(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) **EP 4 580 094 A1**

(12) **EUROPEAN PATENT APPLICATION**

(43) Date of publication:
02.07.2025 Bulletin 2025/27

(21) Application number: **23220615.1**

(22) Date of filing: **28.12.2023**

(51) International Patent Classification (IPC):
H04K 3/00 *(2006.01)*

(52) Cooperative Patent Classification (CPC):
H04K 3/22; H04K 3/224; H04K 3/226;
H04K 2203/16

(84) Designated Contracting States:
AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC ME MK MT NL NO PL PT RO RS SE SI SK SM TR
Designated Extension States:
BA
Designated Validation States:
KH MA MD TN

(71) Applicant: **ABB SCHWEIZ AG**
5400 Baden (CH)

(72) Inventor: **KARAAGAC, Abdulkadir**
68526 Ladenburg (DE)

(74) Representative: **Maiwald GmbH**
Engineering
Elisenhof
Elisenstrasse 3
80335 München (DE)

(54) **A METHOD FOR DETECTING AN INTERFERING COMMUNICATION SIGNAL**

(57) The invention relates to the field of wireless non-public network, particularly to a method for detecting an interfering communication signal (32) in a wireless non-public network (10). The method comprises the steps of:
providing a plurality of communication devices (14x, 16x) capable of receiving signals in a predefined spectrum, each one of the plurality of communication devices (14x, 16x) located in a known place;
monitoring, by each one of the plurality of communication devices (14x, 16x), for each frequency band in the predefined spectrum, the interfering communication signal;
transmitting, by each one of the plurality of communication devices (14x, 16x), the monitored interfering communication signal and the communication device's known place to a centralized network management entity (12); and
detecting, by the centralized network management entity (12), the interfering communication signal, based on the monitored interfering communication signal and the known place transmitted by each one of the plurality of communication devices (14x, 16x).

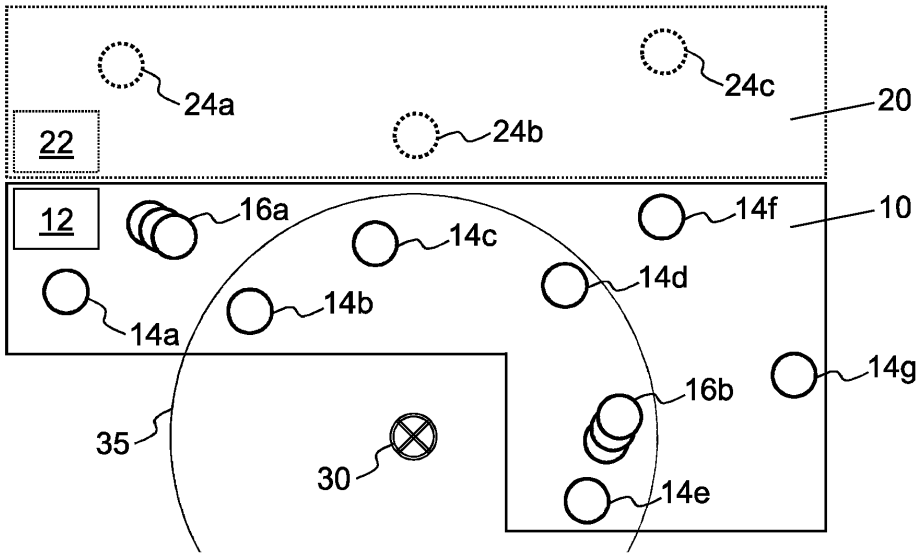

Fig. 1

EP 4 580 094 A1

Description

Field of the Invention

[0001] The invention relates to the field of wireless non-public network, particularly to a method for detecting an interfering communication signal in the wireless non-public network. The invention further relates to an app, a communication device, a system, and to a use.

Background

[0002] So-called wireless non-public networks offer powerful communication capabilities, for example a greater capacity, scalability, increased bandwidth, lower latency, and further benefits. Therefore, said wireless non-public networks become widely used for commercial purposes, e.g. for industrial plants or agricultural systems. However, since administration is no longer necessarily done by a telecommunication company, it may require considerable resources for a private administration to detect an interfering signal, e.g. caused by an external jammer.

