International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Q.3060

(12/2020)

SERIES Q: SWITCHING AND SIGNALLING, AND ASSOCIATED MEASUREMENTS AND TESTS

Signalling requirements and protocols for the NGN – Network signalling and control functional architecture

Signalling architecture of fast deployment emergency telecommunication networks to be used in a natural disaster

Recommendation ITU-T Q.3060

ITU-T Q-SERIES RECOMMENDATIONS

SWITCHING AND SIGNALLING, AND ASSOCIATED MEASUREMENTS AND TESTS

SIGNALLING IN THE INTERNATIONAL MANUAL SERVICE	Q.1–Q.3
INTERNATIONAL AUTOMATIC AND SEMI-AUTOMATIC WORKING	Q.4–Q.59
FUNCTIONS AND INFORMATION FLOWS FOR SERVICES IN THE ISDN	Q.60–Q.99
CLAUSES APPLICABLE TO ITU-T STANDARD SYSTEMS	Q.100–Q.119
SPECIFICATIONS OF SIGNALLING SYSTEMS No. 4, 5, 6, R1 AND R2	Q.120–Q.499
DIGITAL EXCHANGES	Q.500–Q.599
INTERWORKING OF SIGNALLING SYSTEMS	Q.600–Q.699
SPECIFICATIONS OF SIGNALLING SYSTEM No. 7	Q.700–Q.799
Q3 INTERFACE	Q.800–Q.849
DIGITAL SUBSCRIBER SIGNALLING SYSTEM No. 1	Q.850–Q.999
PUBLIC LAND MOBILE NETWORK	Q.1000–Q.1099
INTERWORKING WITH SATELLITE MOBILE SYSTEMS	Q.1100–Q.1199
INTELLIGENT NETWORK	Q.1200–Q.1699
SIGNALLING REQUIREMENTS AND PROTOCOLS FOR IMT-2000	Q.1700–Q.1799
SPECIFICATIONS OF SIGNALLING RELATED TO BEARER INDEPENDENT CALL CONTROL (BICC)	Q.1900–Q.1999
BROADBAND ISDN	Q.2000–Q.2999
SIGNALLING REQUIREMENTS AND PROTOCOLS FOR THE NGN	Q.3000–Q.3709
General	Q.3000–Q.3029
Network signalling and control functional architecture	**Q.3030–Q.3099**
Network data organization within the NGN	Q.3100–Q.3129
Bearer control signalling	Q.3130–Q.3179
Signalling and control requirements and protocols to support attachment in NGN environments	Q.3200–Q.3249
Resource control protocols	Q.3300–Q.3369
Service and session control protocols	Q.3400–Q.3499
Service and session control protocols – supplementary services	Q.3600–Q.3616
Service and session control protocols – supplementary services based on SIP-IMS	Q.3617–Q.3639
VoLTE/ViLTE network signalling	Q.3640–Q.3655
NGN applications	Q.3700–Q.3709
SIGNALLING REQUIREMENTS AND PROTOCOLS FOR SDN	Q.3710–Q.3899
TESTING SPECIFICATIONS	Q.3900–Q.4099
PROTOCOLS AND SIGNALLING FOR PEER-TO-PEER COMMUNICATIONS	Q.4100–Q.4139
SIGNALLING REQUIREMENTS AND PROTOCOLS FOR IMT-2020	Q.5000–Q.5049
COMBATING COUNTERFEITING AND STOLEN ICT DEVICES	Q.5050–Q.5069

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T Q.3060

Signalling architecture of fast deployment emergency telecommunication networks to be used in a natural disaster

Summary

Recommendation ITU-T Q.3060 describes the functional elements, services and signalling architecture of emergency telecommunication networks and provides an example of the use of IEEE technologies that can be rapidly deployed in a country affected by a natural disaster.

In the last decade, climate change and natural disasters have affected countries all over the globe. The consequences, such as tropical storms, floods and droughts, directly affect social and various industrial sectors, including information and communication technologies (ICTs).

In this regard, the deployment of a special emergency telecommunication network becomes a first and important aid for civilians afflicted by natural disasters. The rapid deployment of such networks is fundamental.

Currently, the emergency communications systems that are used in natural disasters are based on existing technologies, such as two-way radios, mobile cellular communications and space-based networks (e.g., Iridium). However, in the forthcoming fifth generation (5G) and Internet of things (IoT) era, there are some technologies that may play an important role in helping to provide a wide range of ICT services from simple voice or video communication up to telemetry exchange. All these services, when rapidly deployed in an affected country, may sufficiently change the situation and help to save the lives of victims of natural disasters.

It may be noted that there are many other wireless technologies that may also be deployed to meet such requirements.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Q.3060	2020-12-07	11	11.1002/1000/14413

Keywords

Q.3060,Q,3060.

* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents/software copyrights, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the appropriate ITU-T databases available via the ITU-T website at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Introduction

Climate change and natural disasters affect countries all over the globe. The consequences, such as tropical storms, floods and droughts, directly affect social and various industrial sectors including information and communication technology (ICT).

Recommendation ITU-T Q.3060 describes the signalling architecture of fast deployment emergency telecommunication networks and provide an example of the use of IEEE technologies that may be used in a natural disaster. It may be noted that there are many such networks that may also be deployed to meet such requirements.

Recommendation ITU-T Q.3060

Signalling architecture of fast deployment emergency telecommunication networks to be used in a natural disaster

1 Scope

This Recommendation describes a general framework for fast deployment emergency telecommunication networks (fdETNs) to be used in a natural disaster. It describes different technologies that might be used as a part of such a network including: self-organizing communication technologies (ubiquitous sensor network; USN); unmanned aerial vehicles (UAVs); Internet of things (IoT); and flying ubiquitous sensor network (FUSN). This Recommendation also specifies functional elements of such emergency telecommunication networks and contains requirements for services and protocols.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-R M.2009] Recommendation ITU-R M.2009-2 (2019), *Radio interface standards for use by public protection and disaster relief operations in accordance with Resolution 646 (Rev.WRC-15).*

[ITU-R M.2015] Recommendation ITU-R M.2015-2 (2018), *Frequency arrangements for public protection and disaster relief radiocommunication systems in accordance with Resolution 646 (Rev.WRC-15).*

[ITU-R M.2084] Recommendation ITU-R M.2084-1 (2019), *Radio interface standards of vehicle-to-vehicle and vehicle-to-infrastructure two-way communications for intelligent transport system applications.*

[ITU-R M.2121] Recommendation ITU-R M.2121-0 (2019), *Harmonization of frequency bands for intelligent transport systems in the mobile service.*

[WRC Res. 646] Resolution 646 (Rev.WRC-19), Public protection and disaster relief. In: *World Radiocommunication Conference 2019 (WRC-19) – Final acts,* pp. 440-445. Geneva: International Telecommunication Union. Available [viewed 2021-02-25] at: https://www.itu.int/dms_pub/itu-r/opb/act/R-ACT-WRC.14-2019-PDF-E.pdf

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 Internet of things (IoT) [b-ITU-T Y.4000]: A global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies.

3.1.2 public protection radiocommunication [WRC Res. 646]: Radiocommunications used by agencies and organizations responsible for the maintenance of law and order, protection of life and property and emergency situations.

3.1.3 disaster relief radiocommunication [WRC Res. 646]: Radiocommunications used by agencies and organizations dealing with a serious disruption of the functioning of society, posing a significant widespread threat to human life, health, property or the environment, whether caused by accident, natural phenomena or human activity, and whether developing suddenly or as a result of complex, long-term processes.

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

3G	third Generation
5G	fifth Generation
6LoWPAN	IPv6 over Low-power Wireless Personal Area Network
AC	Access Category
AIFS	Arbitration Inter-Frame Space
BLE	Bluetooth Low Energy
BS	Base Station
CCH	Control Channel
CCHI	CCH Interval
CH	Cluster Head
CM	Cluster Member
CMMpP	Cluster-based Multichannel MAC IEEE 802.11p Protocol
CMP	Cluster Management Protocol
CSMA/CA	Carrier-Sense Multiple Access with Collision Avoidance
CW	Contention Window
DSRC	Dedicated Short-Range Communication
EDCA	Enhanced Distributed Channel Access
FUSN	Flying Ubiquitous Sensor Network
fdETN	fast deployment Emergency Telecommunication Network
GPS	Global Positioning System
ICT	Information and Communication Technology
IMT	International Mobile Telecommunications
InterCP	Inter-cluster Communication Protocol
IntraCP	Intra-cluster Communication Protocol
IoT	Internet of Things
IP	Internet Protocol

IPv6	Internet Protocol version 6
IUDI	Inter-cluster Update Information
LPWAN	Low-Power Wide-Area Network
LTE	Long Term Evolution
LTE-A	LTE Advanced
MAC	Medium Access Control
MBS	Mobile Base Station
NB-IoT	Narrow Band Internet of Things
PAN	Personal Area Network
PHY	Physical Layer
PPDR	Public Protection and Disaster Relief
PSID	Provider Service Identifier
QoS	Quality of Service
SCH	Service Channel
SCHI	SCH Interval
SI	Synchronization Interval
SMS	Short Message Service
ST	Schedule of Transmission
TCS	Telecommunication Control System
TDMA	Time-Division Multiple Access
tUAV	tethered UAV
UAV	Unmanned Aerial Vehicle
UDI	Update Information
UE	User Equipment
USN	Ubiquitous Sensor Network
VANET	Vehicular Ad hoc Network
VoWi-Fi	Voice over Wi-Fi
WAVE	Wireless Access in Vehicular Environment
Wi-Fi	Wireless Fidelity
WiMax	Worldwide interoperability for Microwave access
WLAN	Wireless Local Area Network
WPAN	Wireless Personal Area Network
WSA	WAVE Service Advertisement
WSM	WAVE Short Message

5 Conventions

None.

