

(51) International Patent Classification:
H04W 16/14 (2009.01)(21) International Application Number:
PCT/EP2017/066880(22) International Filing Date:
06 July 2017 (06.07.2017)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
16305869.6 11 July 2016 (11.07.2016) EP(71) Applicant: **ALCATEL LUCENT** [FR/FR]; 148/152 route de la Reine, 92100 Boulogne-Billancourt (FR).(72) Inventors: **LIGATA, Amir**; Copernicuslaan 50, 2018 Antwerpen (BE). **GACANIN, Haris**; Copernicuslaan 50, 2018 Antwerpen (BE). **ABOU SALEH, Ahmad**; Copernicuslaan 50, 2018 Antwerpen (BE).(74) Agent: **ALU ANTW PATENT ATTORNEYS (NO 365)**; Copernicuslaan 50, 2018 Antwerp (BE).

(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM,

AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:

— with international search report (Art. 21(3))

(54) Title: METHOD AND DEVICE FOR CONTROLLING A WIRELESS ACCESS POINT

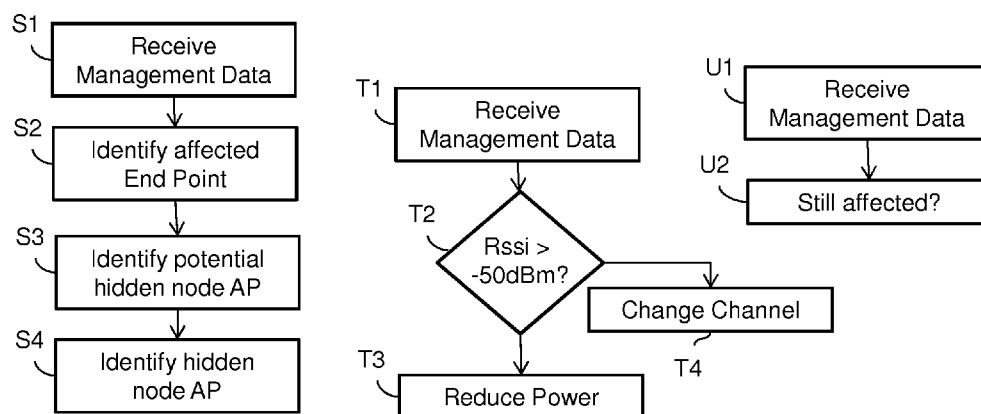


FIG. 2

(57) **Abstract:** Embodiments relate to a method for controlling a wireless access point (3), executed by a control device (2), comprising: - receiving (S1), from a target wireless access point (3), management data representative of, for respective wireless end points (4) associated with the target wireless access point (3), a received signal strength and a number of retransmissions, and IDs associated with neighboring wireless access points (3) detected by the target wireless access point (3), - identifying (S2) at least one wireless end point (4) affected by a hidden node problem in function of the corresponding received signal strength and number of retransmissions, - identifying (S3) at least one potential hidden node in function of a channel used and a received signal strength of the detected neighboring wireless access points (3), - identifying (S4) a hidden node wireless access point (3) by comparing the wireless access points (3) detected by the wireless end point (4) identified as affected by a hidden node problem and the identified potential hidden node.



- 1 -

Method and device for controlling a wireless access point

FIELD OF THE INVENTION

The present invention relates to the field of telecommunications. In particular, the present invention relates to a method and a device for controlling a wireless access point, in particular in view of the hidden node problem.

BACKGROUND

One of the most common problems in Wi-Fi networks is related to interference. Dense deployments of Wi-Fi access points (APs) lead to a coverage overlapping which might have negative impact on the end-user's performance in the case that the neighboring APs operate on the same or adjacent – nonorthogonal (with distance lower than 5) WLAN channels.

One should clearly distinguish two scenarios:

- (1) Exposed node scenario, where the neighboring APs (operating on the same or adjacent channels) sense each other and adapt their transmission in line with the CSMA protocol. In this case, there is no direct interference between them (no package collision). Instead, the common resources (frequency) are being shared which results in lower achievable throughput for both networks.
- (2) Hidden node scenario, where the neighboring APs don't sense each other but their coverage areas overlap. In such a scenario, the users located in the overlapping areas will be affected by downlink transmission from the neighboring - interfering AP. This is considered as a direct interference. This increases the number of retransmissions significantly. Moreover, these users usually do not experience high rssi levels, meaning that their performance can easily deteriorate.