Description

[0003] It is an objective of the disclosure to provide a method for detecting at least some types of interfering signals. This objective is achieved by the subject-matter of the independent claims. Further embodiments are evident from the dependent claims and the following description.

[0004] One aspect relates to a method for detecting an interfering communication signal in a wireless non-public network, the method comprising the steps of:

providing a plurality of communication devices capable of receiving signals in a predefined spectrum, each one of the plurality of communication devices located in a known place;

monitoring, by each one of the plurality of communication devices, for each frequency band in the predefined spectrum, the interfering communication signal;

transmitting, by each one of the plurality of communication devices, the monitored interfering communication signal and the communication device's known place to a centralized network management entity; and

detecting, by the centralized network management entity, the interfering communication signal, based on the monitored interfering communication signal and the known place transmitted by each one of the plurality of communication devices.

[0005] A wireless non-public network may be a network having a private ownership and having the capability of being administered by a private centralized network management entity. The licence for the wireless non-public network is usually limited by a predefined area and limited to a predefined set of frequency bands or channels to be used. Examples of wireless non-public networks may comprise so-called 5G NPNs (5th Generation Non-Public Network), e.g. a Standalone Non-Public Network (SNPN) or a Public network integrated NPN (PNI-NPN), a 6G NPN, a 7G NPN, and/or a wireless non-public network that fulfils the above definitions.

[0006] An interfering signal or an interfering communication signal may be a signal that is strong enough to disturb a regular communication in a wireless non-public network. The interfering signal may be caused, for example, by neighbouring senders that are too strong and/or use at least one of the frequency bands of the wireless non-public network. Further examples may comprise a so-called jammer, which sends - unintentionally or intentionally - radio waves that interfere with frequency band(s) of the wireless non-public network.

[0007] The communication devices may be regular communication devices, i.e. devices that are configured for regular use in the area of interest, e.g. communication devices for industrial and/or agricultural machines, particularly for Future Industrial Systems. The communication devices may also comprise fixed devices - e.g. sensors, actuators, controllers - that have a unit for wireless communication. The communication devices may further comprise mobile devices like smartphones, pads, laptops, and the like. It should be noted that the method described above and/or below does advantageously not need specialized communication devices, that are configured for interference detection. However, if necessary, those devices may also be integrated into this method, as far as technically feasible.

[0008] The communication devices need to be capable to receive at least the predefined frequency bands (aka channels or spectra) that are allowed and/or licensed for the wireless non-public network of interest. The predefined frequency bands may comprise spectra within the so-called "mid-band spectrum" (1 GHz - 6 GHz). This is considered as advantageous for the intended applications, because it can carry plenty of data while traveling significant distances. Particularly for 5G networks, a spectrum between 3.3 GHz and 3.8 GHz is considered as advantageous, e.g. by the GSM Association (GSMA).

[0009] The communication devices are located in a known place. "Known place" may mean for a fixed device that its position is known from a database and/or from a message sent by this device. "Known place" may mean for a mobile device that its position is known from any positioning system, e.g. based on a satellite (like GPS and/or other country- or region-specific ones), on a corrected satellite, on position-determining systems, like the ones based, e.g., on WLAN or Bluetooth, and/or other systems that allow to determine the device's position precisely enough for this method and/or for the wireless non-public network of interest. Communication devices that are located at the same place - or very close to each

other, depending on the required position - may be evaluated as one device.

[0010] Due to the fact that the communication devices are capable to receive at least the predefined frequency bands, each one of the plurality of communication devices is able to monitor, for each frequency band in the predefined spectrum, the interfering communication signal. The monitoring may be done on demand or periodically. The monitoring demand and/or its periodicity may be controlled by the centralized network management entity. The monitoring on demand may be initiated by the centralized network management entity for checking the functionality of the system; this may be done, e.g., once per day. The monitoring on demand may, further, be initiated by the centralized network management entity as soon as at least one of the communication devices transmits an "interference occurred" message. The periodic monitoring may, for instance, be performed 0.1, 1, 10, 100 times per second, i.e. quite rarely, compared to the "productive" communication. The periodicity may be changed from time to time. The periodicity may depend on the vulnerability of the system and/or on other factors. The monitoring may be followed (possibly immediately) by transmitting the monitored information.