6 Radio interface technologies for fast deployment emergency telecommunications networks

Various radio interface technologies that may be used to implement fdETNs are identified in [ITU-R M.2009] on radio interface standards applicable for public protection and disaster relief (PPDR). The PPDR concept covers both public protection radiocommunication (defined in clause 3.1.2) and disaster relief radiocommunication (defined in clause 3.1.3). [b-ITU-R M.2291] addresses the use of advanced[1] international mobile telecommunications (IMT) for supporting emergency users with broadband data that can support video and high-speed Internet access and in particular the benefits of using long-term evolution (LTE) technology for emergency telecommunications. [ITU-R M.2015] provides frequency arrangements for PPDR radiocommunication systems in accordance with [WRC Res. 646].

6.1 An example of the architecture of the fast deployment emergency telecommunication network using IEEE standards

This Recommendation covers the architecture of a fast-deployment flying emergency services network in which one or more UAVs are proposed as the flying network, as shown in Figure 6-1. Figure 6-1 shows that communications between the UAVs can be based on [b-IEEE 802.11p], which makes it possible to set up a hierarchical ad hoc wireless network with mobile nodes. Additional information is given in Appendix I.

Figure 6-2 shows the architecture of an aerial emergency network in which one or more UAVs form the flying network. If all telecommunication infrastructure in a given disaster area is destroyed, normal mobile calls are not possible; in that case, the most effective solution is to call via wireless fidelity (Wi-Fi) or voice over Wi-Fi (VoWi-Fi). For this, the entire territory must have Wi-Fi coverage, and an assumption therefore would be made in terms of using the flying network as the remote base station (BS). Each UAV has an on-board heterogeneous gateway as a Wi-Fi router. Communication between UAVs is based on the [b-IEEE 802.11p] protocol. This makes it possible to set up a hierarchical ad hoc wireless network with mobile nodes. The function of subscriber BS will be performed by the Wi-Fi router, which supports [b-IEEE 802.11n] or [b-IEEE 802.11ac]. VoWi-Fi technology allows calls over Wi-Fi. Voice traffic from the subscriber's phone is transmitted over a chain of UAVs based on [b-IEEE 802.11p] to a remote BS [b-IEEE 802.11p] – Internet protocol (IP), where it is processed and sent over the Internet to the telecom operator. All calls are made via the operator's network.

Figure 6-3 shows the UAV hierarchical structure for providing voice services. Since the distance between an endangered person and the position of the emergency services operator is considerable, to ensure communication, many UAVs are required even within the line of sight. It is also worth considering that the signal is transmitted via several relays and due to an increase in network delay, the quality of voice transmission decreases. To improve the quality of service (QoS) and also reduce the required number of UAVs, it is proposed to divide them into two levels. The first consists of the head UAV and the second of UAV members in each group interconnecting with the head UAV. Second-level UAVs interact with subscribers and search for the shortest route to transfer data to the head UAV. A first-level UAV can transmit data to a stationary BS through other head UAVs. Thus, instead of transferring data through all UAVs, the number of intermediate nodes is reduced by introducing two levels of hierarchy.

The role of the mobile base station (MBS) for subscribers will be performed by a Wi-Fi access point on board a UAV, which supports the Wi-Fi standards ([b-IEEE 802.11n], [b-IEEE 802.11ac], [b-IEEE 802.11p]).

---

[1] [b-ITU-R M.2291] addresses the use of IMT-2020 (also commonly known as 5G) for emergency communications.

The connection between the UAV and mobile phones is based on [b-IEEE 802.11n] and [b-IEEE 802.11ac]. Currently, most mobile phones support these technologies. When a mobile phone supports VoWi-Fi mode, it can make calls over Wi-Fi while organizing a flying network with support for these technologies. VoWi-Fi calls are made through the operator with the preservation of numbering and identification of subscribers of the mobile communication network. Voice traffic from the subscriber's phone is transmitted over a chain of UAVs based on [b-IEEE 802.11p] to a remote BS [b-IEEE802.11p] – IP, where it is processed and sent over the Internet to the telecom operator. Communication between the first level UAV head and second level UAV members is based on [b-IEEE 802.11p], which was developed for wireless information transfer between UAVs with the support of self-organization. Communication between the head UAVs in different groups is performed using [b-IEEE 802.11p] technology in advanced mode, within which data can be transmitted over a distance of 750 m.

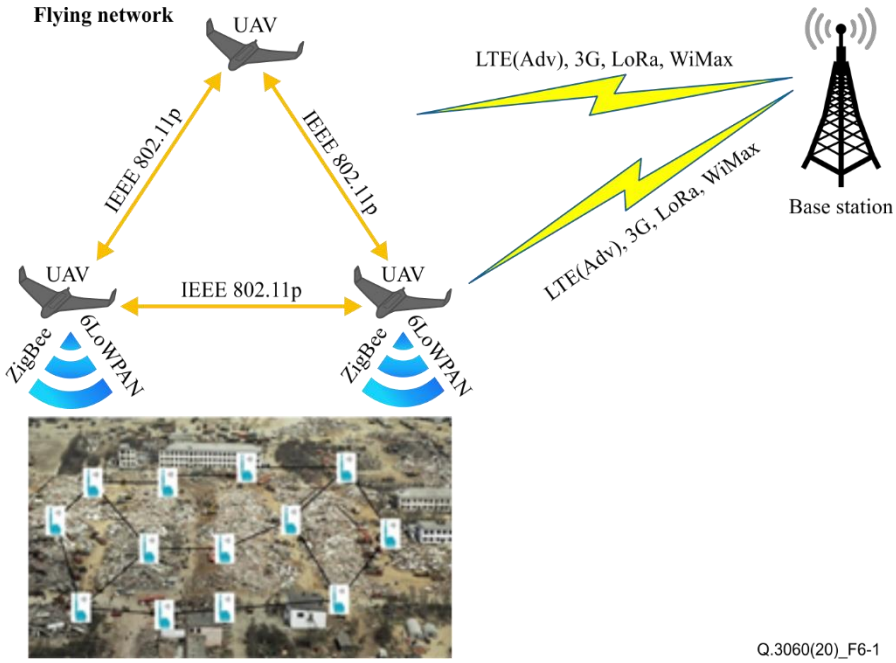


Figure 6-1 – Structure of a fast-deployment flying emergency services network for data collection from a sensor field

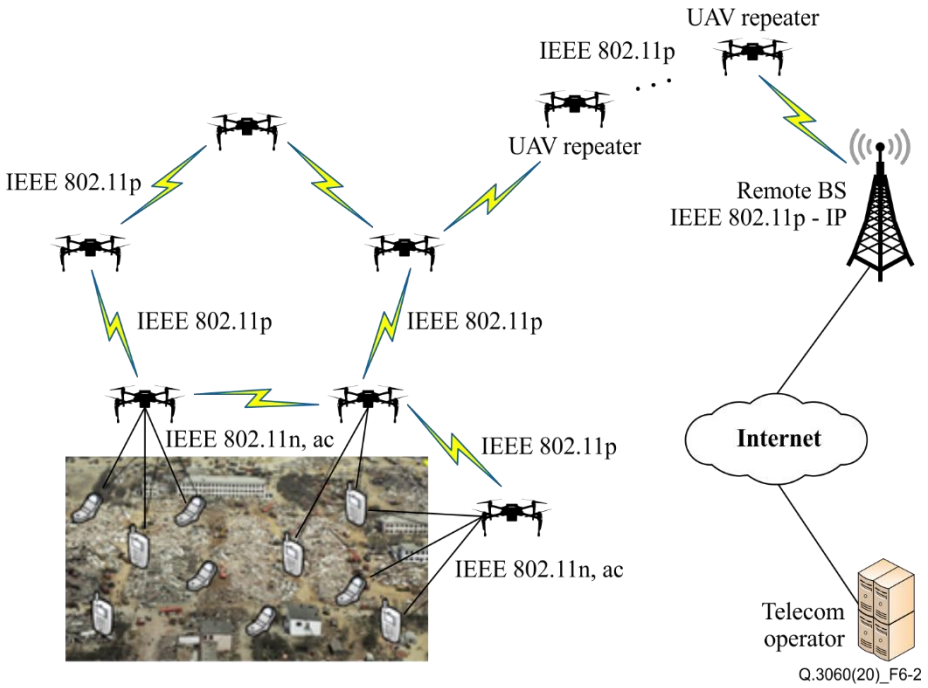


Figure 6-2 – Structure of a fast-deployment flying emergency services network providing communications between subscribers

