emulator'. 2018 26th International Conference on Software, Telecommunications and Computer Networks (SoftCOM); 2018. pp. 1–6.

[33] Jovanović N., Zakić A., Veinović M. 'VirtualMeshLab: virtual laboratory for teaching wireless mesh network'. *Computer Applications in Engineering Education*. 2016;24(4):567–76.

[34] Belli L., Cirani S., Davoli L. 'An open-source cloud architecture for big stream IoT applications' in Žarko I.P., Pripužić K., Serrano M. (eds.). *Interoperability and Open-Source Solutions for the Internet of Things: International Workshop, FP7 OpenIoT Project, Held in Conjunction with Soft- COM 2014, Split, Croatia*. Springer International Publishing; 2014. pp. 73–88.

[35] Yi X., Liu F., Liu J., Jin H. 'Building a network highway for big data: architecture and challenges'. *IEEE Network*. 2014;28(4):5–13.