[0011] The monitored interfering communication signal may be transmitted, along with the communication device's known place, to the centralized network management entity. The transmitting may be done on a regular basis and/or if an interfering signal has been monitored by at least one of the communication devices. The transmitting may further be done on request by the centralized network management entity. The centralized network management entity may be similar, equal to and/or based on 5G's NME (Network Management Engine). The centralized network management entity may collect said transmitted information.

[0012] The transmitted information may be used by the centralized network management entity to detect the interfering communication signal, i.e. to determine at least an existence of the interfering communication signal.

[0013] The method advantageously uses the existing communication devices - and also already existing infrastructure and communication technology - to detect and/or to determine an interfering communication signal. Particularly, no dedicated receivers are necessary for detecting the interfering signal. Furthermore, several types of interfering signals can be detected, i.e. both jammers that spread over several frequencies or channels, and also interfering signals that have impact on only one channel, and, of course, anything in between.

[0014] In various embodiments, monitoring the communication signal comprises measuring a signal strength of the interfering communication signal. Measuring the signal strength may, e.g., be performed by using the Received Signal Strength Indicator (RSSI). Knowing the signal strength may be relevant for evaluating the seriousness of the impact.

[0015] In various embodiments, the method further comprises the step of stopping, by the centralized network management entity, any communication in the wireless non-public network, while monitoring the communication signal. The stopping may be called to define a "quiet slot". The stopping may be eased by the fact that in the wireless non-public network exists the centralized network management entity, which is able to control all the devices of this non-public network. For Orthogonal Frequency Division Multiple Access (OFDMA) systems - e.g. 5G NR, WiFi6, and/or others - the stopping may be implemented by allocating certain slots for sniffing for all subcarriers. By stopping any communication in the wireless non-public network, the interfering signal advantageously remains the only communication signal that is received by the plurality of communication devices. This may lead to a very precise determination of the existence, the type and/or the location of the interfering signal's source.

[0016] In various embodiments, determining the interfering communication signal comprises determining an existence and/or a location of a jammer that sends the interfering communication signal. Countermeasures and/or other reactions may be based on this information.

[0017] In various embodiments, the method further comprises the step of mitigating, based on determining the interfering communication signal, the effect of the interfering communication signal. The mitigating may comprise avoiding the spectrum of the interfering communication signal and/or sending an alarm that contains the spectrum of the interfering communication signal. The mitigating may further comprise enabling or increasing redundancy measures to enhance the reliability of the communication, and/or reconfiguring physical layer parameters of the wireless communication technology to enhance the network's resilience to errors.

[0018] In some embodiments, the wireless non-public network is a local 5G Non-Public Network, NPN. Using the 5G NPN may have the advantage that the communication is precisely defined by a standardization committee. This may, further, lead to lower costs of the components used.

[0019] An aspect relates to an app for a communication device that is configured for performing at least parts of a method described above and/or below.

[0020] An aspect relates to a communication device with an app as described above and/or below.

[0021] An aspect relates to a system comprising a plurality of communication devices as described above and/or below and a centralized network management entity, wherein the system is configured for performing a method as described above and/or below.

[0022] An aspect relates to a use of the system described above and/or below for a communication within a Future Industrial System.

[0023] For further elucidation, the disclosure is described by means of embodiments shown in the figures. These embodiments are to be considered as examples

only, but not as limiting.

Brief Description of the Drawings

[0024] The drawings depict:

Fig. 1 schematically a wireless non-public network according to an embodiment;
Fig. 2 schematically communication channels according to an embodiment;
Fig. 3 a flow diagram according to an embodiment.

Detailed Description of Embodiments

[0025] **Fig. 1** shows schematically a wireless non-public network 10 according to an embodiment. The wireless non-public network 10 comprises a plurality of communication devices 14x (= 14a- 14g) and 16x (= 16a, 16b). Communication devices 14x are fixed devices, communication devices 16x are mobile devices, whose direction of movement is depicted by several overlapping circles. Each one of the communication devices 14x, 16x is capable of receiving signals in a predefined spectrum or frequency band. The predefined frequency bands may be the frequency bands that are allowed and/or licensed for this wireless non-public network 10. The wireless non-public network 10 further comprises a centralized network management entity, which is configured for controlling and/or communicating with the communication devices 14x, 16x. The wireless non-public network 10 may have a neighbouring wireless non-public network 20, which may use different frequency bands. The neighbouring wireless non-public network 20 has, analogously, communication devices 24a - 24c and a neighbouring centralized network management entity 22.