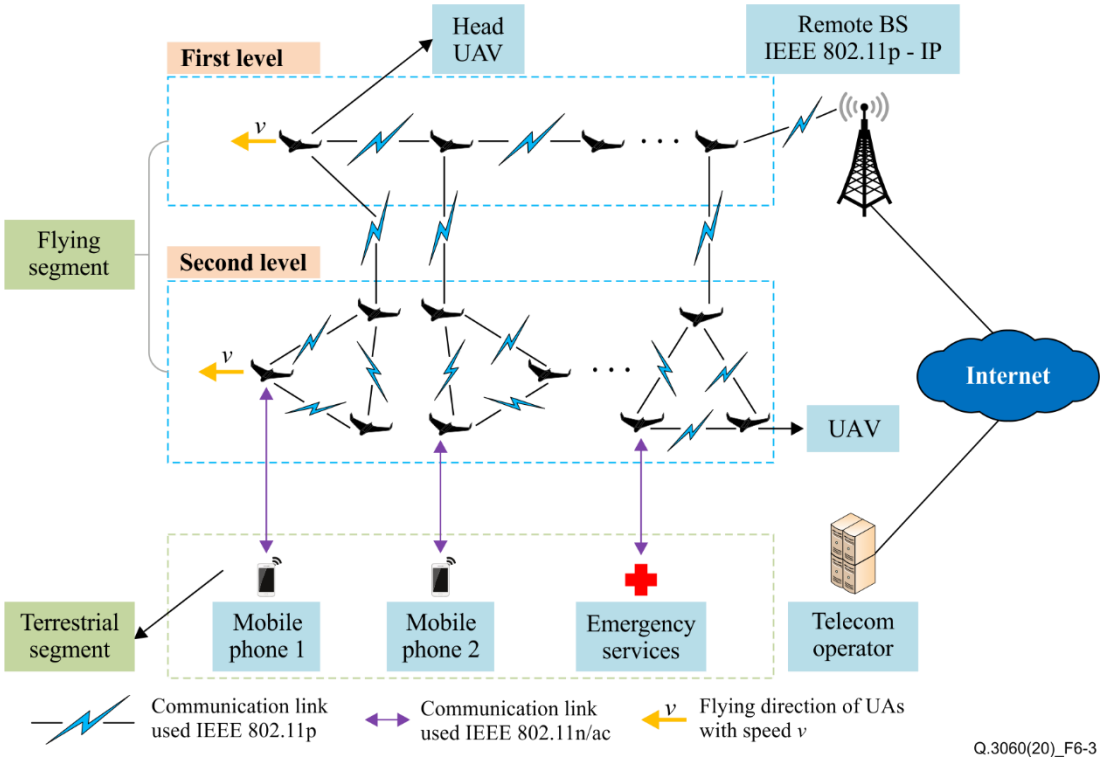


Figure 6-3 – UAV hierarchical structure for providing voice services

7 Service and capability requirements of a fast deployment emergency telecommunication network

The service and capability requirements of an fdETN include the following.

– Install sensor nodes in the area of destruction.

– Collect data from sensor nodes.

– Send data to BS via different data transmission technologies using heterogeneous gateways.

– Establish an emergency service for calls to police, fire service, medical services, etc. This service should have the highest service priority and transfer the call to the nearest call emergency centre or rescue platform by the shortest path. It supports emergency call requirements, such as carrying user location information.

– Establish an emergency broadcast service, including text messaging and voice broadcasting. This service should have secondary priority and be used for urgent announcements that must be delivered to the public with minimum delay, e.g., the service can send or cancel warning notices to subscribers at a time of disaster.

– Establish an emergency command service, including fixed and mobile phone calls, telephone conference and other communication services required by the command system. This service is also very important during emergency, disaster relief and mitigation operations. It ensures interconnection between the command centre and all groups participating in the rescue, on site and remote. For instance, the command centre needs to guarantee connectivity and interaction with the local or national government or the military for rescue efficiency.

– Establish disaster monitoring services, which provide real time surveillance of the disaster situation using an emergency sensor network. It allows automatic data collection and measurement, and offers reliable data transmission to the rescuer. It can help people to evaluate the impact and scale of damage.

– Create a network and provide a public communication service for users, which offers common message and call services to subscribers in the disaster area. The service supports text messaging, multimedia short message service (SMS), audio and video calls. It maintains an information channel for subscribers to communicate with people inside and outside the disaster area.

8 Interface and signalling protocols of fast deployment emergency telecommunication network

8.1 Interface between user equipment and UAV using IEEE technologies

The following wireless local area network (WLAN) protocols may be used at the interface between user equipment (UE) and UAV:

– [b-IEEE 802.11n];

– [b-IEEE 802.11ac].

The following protocols related to personal area networks (PANs) may be used at the interface between UE and UAV:

– [b-Zigbee];

NOTE 1 – Zigbee is a specification based on [b-IEEE 802.15.4] for a suite of high-level communication protocols used to create PANs with small, low-power digital radios, such as for home automation, medical device data collection and other low-power low-bandwidth needs, designed for small scale projects that need wireless connection.

– IPv6 over low-power wireless personal area network (6LoWPAN);

NOTE 2 – 6LoWPAN is specified in [b-IETF RFC 6282].

– [b-Thread].

NOTE 3 – A networking protocol based on Internet protocol version 6 (IPv6) designed for low-power IoT devices in an IEEE 802.15.4 wireless mesh network, commonly called a wireless personal area network (WPAN).

Protocols related to a low-power wide-area network (LPWAN), such as [b-MAVLink], for microair vehicle communication with small unmanned vehicles, or [b-LoRa], for an LPWAN, may be used at the interface between UE and UAV.

8.2 Interface between UAVs

Due to the fact that a large number of UAVs are simultaneously available in the air, problems may arise between them that will cause harm to human health or economic losses. Transmission delay and transmission rate are critical factors in network environments when UAVs interact to send and receive messages. To solve these problems, control messages sent by the head UAV must be delivered with low latency and high probability of delivery. To transmit information, such as images, voice and video, the appropriate communication channel bandwidth is required. In addition, it is necessary to consider the QoS for several priority services in a flying network.

It is necessary to support many types of services with different priorities.

The [b-IEEE 802.11p] protocol is a modified version of the familiar IEEE 802.11 (Wi-Fi) standard. The use of that protocol in a flying network has proven to be the most suitable for a flying network due to public communications between UAVs. It was originally developed for vehicular ad hoc networks (VANETs). [b-IEEE 802.11p] was adopted as the source of medium access control (MAC) and physical layer (PHY) specifications for the lower-layer dedicated short-range communication (DSRC) standard, for which radio interface standards are specified in [ITU-R M.2084] and the frequency band for current and future ITS applications is specified in [ITU-R M.2121]. It is expected that these characteristics will demonstrate excellent performance, not only in vehicles on the ground, but also in the interaction of UAVs in the air. VANETs are supposed to be moved into the air and used for UAVs.

The [b-IEEE 802.11p] protocol uses the enhanced distributed channel access (EDCA) mechanism, which uses carrier-sense multiple access with collision avoidance (CSMA/CA) to support various types of applications with QoS. The EDCA mechanism allows messages that have higher priority to have a better chance of being transmitted than those with lower priority. There are four types of access categories (ACs): background traffic (AC0); traffic from the best attempt (AC1); video traffic (AC2); and voice traffic (AC3). Prioritization is achieved by varying the EDCA parameter set including contention windows (CWs) and the arbitration inter-frame spaces (AIFSs), which increase the probability of successful medium access for real-time messages.

A MAC layer based on [b-IEEE 802.11p] and [b-IEEE 1609.4] protocols to perform communications between UAVs, as well as between groups of UAVs, is proposed. UAVs will be divided into different groups called clusters to move in rescue areas and perform missions. The proposed protocol includes three different protocols: cluster management protocol (CMP); intra-cluster communication protocol (IntraCP); and inter-cluster communication protocol (InterCP). These protocols use different modified wireless access in vehicular environment (WAVE) service advertisement (WSA) and WAVE short message (WSM) packets to update information (UDI), and transmit data within and between clusters.

In the proposed mission-oriented flying network, the UAVs move in accordance with the mission and are subject to geographical restriction. In a mission-oriented flying network environment, UAVs cooperatively communicate with each other to receive information on mission assignment from the BS or forward the collected data to the BS.

In particular, MBSs will deploy UAVs groups to areas around them to gather information, which will be disseminated between groups and transmitted to the BS. UAVs groups also act as intermediaries to make connections and transfer data between the BSs to create a timely, efficient and effective rescue system, and increase the coverage area of the flying networks (Figure 8-1).