Hidden node scenario is one of the most severe interference problems, and as such, has to be carefully studied. Known techniques related to the hidden node problem comprise:

- Hidden node detection in dense Wi-Fi networks using MAC packet analysis aggregated from multiple APs.
- Differentiation of the packet loss due to collisions or hidden node.
- Detecting the hidden node, based on inspection of the MAC layer packet headers.
- Hidden node removal driven by the physical carrier sensing (PCS) threshold tuning – that results with reduced coverage (shortening the maximum link length) and potential exposed node problems.

- 2 -

Nonetheless, the above mentioned techniques were tested and validated on the level of simulations with a lot of assumptions and simplifications, and thus may be difficult to implement. Furthermore, a feasible method to overcome a problem of hidden node has yet to be addressed.

5

SUMMARY

10 It is thus an object of embodiments of the present invention to propose a method and a device for controlling a wireless access point, which do not show the inherent shortcomings of the prior art.

Accordingly, embodiments relate to a method for controlling a wireless access point, executed by a control device, comprising:

- 15 - receiving, from a target wireless access point, management data representative of, for respective wireless end points associated with the target wireless access point, a received signal strength and a number of retransmissions and of, for respective neighboring wireless access points detected by the target wireless access point, an ID, a received signal strength and a channel used,
- 20 - identifying at least one wireless end point affected by a hidden node problem in function of the corresponding received signal strength and number of retransmissions,
- identifying at least one potential hidden node in function of the channel used and the received signal strength of a detected neighboring wireless access points,
- 25 - identifying a hidden node wireless access point by comparing the wireless access points detected by the wireless end point identified as affected by a hidden node problem and the identified potential hidden node.

Correspondingly, embodiments relate to a control device for controlling a wireless access point, comprising:

- 30 - means for receiving, from a target wireless access point, management data representative of, for respective wireless end points associated with the target wireless access point, a received signal strength and a number of retransmissions and of, for respective neighboring wireless access points detected by the target wireless access point, an ID, a received signal strength and a channel used,
- 35 - means for identifying at least one wireless end point affected by a hidden node problem in function of the corresponding received signal strength and number of retransmissions,

- 3 -

- means for identifying at least one potential hidden node in function of the channel used and the received signal strength of a detected neighboring wireless access points,

5 - means for identifying a hidden node wireless access point by comparing the wireless access points detected by the wireless end point identified as affected by a hidden node problem and the identified potential hidden node.

10 In some embodiments, wherein identifying at least one wireless end point affected by a hidden node problem comprises determining whether a corresponding received signal strength is below a first threshold and whether a corresponding number of retransmissions is above a second threshold.

Identifying at least one potential hidden node may comprise, for a neighboring wireless access point using the same channel as the target wireless access point, determining whether the received signal strength of said neighboring wireless access point is above a third threshold.

15 Identifying at least one potential hidden node may comprise, for a neighboring wireless access point using a different channel than the target wireless access point, determining whether the received signal strength of said neighboring wireless access point is above a fourth threshold which depends on a channel separation.

20 The method may comprise controlling the identified hidden node wireless access point by reducing power and/or changing channel.

25 The method may comprise comprising, after controlling the identified hidden node wireless access point, checking whether the identified wireless end point is still affected by a hidden node problem, in function of the corresponding received signal strength and number of retransmissions.

Embodiments also relate to a computer program comprising instructions for performing the method mentioned before when said instructions are executed by a computer.

30 BRIEF DESCRIPTION OF THE DRAWINGS

The above and other objects and features of the invention will become more apparent and the invention itself will be best understood by referring to the following description of embodiments taken in conjunction with the accompanying drawings wherein:

35 Figure 1 is a bloc diagram of a telecommunication network,

Figure 2 is a flowchart of a method for controlling a wireless access point in the network of Figure 1, and

Figure 3 is structural view of a control device for executing the method of Figure 2.

- 4 -

DESCRIPTION OF EMBODIMENTS

Figure 1 is a bloc diagram of a telecommunication network 1. The telecommunication network 1 comprises (among other), a control device 2, one or
5 more wireless access points 3 and one or more wireless end points 4.

A wireless access point 3 and a wireless end point 4 are configured for wireless communication according to a wireless local area network protocol, for example the IEEE 802.11 standard (Wi-Fi). When a wireless end point 4 is located in the coverage area of two wireless access points 3, but the wireless access points
10 3 cannot sense each other, the wireless end point 4 may be affected by the hidden node problem.