[0026] The scenario shown further comprises an interfering device or jammer 30, which may send interfering communication signals, e.g. affecting several channels. The interfering signals of the jammer 30 can be monitored within an interference radius 35. Hence, the interfering signals can be monitored by the communication devices 14b, 14c, 14d, 16b, and 14e. The monitored interfering signal, along with the communication devices' known places, are then transmitted to the centralized network management entity 12. Optionally, also the signal strength of the interfering communication signal may be transmitted. With this information, at least an existence of the interfering signal be detected. In some embodiments, also the location of the jammer 30 can be detected.

[0027] With the method described above and/or below, also a different type of interfering signal can be detected. If, for instance, the neighbouring communication device 24b sends - e.g. erroneously - an interfering communication signal, this may be detected by communication device 14c, although the signal of device 24b may only affect one or two channels of the wireless non-public network 10. As a short-time countermeasure, the affected channels may be blocked by the centralized network management entity 12. As a mid-term countermeasure, the owner and/or administrator of the neighbouring wireless non-public network 20 may be informed.

[0028] **Fig. 2** shows schematically communication channels Ch [1] to Ch [5] according to an embodiment. The communication channels may be the ones the wireless non-public network 10 has licensed. It can be seen that several communication devices - e.g. communication devices 14x, 16x of **Fig. 1** - use one or more of the channels Ch [1] to Ch [5] for their regular communication 40. In some slots, an interfering signal 32 can be detected. The interfering communication signal 32 may come from a jammer 30 or from an interfering neighbouring communication device 24b. For a clear detection of the interfering signal 32, a quiet slot 50 may be inserted, e.g. controlled by the centralized network management entity 12. As an effect of inserting the quiet slot 50, all regular or "productive" communication 40 is stopped, and only the interfering signal 32 is detectable by communication devices 14x, 16x. Since the quiet slot 50 is intended to occur only rarely, the performance decrease on the "productive" communication 40 is quite small.

[0029] **Fig. 3** shows a flow diagram 100 of a method for detecting an interfering signal in a wireless non-public network 10 (see **Fig. 1)** according to an embodiment. In a step 102, a plurality of communication devices 14x, 16x is provided. The communication devices 14x, 16x are capable of receiving signals in a predefined spectrum. Each one of the plurality of communication devices 14x, 16x is located in a known place. In a step 104, the interfering communication signal is monitored by each one of the plurality of communication devices 14x, 16x and for each frequency band in the predefined spectrum. In a step 106, the monitored interfering communication signal and the communication device's known place are transmitted to a centralized network management entity 12. This is done by each one of the plurality of communication devices 14x, 16x. In a step 108, the interfering communication signal is detected by the centralized network management entity 12. The detecting is based on the monitored interfering communication signal and the known place transmitted by each one of the plurality of communication devices 14x, 16x. The steps described may be performed on demand or periodically.

List of Reference Symbols

[0030]

10	wireless non-public network
12	centralized network management entity
14x	fixed device
16x	mobile device
20	neighbouring wireless non-public network
22	neighbouring centralized network management entity
24x	neighbouring fixed devices

30 jammer
32 an interfering signal
35 interference radius
40 regular communication
50 quiet slot
100 flow diagram

Claims

1. A method for detecting an interfering communication signal (32) in a wireless non-public network (10), the method comprising the steps of:

providing a plurality of communication devices (14x, 16x) capable of receiving signals in a predefined spectrum, each one of the plurality of communication devices (14x, 16x) located in a known place;
monitoring, by each one of the plurality of communication devices (14x, 16x), for each frequency band in the predefined spectrum, the interfering communication signal;
transmitting, by each one of the plurality of communication devices (14x, 16x), the monitored interfering communication signal and the communication device's known place to a centralized network management entity (12); and
detecting, by the centralized network management entity (12), the interfering communication signal (32), based on the monitored interfering communication signal and the known place transmitted by each one of the plurality of communication devices (14x, 16x).

2. The method of claim 1,
wherein the monitoring is performed on demand or periodically.

3. The method of claim 2,
wherein the periodic monitoring is performed 0.1, 1, 10, 100 times per second.

4. The method of any one of the preceding claims,
wherein a communication device of the plurality of communication devices (14x, 16x) is a fixed device (14x) or a mobile device (16x).