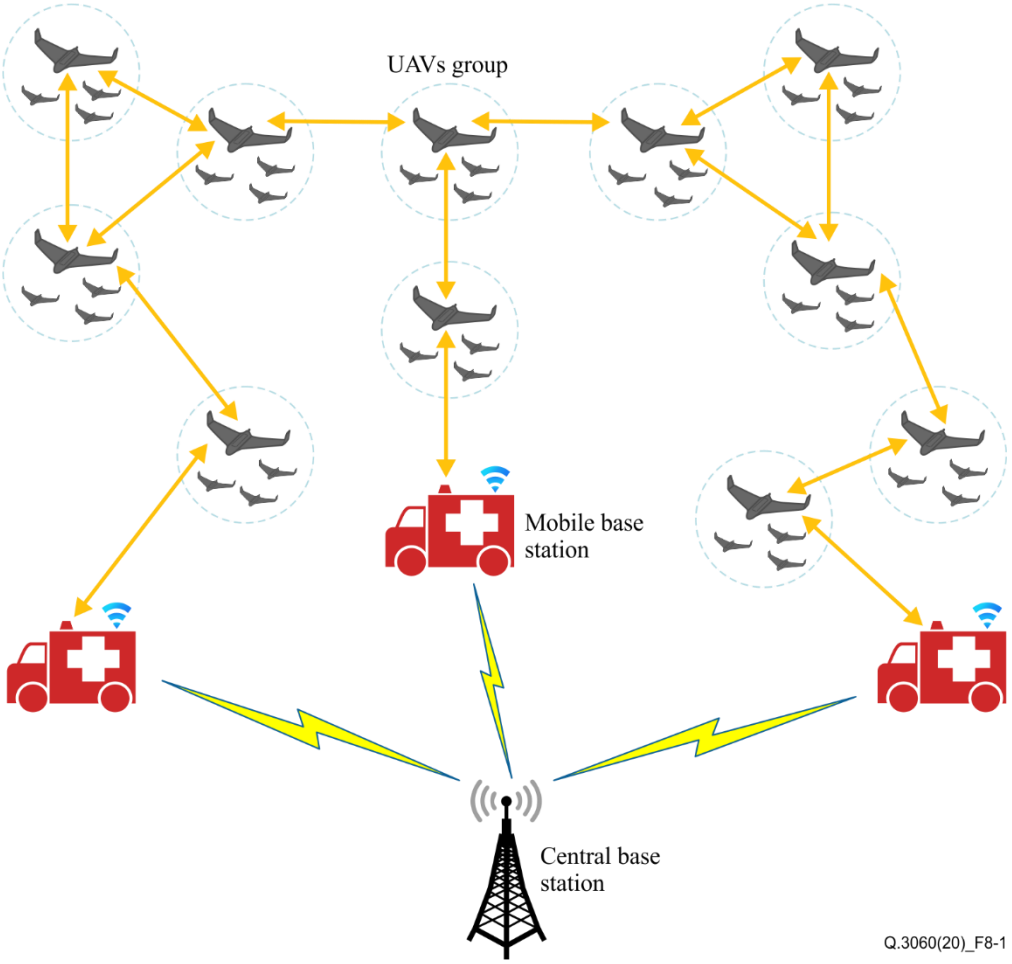


Figure 8-1 – Network of UAVs for emergencies

In addition, in search and rescue, it is very necessary to have communication among rescuers or between rescuers and victims or between victims and their relatives. In order to support these requirements when the telecommunication infrastructure has been destroyed, an architecture for emergency that uses a flying network over satellite systems is proposed. Satellite systems can connect to almost every point on Earth. Satellite user terminals are mobile devices that help quickly connect to satellites. UAVs equipped with a satellite user terminal, and [b-IEEE 802.11p], [b-IEEE 802.11n] and [b-IEEE 802.11ac] modules, can connect to the devices of people in a natural disaster as well as transfer data to MBSs or to satellites. In this architecture, voice traffic can be transmitted from subscriber over UAVs via VoWiFi to the MBS (or to UAV, which can connect to satellite) and over satellite systems to a telecom operator (Figure 8-2).

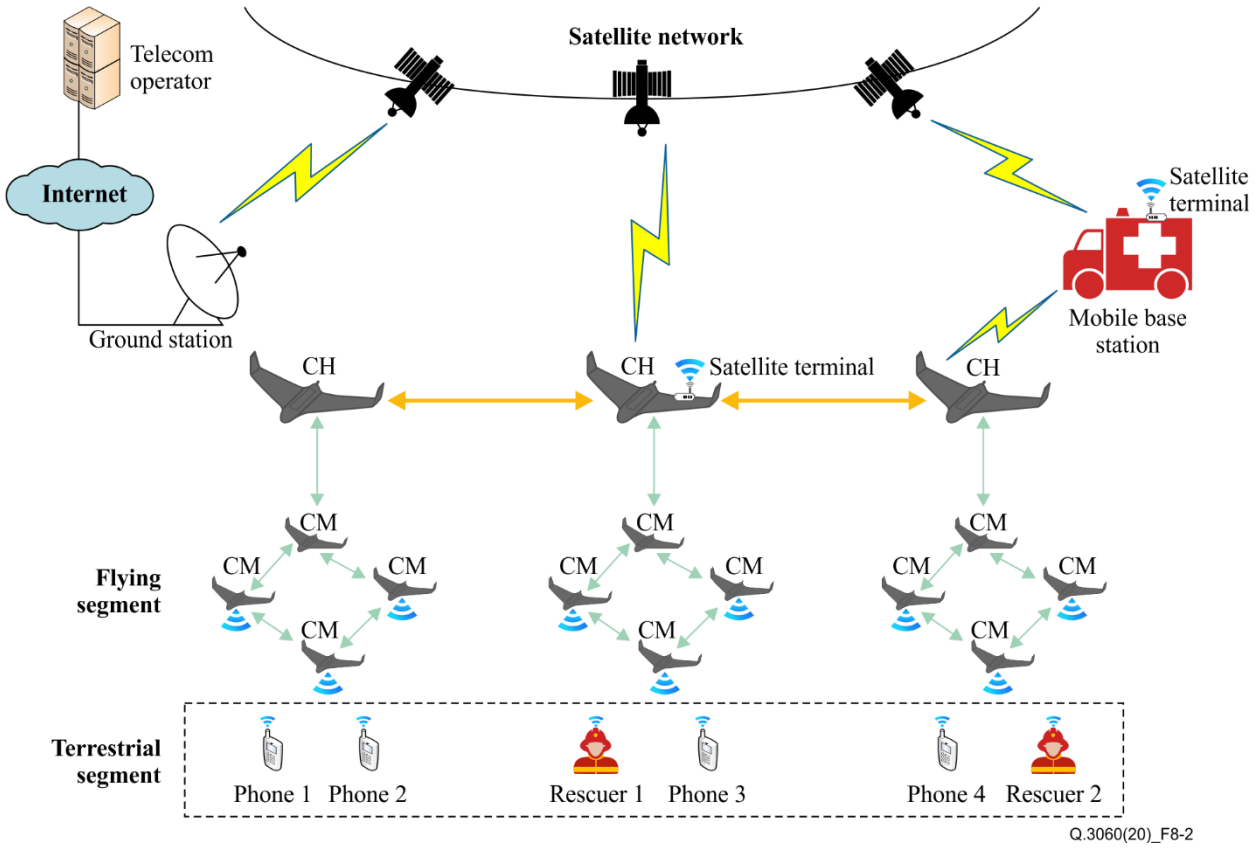


Figure 8-2 – An architecture for flying ad-hoc network for emergency

Figure 8-3 presents a flying network of a CMP, IntraCP and InterCP for a single MBS. The name of the combination of those protocols is the cluster-based multichannel MAC IEEE 802.11p protocol (CMMpP). It should be noted that, in this Recommendation, a group of UAVs can alternatively be called a cluster and a UAV a node.

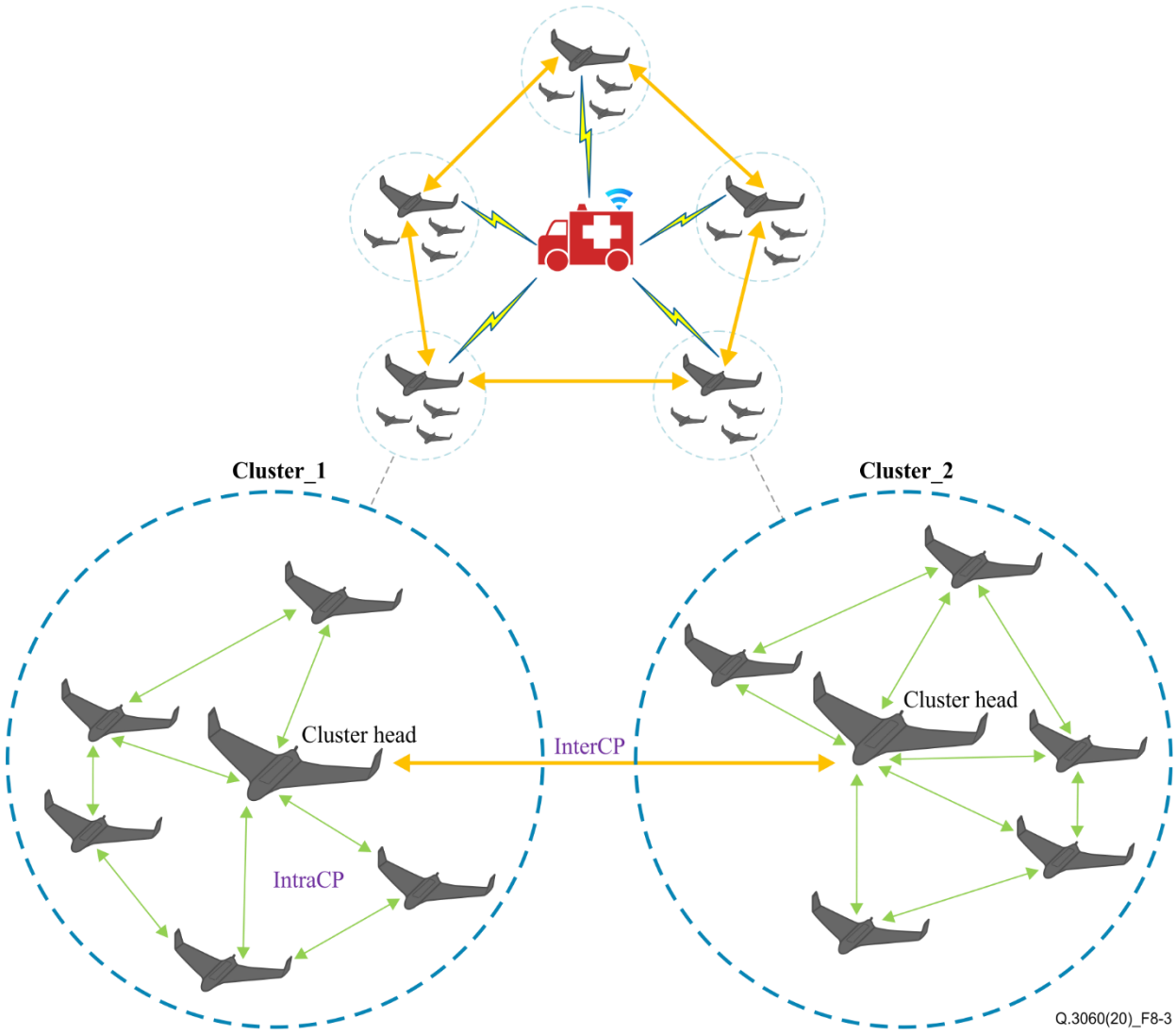


Figure 8-3 – Groups of mission-oriented UAVs around a mobile base station

In order not to complicate the mission, the following assumptions are made.

The nodes are divided into different clusters at the beginning of the mission and each cluster has different flight directions to gather information as well as increase the coverage of the network. Each node in the cluster also has its own flight speed and flight direction, but this difference is within the allowable limit to ensure cluster stability. In addition, during task implementation, no node is allowed to leave or join the cluster.