In an example, a wireless access point 3 is a gateway for broadband access to an operator's network and a wireless end point 4 is a user terminal.

At least one of the wireless access points 3 is a managed node. The control device 2 may obtain management data from a managed node and send configuration data to a managed node, for example based on the Broadband
15 Forum Technical Recommendation TR-181. The control device 2 is for example a server within an operator's network.

Similarly, at least one of the wireless end point 4 is a managed node. For example, a managed wireless end point 4 executes an app installed by the network operator. The app collects management data (for example, performs a WiFi scan) and sends the collected management data in response to a request from
20 the control device 2.

In the telecommunication network 1, the control device 2 may detect a hidden node problem in function of the obtained management data, and take corrective actions in response to detecting a hidden node problem, as will be
25 described in more details with reference to Figure 2.

Figure 2 is a flowchart of a method for controlling a wireless access point 3, executed by the control device 2. Hereafter, the wireless access point 3 controlled by the control device 2 may be referred to as the target wireless access point or the target AP, and other wireless access points 3 may be referred to as
30 neighboring wireless access points.

The control device 2 receives management data from the wireless access point 3 (Step S1). The management data specify at least one of:
35

- For respective wireless end points 4 associated with the target wireless access point 3, a received signal strength and a number of retransmissions (for example a retransmission counter). This is for example specified by

- 5 -

Device.WiFi.AccessPoint.{i}.AssociatedDevice.{i}.SignalStrength and Device.WiFi.AccessPoint.{i}.AssociatedDevice.{i}.Retransmissions according to TR-181.

- 5 - For respective neighboring wireless access points 3 detected by the target wireless access point 3, an ID (for example SSID), a received signal strength (for example rssi), a channel in use. This is for example specified by Device.WiFi.NeighboringWiFiDiagnostic.Result.{i} of TR-181.

10 Then, the control device 2 identifies wireless end points 4 affected by the hidden node problem in function of the received management data (Step S2). More specifically, a end point 4 affected by the hidden node problem may be identified for example in response to determining that the received signal strength is below a predetermined threshold and that the retransmission counter is above a predetermined threshold. For example if, for a wireless end point 4, rssi is below -
15 55dBm and retransmission > TH, where TH is a threshold which may be derived experimentally and may be function of the rssi, the wireless end point 4 is identified as affected by the hidden node problem.

20 The control device 2 obtains, from the identified wireless end point 4, management data specifying IDs (for example SSID) associated with neighboring wireless access points 3 detected by the identified wireless end points 4 (for example through Wi-Fi scan).

25 Then, the control device 2 identifies potential hidden nodes among the neighboring wireless access point 3 detected by the target AP (Step S3). More specifically, the control device 2 classifies the detected neighboring wireless access points 3 as either exposed node or potential hidden node in function of the channel used and the received signal strength of the neighboring wireless access point 3. For example:

- 30 - For a neighboring AP{j} operating on the same channel as the target AP, if $rssi(j) > CCA\ threshold$, the control device 2 keeps AP{j} in an exposedNode list, and if $rssi(j) < CCA\ threshold$, the control device 2 keeps AP{j} in a potential hiddenNode list, where CCA threshold is a Clear Channel Assessment threshold.
- 35 - For a neighboring AP{j} operating on an adjacent non-orthogonal channel, if $rssi(j) - A(j-i) > EDthreshold$, where "i" is the target AP channel, A(.) is an attenuation factor given by Table 1, and EDthreshold is the energy detection threshold, the control device 2 keeps the neighboring AP{j} in the exposedNode list, and if $rssi(j) - A(j-i) < EDthreshold$, the control device 2 keeps the neighboring AP{j} in the potential hiddenNode list. Note that this is equivalent to

- 6 -

comparing the rssi with a threshold which depends on the channel separation.

Channel Separation	1	2	3	4	5
A(i)	0.55	2.46	6.6	34.97	51.87

Table 1

5

Here, it should be remarked that this does not contradict the definition of an hidden node. Indeed, the hidden nodes can be sensed by the target AP but with low rssi, and because of that they will not contend (rssi is below CCA threshold), meaning that they can transmit at the same time. For instance, the target AP can sense neighbors with rssi all the way to -95dBm (noise floor) but will contend only with those that have rssi above CCA threshold, say -82dBm. So all neighboring APs with rssi between -82dBm and -95dBm are considered as a potential hidden node. However, a wireless end point 4 may sense this hidden node with higher rssi – in case the end point is between the target AP and the hidden node.