5. The method of any one of the preceding claims,
wherein monitoring the interfering communication signal (32) comprises measuring a signal strength of the interfering communication signal (32).

6. The method of any one of the preceding claims, further comprising the step of:
stopping, by the centralized network management entity (12), any communication in the wireless non-public network (10), while monitoring the interfering communication signal (32).

7. The method of any one of the preceding claims,
wherein determining the interfering communication signal comprises determining an existence and/or a location of a jammer (30) that sends the interfering communication signal (32).

8. The method of any one of the preceding claims, further comprising the step of:
mitigating, based on determining the interfering communication signal, the effect of the interfering communication signal (32).

9. The method of claim 8,
wherein mitigating comprises avoiding the spectrum of the interfering communication signal and/or sending an alarm that contains the spectrum of the interfering communication signal (32).

10. The method of any one of the preceding claims,
wherein the wireless non-public network (10) is a local 5G Non-Public Network, NPN.

11. An app for a communication device (14x, 16x), configured for performing at least parts of a method of any one of the preceding claims.

12. A communication device (14x, 16x) with an app according to claim 11.

13. A system comprising a plurality of communication devices (14x, 16x) according to claim 12 and a centralized network management entity (12), the system configured for performing a method of any one of the claims 1-10.

14. Use of a system according to claim 13 for a communication and for detecting an interfering communication signal within a Future Industrial System.

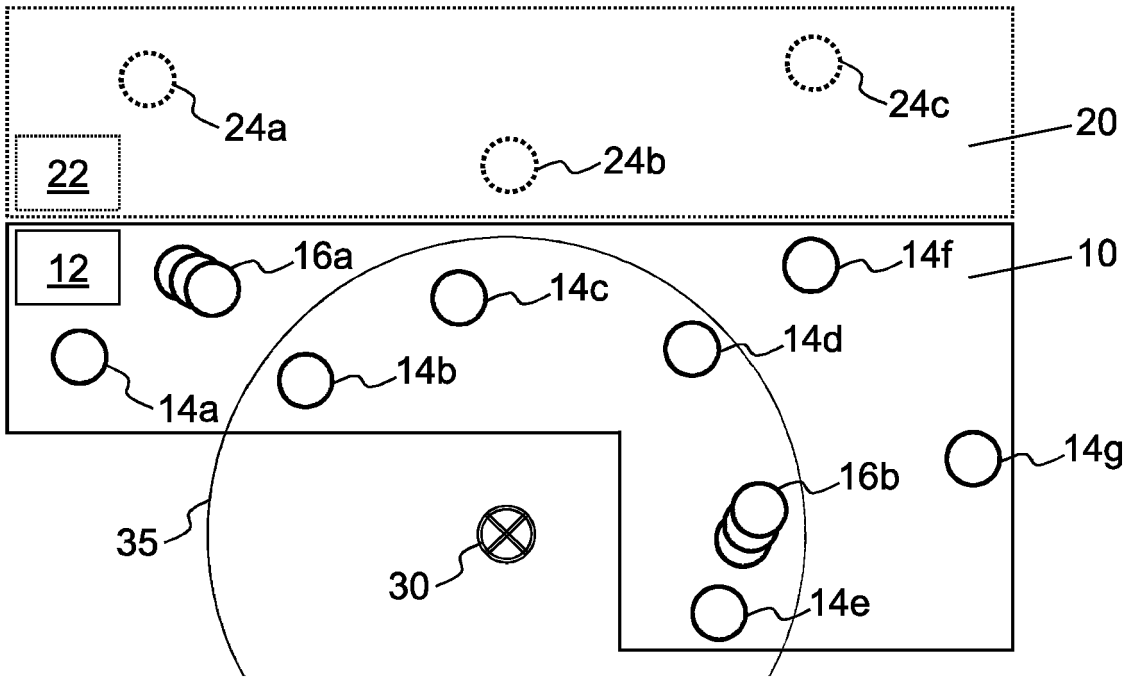
24a
24c
20
22
24b
12
16a
14f
10
14c
14d
14b
14a
14g
16b
35
30
14e