All UAVs are equipped with a global positioning system (GPS) device to define location, and time popularity coordinates of UAV are small enough to allow calculation errors to be ignored.

There are two transceivers on each UAV to support simultaneous multichannel transmission due to the negative effects of channel switching on spectrum efficiency. In addition, performance of safety applications does not make the single-radio approach a good candidate for multi-channel MAC architectures.

The mission can be stated as follows.

First, the MBSs will move to the rescue area. There they will deploy groups of mission-oriented UAVs (clusters) to collect information, make connections and exchange data. These clusters will use a CMP to elect their own cluster head (CH) node, which may change during the execution of the task depending on the location and speed of the nodes in the cluster. The CH node is responsible for

collecting information from cluster members (CMs) and then transferring it to the BS or passing it to the CHs of other clusters. The CH node also acts as intermediate for data transmission, scheduling and channel assignment through message controls.

Nodes will use IntraCP and InterCP to transmit data. These protocols employ the multichannel MAC protocol [b-IEEE 1609.4] and [b-IEEE 802.11p] protocol in combination with time-division multiple access (TDMA) to conduct every communication. In particular, the IntraCP performs the following main tasks:

– collecting/delivering control messages from/to CMs on the control channel (CCH);

– allocating the available service channels (SCHs) to CMs for data traffic;

– contending to transmit data on the SCHs in clusters.

Meanwhile, the InterCP is responsible for making communications between different clusters (transmitting both control messages on the CCH and data traffic on the SCH).

To ensure communication over a large coverage area, the launch of many UAVs is required. For UAV interaction problems, it is advisable to use a hierarchical structure, dividing the UAVs into clusters. For communication tasks between clusters, the CMP can be used, which is described in the Appendix III.

8.3 Interface between UAVs and base station

Use the CMMpP with InterCP.

9 Architecture for long-term use fast deployment emergency telecommunication network base on tethered high-altitude unmanned platforms

9.1 Architecture for tethered high-altitude unmanned platforms

Tethered high-altitude unmanned platforms are designed for lifting and long-term holding of telecommunication payloads at altitudes up to 500 m. Their long-term operation is ensured by the transmission of electrical energy from a ground source to the flight module via a low-diameter cable to supply power to the propulsion systems and on-board telecommunication equipment. The long-term operation of a high-altitude unmanned module based on internal combustion engines can be provided by fuel supply from a ground-based compressor. Thus, the tethered high-altitude platforms fall in-between satellite and terrestrial systems whose equipment (cellular BSs, radio-relay, radar equipment, etc.) is deployed in high-rise structures. Tethered high-altitude platforms, as compared with expensive satellite systems, are highly cost-efficient, while ground-based telecommunication systems surpass the vastness of the field of telecommunications and video coverage.

The architecture of tethered high-altitude unmanned platform includes the following main components.

1) A multi-rotor UAV of large carrying capacity and a long operating time, designed to ascend to 500 m and hold the telecommunications payload, video surveillance equipment, etc.

2) A high-power ground-to-board energy transmission system that provides power to the propulsion systems of the unmanned multi-rotor flight module and the payload equipment.

3) Control and stabilization system for the high-altitude platform, including a local navigation subsystem with ground-based radio beacons, providing increased positioning accuracy and noise immunity in the absence of signals from satellite navigation systems.

4) On-board payload equipment including: BS of the cellular network of the fourth generation (LTE); radar and radio relay equipment; and equipment for video surveillance and environmental monitoring.

5) Cable with a poly(paraphenylene terephthalamide) covering, including copper wires of small cross-section (0.5 mm^2) for transmission of high-voltage (up to 2 000 V), high-frequency (up to 200 kHz) signals and optical fibre for digital information transmission with a speed of up to 10 Gbit/s.

6) Ground control complex, which includes a 380/2000 V voltage converter, a diagnostic system for high-altitude platform parameters and an intelligent wrench with a microprocessor unit to control the cable tension during lifting, descending and wind loads. In the mobile configuration, the ground control centre is located on a mobile platform on to which an electric generator is installed, the output power of which is not less than 20 kW.

9.2 Services on tethered high-altitude unmanned platforms

The possibility to lift telecommunication hardware and other payloads to altitudes of up to 500 m and its long-term operation opens up wide possibilities for the practical application of robotic systems of this class. Tethered high-altitude unmanned platforms provide solutions to the following challenges:

– fast deployment of a modern telecommunication infrastructure over a vast territory in emergency conditions when communication facilities are destroyed (an LTE BS is installed on board a high-altitude module in this case);

– organization of high-speed wireless links over long distances in direct line of sight (for this purpose, radio relay or equipment is installed on board the high-altitude module);

– implementation of the control and monitoring functions of a group of UAVs, as well as coordination of the work of a flying network that provides communication and data transmission services;

– implementation of the functions of environmental monitoring, forest fire control, video monitoring of mass events, etc. (equipment for night and day vision, environmental monitoring, etc. are installed on board the high-altitude module);

– control of unmanned terrestrial mobile robots during search and rescue operations, while ensuring the functioning of ground-based unmanned transport vehicles, etc. (for these use cases on board the flight module, wireless communication, radio frequency identification, IoT and video equipment are installed);

– detection of unauthorized UAV flights in order to ensure the safety of critically important objects (video and radar equipment are installed on-board the high-altitude module).

Figure 9-1 shows an example of the application of a tethered high-altitude unmanned platform.

Figure 9-1 – Tethered high-altitude unmanned platform application example

Various scenarios for using tethered high-altitude unmanned platforms are described in Appendix II.

Appendix I

Introduction of fast deployment emergency telecommunication network approaches

(This appendix does not form an integral part of this Recommendation.)

I.1 Internet of things

It is assumed that, following a natural disaster, a large part of the telecommunication infrastructure will be destroyed. For this reason, it is essential before anything else to assess the impact and scale of the damage, and for this it is indispensable to read data from sensor nodes deployed in the area of destruction. Given that sensor nodes can communicate using a range of different technologies, it makes sense to use a heterogeneous gateway for data collection. Such a gateway, carried by a UAV, can be used to collect data from the sensor nodes and relay the data to the public network.

I.2 Heterogeneous gateway

A heterogeneous gateway is a network device or relay system intended to allow intercommunication between two IT networks with differing characteristics, using different sets of protocols and supporting different data transmission technologies. Such gateways can support different data transmission technologies such as [b-ZigBee], Bluetooth low energy (BLE), 6LoWPAN, [b-LoRa], narrow-band Internet of things (NB-IoT), Wi-Fi ([b-IEEE 802.11n], [b-IEEE 802.11ac], [b-IEEE 802.11p], [b-IEEE 802.11ad]), LTE advanced (LTE-A), third generation (3G), worldwide interoperability for microwave access (WiMax) and others, and act as a connecting link between the various devices and the public network.

I.3 Wireless sensor network

There are two scenarios of intercommunication between nodes and a network coordinator.

1 Peer-to-peer network: all sensor nodes are equivalent; during flight over a given area the UAV transmits broadcast service data that switch the sensor nodes from "standby" to "active"; the sensor nodes then begin transferring data to the network coordinator.

2 Hierarchical network: the terrestrial segment takes the form of a hierarchical network consisting of sensor nodes and node-routers. The sensor nodes feed data to the routers that carry out aggregation of the data before transmitting them to the coordinator located on the UAV.

The FUSN is one technology that might be used as a part of an fdETN (see Figure I.1). The aim of this segment is to cover an extensive area with restricted access.

In general, such a network may provide voice or video and data communication using flying BSs that transmit the payload through heterogeneous gateways using the USN principle.

This segment is based on two sub-systems; air; and terrestrial.

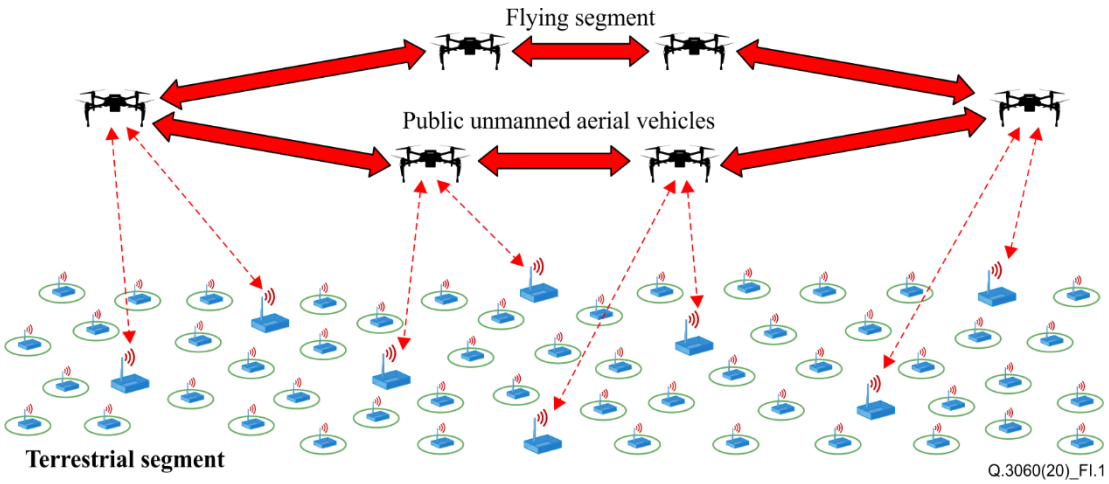


Figure I.1 – Flying ubiquitous sensor network architecture

The terrestrial sub-system includes a set of sensors that interact with different items (sensors may also be located remotely); while the air sub-system is represented by flying objects such as UAVs, drones and quadcopters. The key task of the air subsystem is to exchange and transmit traffic among flying nodes.

A detailed description of such functional subsystems is under study.

Appendix II

Scenarios for using tethered high-altitude unmanned platforms

(This appendix does not form an integral part of this Recommendation.)

A high-altitude platform of tethered UAVs (tUAVs) consists of terrestrial and flying modules. The terrestrial module consists of a ground control station for a high-altitude platform (telecommunication control system; TCS), a ground voltage converter, a winch for tethered cable of a high-altitude platform and a mooring device (Figure II.1).

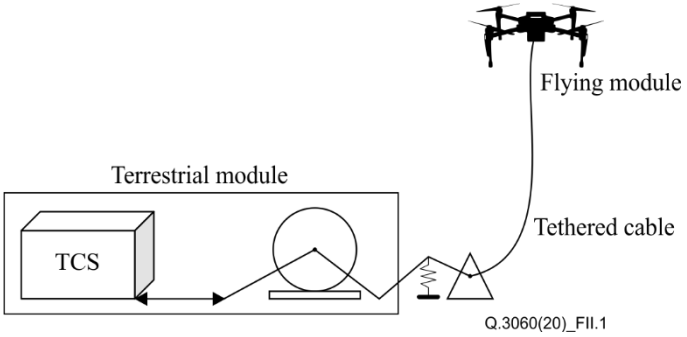


Figure II.1 – Tethered unmanned aerial vehicles high-altitude platform

The operating range of UAVs can be expanded by using a chain of UAVs tethered one to another. The first UAV in the chain is tethered to a ground station, while the last one serves as end effector.

Architectures of flying networks for emergencies using tethered multicopters are considered in the following scenarios.

1) Collect data from sensor filed in flying network for emergencies using tethered multicopters.

After a natural disaster, it is impossible for most telecommunication infrastructures to avoid damage, so the consequences and scale of the destruction must first be assessed. To do this, it is necessary to read data from sensory nodes located in the destruction zone. Due to the fact that sensor nodes can communicate using various technologies, it is advisable to use a heterogeneous gateway for data collection. Such a gateway, mounted on a UAV, will allow data collection from sensor nodes and delivery to a public communication network.

In a search and rescue operation, MBSs will deploy a group of UAVs to areas around them to gather information, including tUAVs. All UAVs are equipped with a heterogeneous gateway, which is a network device or a relay system designed to ensure the interaction of two information networks that have different characteristics, use different sets of protocols and support different transmission technologies. Data can be collected by UAVs from nodes in sensor fields with technologies such as [b-ZigBee], 6LoWPAN, [b-LoRa], BLE and NB-IoT. Therefore, these data can be transmitted through a chain of UAVs via [b-IEEE 802.11p]. By using tUAVs, which have a long working time, data can be transmitted to the MBS via [b-IEEE 802.11p], LTE-A or [b-LoRa], depending on the specific situation (Figure II.2).

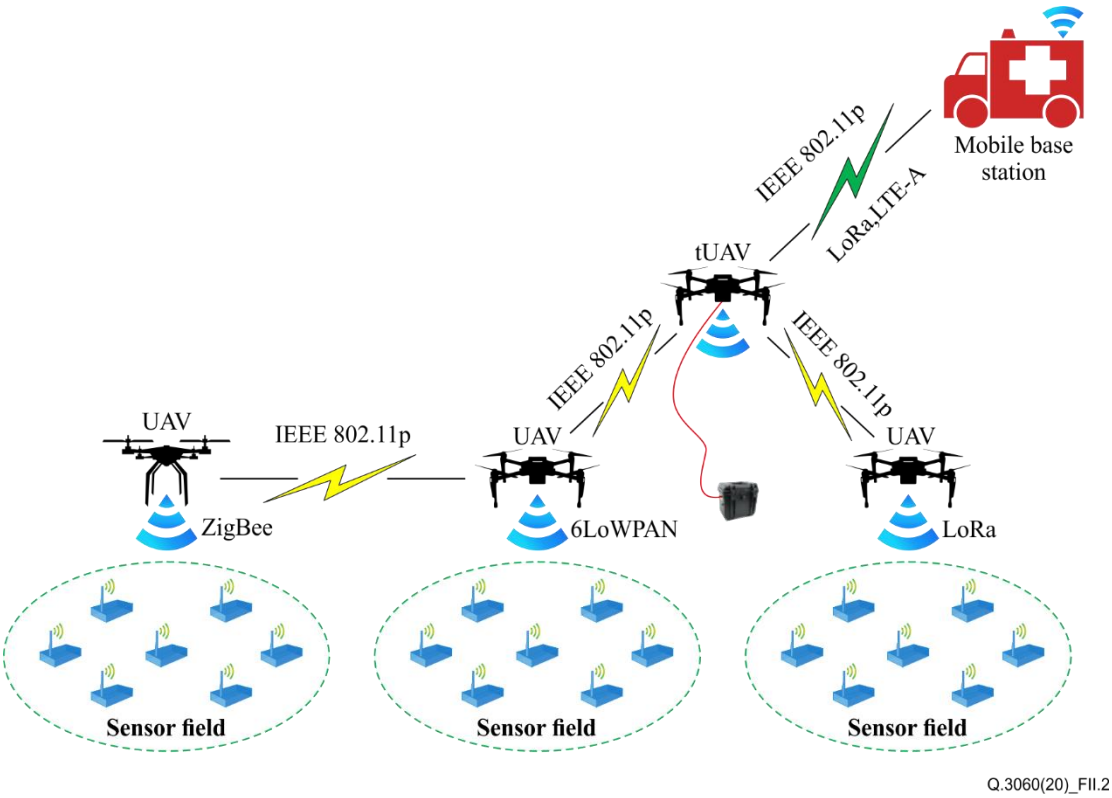


Figure II.2 – Architecture for data collection from sensor fields in a flying network for emergencies using tethered multicopters

2) Interaction of flying network for emergencies using tethered multicopters.

In a flying network for emergencies, communication among UAVs in a group and UAV groups is very important. Technology [b-IEEE 802.11p] with the modified CMMpP was developed to solve these issues. Moreover, tUAVs can be used in this network, which is presented in Figure II.3. tUAVs can become super cluster nodes, which can receive information from cluster nodes of the groups or can replace cluster nodes when all UAVs in the group cannot be the CH. Furthermore, with their own advantages, tUAVs can carry LTE modules to support the transmission of data with LTE-A technology. These tUAVs, therefore, can cover areas no longer supported by destroyed cellular BSs after adisaster. In addition, with tUAVs, the network will be more stable and reliable.

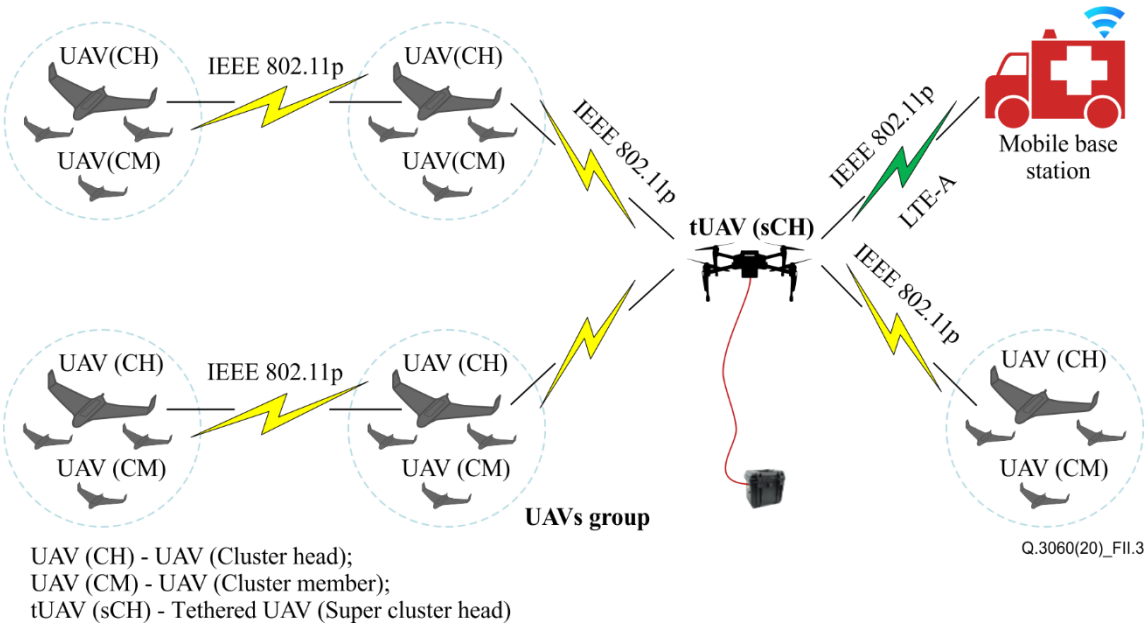
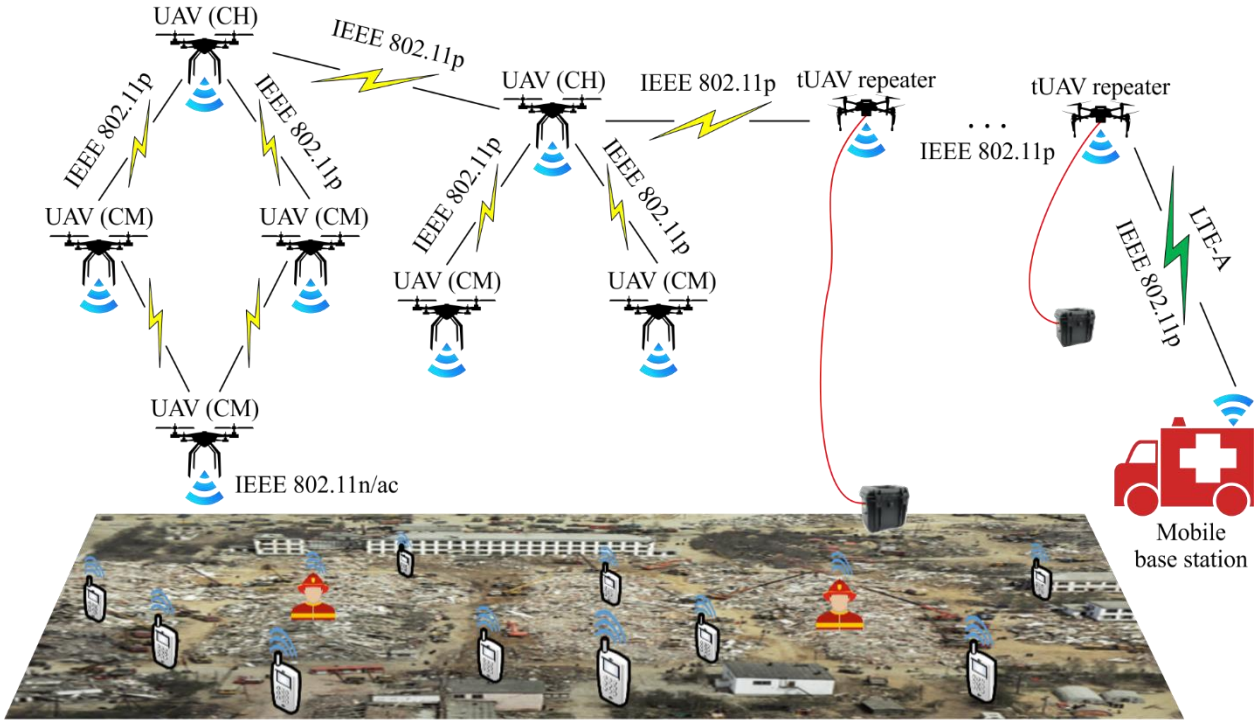