Fig. 1

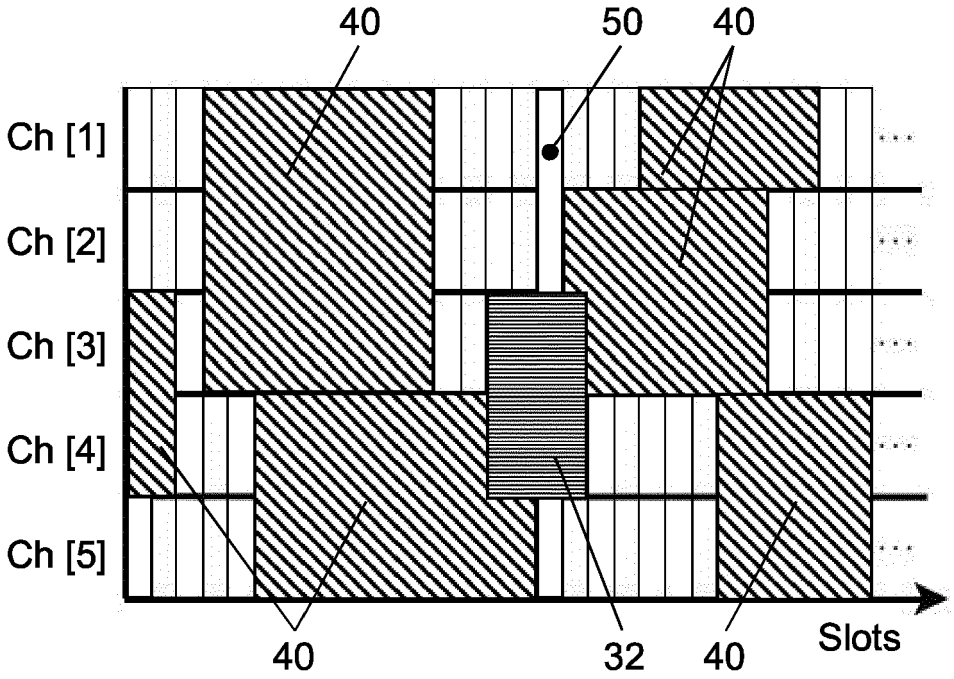
40
50
40
Ch [1]
Ch [2]
Ch [3]
Ch [4]
Ch [5]
40
32
40
Slots

Fig. 2

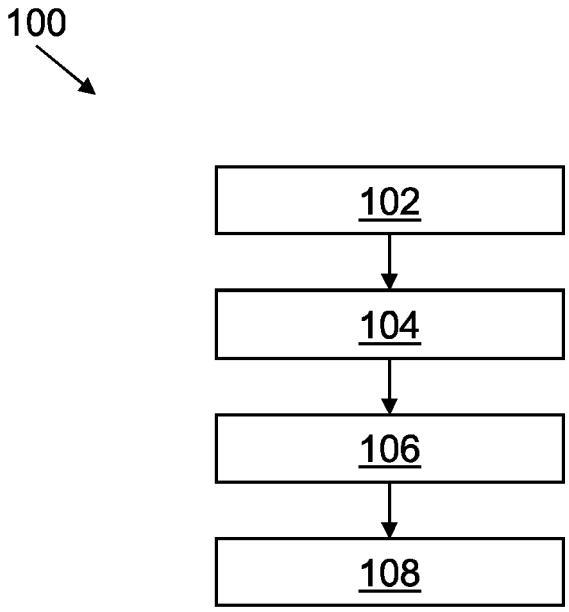

Fig. 3

Europäisches Patentamt
European Patent Office
Office européen des brevets

EUROPEAN SEARCH REPORT

Application Number
EP 23 22 0615

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (IPC)
X	WO 2023/172172 A1 (ERICSSON TELEFON AB L M [SE]) 14 September 2023 (2023-09-14) * abstract * * page 1, line 10 - page 4, line 3 * * page 4, line 26 - page 18, line 27 * * figures 1-11 * -----	1-14	INV. H04K3/00

TECHNICAL FIELDS SEARCHED (IPC)

H04K
H04W

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
The Hague	21 May 2024	Dujardin, Corinne

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons
.....
& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 23 22 0615

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

21-05-2024

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2023172172 A1	14-09-2023	NONE	

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82