Figure II.3 – Architecture of flying network interactions for emergencies using tethered multicopters

3) Multimedia transfers over a flying network for emergencies using tethered multicopters.

Because they are equipped like any other UAV, tUAVs can participate in multimedia transfers over flying networks for emergencies. Take a case where in a disaster area two subscribers want to call each other via VoWi-Fi using the UAV group. An example of such a call may be the connection of an emergency service officer with subscribers in the disaster zone. According to mobile phone function algorithms, in the absence of communication with the BS, the phones switch to scanning mode for available Wi-Fi networks. Scanning in the area of a natural disaster will help discover subscribers who potentially could be under rubble waiting for help. A call between two subscribers will be performed through a chain of UAVs interacting with each other. A UAV can received voice traffic by [b-IEEE 802.11n] or [b-IEEE 802.11ac] from subscribers and transmit through chain of UAVs to the MBS and connect to a mobile operator to set up the call (Figure II.4).



UAV (CH) - UAV (Cluster head);
UAV (CM) - UAV (Cluster member);
tUAV - Tethered UAV.

Figure II.4 – Architecture of multimedia transfers over a flying network for emergencies using tethered multicopters

Appendix III

Cluster-based multichannel MAC IEEE 802.11p protocol

(This appendix does not form an integral part of this Recommendation.)

III.1 Cluster management protocol

The CMPis responsible for maintaining and selecting the CH for the current cluster. A node in the centre of the cluster is first selected as the CH. This ensures that from the beginning nodes can exchange information with each other.

The decision about which node remains a CH is based on a total weighted factor *F*, which takes into account different metrics. These metrics involve the mobility information of each node including the speed of a node (*v*) and the distance to the neighbours (*d*). A node identifies its neighbours by sharing this mobility information through control messages by using an IntraCP.

The speed weight of the *i*th node can be expressed as:

$$f_v(i) = \frac{1}{|v_i - \bar{v}|} \quad \text{(III-1)}$$

where

$$\bar{v} = \frac{v_1 + v_2 + v_3 + \ldots v_n}{n} \quad \text{(III-2)}$$

n is the number of neighbours;

v_i is the speed of *i*th node.

The denominator of Equation III-1 represents the average difference of speed between one node and all its CMs. The idea here is that a node with similar velocity to most nodes in its neighbourhood will cause less change in the CMs than a node, which is much faster or slower than the rest.

Next, the central position is calculated by:

$$\bar{d} = \frac{1}{n}\left(\sum_{i=1}^{n} x_i, \sum_{i=1}^{n} y_i, \sum_{i=1}^{n} z_i\right), \quad \text{(III-3)}$$

where (x_i, y_i, z_i) are the coordinates of the *i*th node and distance weight of the *i*th node can be presented as:

$$f_d(i) = \frac{1}{[(x_i - \bar{d})^2 + (y_i - \bar{d})^2 + (z_i - \bar{d})^2]^{1/2}} \quad \text{(III-4)}$$

Equation III-4 represents the average distance between all neighbours and the central position. It indicates how close the neighbours to one node are. Here, a large value is preferable, as it can be expected that nodes that are placed closer together will stay longer in their transmission range.

Combining these measures, the total weight factor *F* is obtained which shows the suitability of a node to become the CH. The greater the value of *F*, the better it is qualified to be the CH. The values of factors w_v and w_d can be chosen between 0 and 1 according to the different scenarios. Their sum has to be 1.

$$F = w_v f_v(i) + w_d f_d(i) \quad \text{(III-5)}$$

III.2 Sharing information

In order for the protocols to be deployed, each node periodically updates information about its location, speed in cluster, ClusterID, SCH requests (if there is data to send) and priority of service (with EDCA parameter sets) to all members in its cluster through control messages, as follows.

– Location is defined by a GPS system.
– ClusterID is the identification of the cluster.
– An SCH request is information, which indicates that this node needs to be assigned an SCH to transmit data. It also specifies whether it needs an SCH for intra-cluster or inter-cluster communication.
– Priority indicates the type of traffic transmitted via the SCHin the next interval. Usually four levels of priority are used, as shown in Table III.1.

Table III.1 – Delay parameter requirements for each type of traffic

Priority	Traffic type	Acceptable delay value
1	Voice, highly interactive video	100 ms
2	Interactive video	100-400 ms
	Video streaming	<1 s
3	Best effort	not normalized
4	Background	not normalized

III.3 Cluster-based multichannel MAC IEEE 802.11p protocol

Since both the IntraCP and InterCP support each other, it is not advisable to present each separately but to combine them in the CMMpP.

In the proposed CMMpP protocol, each node is equipped with two transceivers, denoted Trans_1 and Trans_2, respectively, that can operate simultaneously on different channels. Trans_1 is always tuned to the CCH to monitor and transmit control messages, while Trans_2 is tuned to any SCH (channels 174, 176, 180, 182) to transmit data. This is an alternative to using CCH intervals (CCHIs) and SCH intervals (SCHIs) of 50 ms duration for each. In this regard, the whole synchronization interval (SI) of 100 ms can be used (Figure 8-1). In addition to using the CCH (channel 178) for control messages, the main proposal is to use one SCH (channel 182) exclusively for inter-cluster transmission of data. The other SCHs (channels 174, 176, 180) will then be assigned to CMs for the intra-cluster transmission of data.

Operation of Trans_1

First, the CH sends a beacon message (B) packet to notify the starting SI via the CCH to all CMs. After receiving the notification, the CMs reply to update all node information using UDI packets during the information update period. The information in this UDI packet is used to redefine the CH for the next SI, if necessary, and update requests for using SCHs from CMs. Based on SCH requests, the CH creates schedules for CM intra-cluster and inter-cluster transmissions in the next SI. Next, in the assignment period, the CH broadcasts a packet to announce a schedule of transmission (ST) packet to the CMs. The ST packet indicates which node will use which SCH to transmit data in the cluster or between different clusters. In addition, the ST also shows information about the CH node for the next interval. To increase reliability and ensure CMs receive ST packets, the CH will send them twice. All these processes occur with the TDMA mechanism on the CCH under the IntraCP. Figure III.1 shows the operation of the CMMpP.

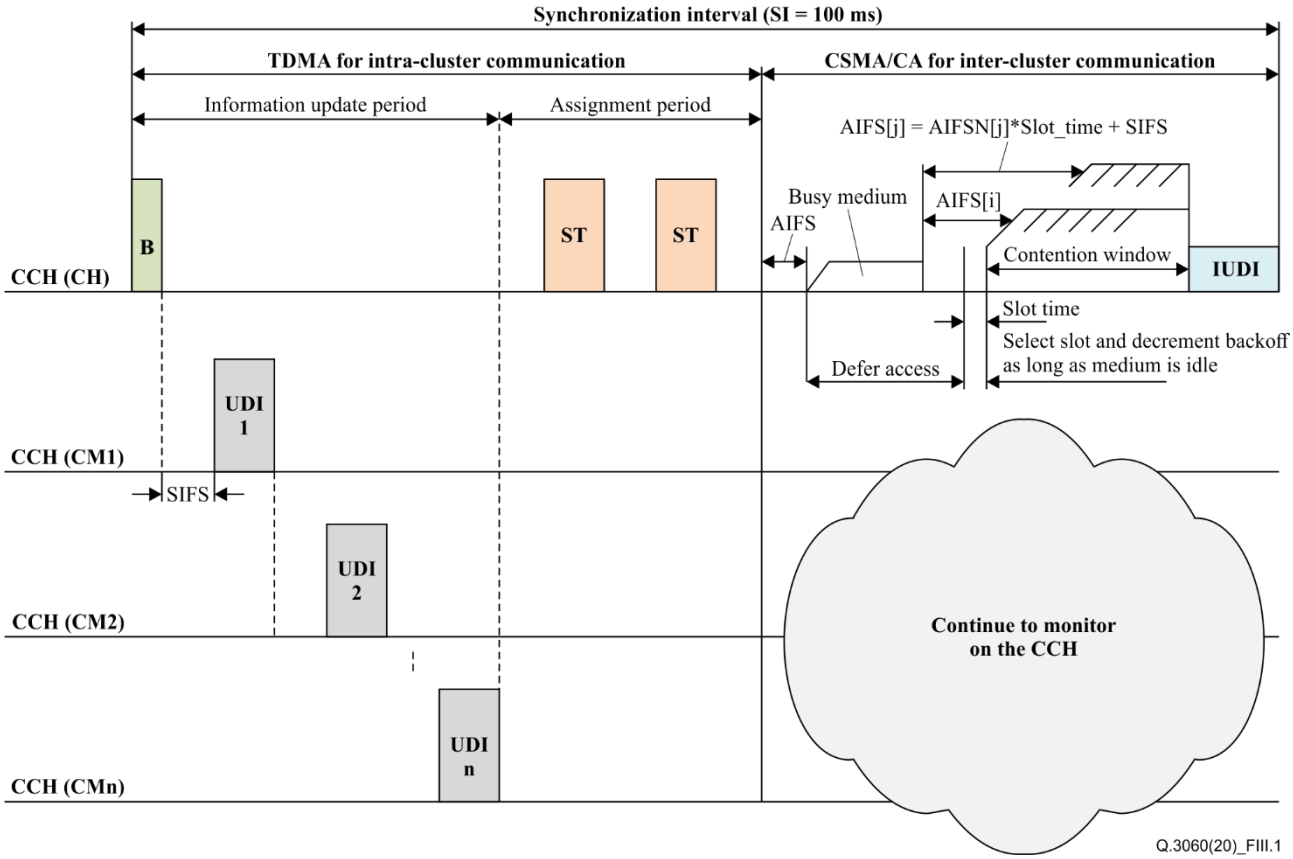


Figure III.1 – Operation of CMMpP including IntraCP and InterCP on the CCH

The principle of assigning SCHs for CMs is as follows: the CH receives the SCH request information from a CM. The CH then searches for a rarely used (to reduce interference) SCH in the list of available SCHs in accordance with the purpose of intra-cluster or inter-cluster communication. Then an SCH is assigned to the CM through an ST packet.

After the intra-cluster communication period, the CH performs inter-cluster communication using the contention-based CSMA/CA mechanism in [b-IEEE 802.11p] in order to compete with the CHs of other clusters. When the environment is idle, it broadcasts the inter-cluster update-information (IUDI) communication packet to disseminate all information about the cluster, the list of active nodes and assigned SCHs to other CHs (Figure III.1).

Operation of Trans_2

At the same time as the processes on the CCH, nodes also transmit data on SCHs. On SCHs, nodes including the CH always compete for data transmission via the CSMA/CA mechanism of EDCA of [b-IEEE 802.11p]. This means that those nodes that participate in data transmission while having the same assigned SCH will compete based on updated priority information and their respective EDCA parameter sets. Priority is determined by assigning different EDCA parameters to make sure that delay-tolerant data traffic is transmitted before other traffic streams (see Table III.1). It should be noted that transmissions taking place in the cluster (IntraCP) can use only channels 174, 176, 180 as an SCH. Meanwhile, the InterCP is deployed on the SCH numbered channel 182. These operations occur on non-overlapped channels, so they do not affect each other.

The WSA packet format is modified by using optional fields to create an UDI packet. Figure III.2 shows the format of an UDI packet.

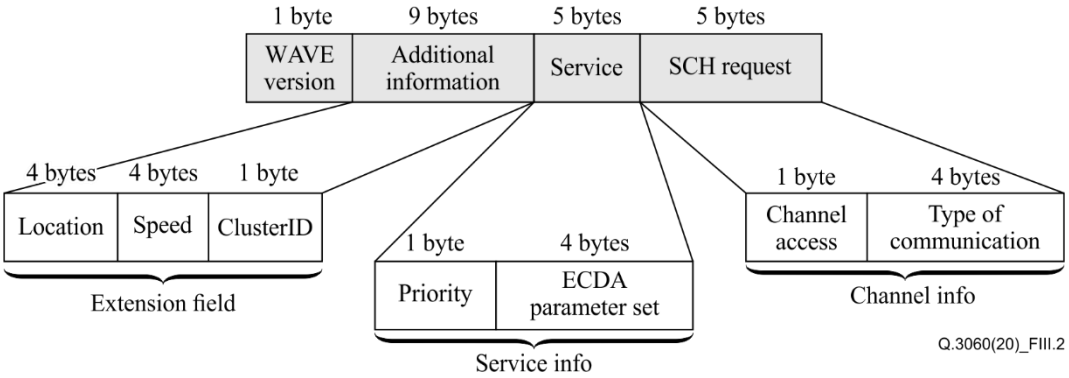


Figure III.2 – UDI packet format

The WAVE version field defines the format of this WSA. The version number associated with the current standard is 1.

The additional information field includes subfields:

– indicating location and speed of the node in the cluster;

– identifying the cluster (ClusterID).

The service field includes the priority and EDCA parameter set subfields. Priority indicates the priority of traffic that the current node needs to send as shown in Table III.1. The EDCA parameter set indicates the predefined EDCA parameters according to the priority.

The SCH request field includes two subfields to notify the CH about transmission demand on the SCH in the next interval.

– The channel access subfield is used to indicate whether this node needs an SCH assignment. In particular, if the last bit is 1, it demands the CH to assign an SCH; if the last bit is 0, it does not need an SCH in the next interval.

– The type of communication subfield indicates intra-cluster communication (if the last bit is 1) or inter-cluster communication (if the last bit is 0). The CH node uses this information to make assignments accordingly.

For the ST packet, the WSM packet format is modified as shown in Figure III.3.

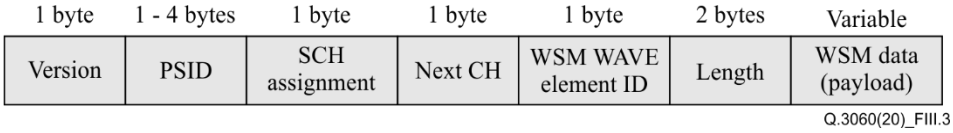


Figure III.3 – Schedule of transmission packet format

The version, provider service identifier (PSID), WSM WAVE element ID, length and WSM data (payload) are required fields of a WSM packet. The SCH assignment field is added to indicate the list of SCHs assigned to CMs.

The next CH field is used to notify a new CH node in the next SI. A broadcast packet IUDI is proposed to inform the CHs of other clusters about its own cluster (Figure III.4). This packet is similar to the ST packet. See Figure III.4.

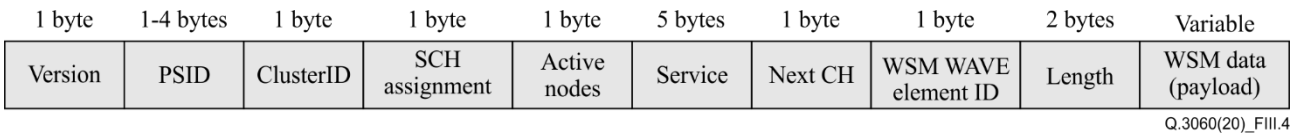


Figure III.4 – IUDI packet format

The version, PSID, WSM WAVE element ID, length, WSM data (payload) fields are required fields.

The active nodes field indicates the list of active nodes that have data to transmit via SCHs.

The service field is similar to the service field in the UDI packet format.

Bibliography

[b-ITU-T Y.4000] Recommendation ITU-T Y.4000/Y.2060 (2012), *Overview of the Internet of things.*

[b-ITU-R M.2291] Report ITU-R M.2291 (2016), *The use of international mobile telecommunications for broadband public protection and disaster relief applications.*

[b-IEEE 802.11ac] IEEE 802.11ac-2013, *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 4: Enhancements for very high throughput for operation in bands below 6 GHz.*

[b-IEEE 802.11ad] IEEE 802.11ad-2012, *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 3: Enhancements for very high throughput in the 60 GHz band.*

[b-IEEE 802.11n] IEEE 802.11n-2009, *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 5: Enhancements for higher throughput.*

[b-IEEE 802.11p] IEEE 802.11p-2010, *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.*

[b-IEEE 802.15.4] IEEE 802.15.4-2020, *IEEE Standard for low-rate wireless networks*.

[b-IEEE 1609.4] IEEE 1609.4-2016, *IEEE Standard for wireless access in vehicular environments (WAVE) – Multi-channel operation.*

[b-IETF RFC 6282] IETF RFC 6282 (2011), *Compression format for IPv6 datagrams over IEEE 802.15.4-based networks*.

[b-6LoWPAN] IPv6 over Low -Power Wireless Personal Area Networks. Open standard defined in RFC 6282 (IETF).[b-LoRa] Semtech (2021). *What is LoRa?* Camarillo, CA: Semtech. Available [viewed 2021-02-24] at: https://www.semtech.com/lora/what-is-lora

[b-MAVLink] Dronecode Project (Internet). *MAVLink developer guide*. San Francisco, CA: Linux Foundation. Available [viewed 2021-02-24] at: https://mavlink.io/en/

[b-Thread] Thread (Internet). *What is Thread?* San Ramon, CA: Thread Group. Available [viewed 2021-02-24] at: https://openthread.io/guides/thread-primer

[b-Zigbee] Zigbee Alliance (Internet). *Control your world your way*. Davis, CA: Zigbee Alliance. Available [viewed 2021-02-24] at: https://zigbeealliance.org/

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	**Switching and signalling, and associated measurements and tests**
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2021