10 Then, the control device 2 identifies a hidden node in function of the end points 4 affected by the hidden node problem identified at step S2 and of potential hidden node identified at step S3 (Step S4). For example, if a wireless access point 3 AP{k} is on the neighboring AP list of an affected end point 4 and on the potential hiddenNode list of the target AP, AP{k} is identified as a hidden node.

15 In case the identified hidden node is also a managed node (e.g. another Wi-Fi gateway from the same operator's network), then the control device 2 may take corrective actions. Accordingly, the control device 2 obtains management data from the neighboring wireless access point 3 identified as the hidden node (Step T1). The management data specify, for respective wireless end points 4 associated with the neighboring wireless access point 3, a received signal strength. This is for example specified by Device.WiFi.AccessPoint.{i}.AssociatedDevice.{i}.SignalStrength according to TR-181.

20 Then, the control device 2 compares the received signal strengths with a predetermined threshold (Step T2). For example, the control device 2 determines, for the respective wireless end points 4, whether rssi > -50 dBm.

25 If all associated devices have a signal strength higher than the threshold, they have strong coverage potential, and reducing the power level at the neighboring wireless access point 3 won't impact their achievable throughput. If so, the control device 2 reduces the power level of the neighboring AP (Step T3), for example from 100% to 50%, so that the affected user is no longer in coverage area of the neighboring network or it can hardly sense it.

30

35

- 7 -

In contrast, if one (or more) of the users have signal strengths below -50dBm, the control device 2 controls the neighboring wireless access point 3 to select an orthogonal channel (Step T4).

5 After the corrective operation, the control device 2 checks whether the wireless end point 4 identified as affected by the hidden node problem is still affected.

Accordingly, the control device 2 obtains the rssi level of the neighboring network (i.e., hidden node) at the wireless end point 4 (Wi-Fi scan), and the retransmission counter of the wireless end point 4 (Step U1).

10 Then, if the affected device can hardly, or no longer sense the neighboring network, and retransmission counter is reasonably low, the control device 2 determines that the affected device is no longer affected (Step U2).

Steps S1-S4, T1-T4, U1 and U2 have been described as successive steps, but they may be executed in another order, in parallel, repeated in time... A
15 wireless access point 3 may be regarded both as the target AP (steps S1-S4) and a neighboring AP (steps T1-T4) for another target AP, for example successively or in parallel.

20 In the telecommunication network 1, a wireless end point 4 affected by the hidden node problem and the corresponding hidden node may be identified efficiently in function of management data obtained from the network elements. Moreover, corrective actions may remove the hidden node problem.

Figure 3 is a structural view of the control device 2, which comprises a
25 processor 5 and a memory 6. The memory 6 stores a computer program P which, when executed by the processor 5, causes the control device 2 to execute the method described above with reference to Figure 2.

30 It is to be remarked that the functions of the various elements shown in the figures may be provided through the use of dedicated hardware as well as hardware capable of executing software in association with appropriate software. When provided by a processor, the functions may be provided by a single dedicated processor, by a single shared processor, or by a plurality of individual processors, some of which may be shared, for example in a cloud computing
35 architecture. Moreover, explicit use of the term "processor" should not be construed to refer exclusively to hardware capable of executing software, and may implicitly include, without limitation, digital signal processor (DSP) hardware, network processor, application specific integrated circuit (ASIC), field programmable gate array (FPGA), read only memory (ROM) for storing software, random access

- 8 -

memory (RAM), and non volatile storage. Other hardware, conventional and/or custom, may also be included. Their function may be carried out through the operation of program logic, through dedicated logic, through the interaction of program control and dedicated logic, or even manually, the particular technique
5 being selectable by the implementer as more specifically understood from the context.

It should be further appreciated by those skilled in the art that any block diagrams herein represent conceptual views of illustrative circuitry embodying the principles of the invention. Similarly, it will be appreciated that any flow charts
10 represents various processes which may be substantially represented in computer readable medium and so executed by a computer or processor, whether or not such computer or processor is explicitly shown.

Embodiments of the method can be performed by means of dedicated hardware and/of software or any combination of both.

15 While the principles of the invention have been described above in connection with specific embodiments, it is to be clearly understood that this description is made only by way of example and not as a limitation on the scope of the invention, as defined in the appended claims.

CLAIMS

1. Method for controlling a wireless access point (3), executed by a control device (2), comprising:

- 5 - receiving (S1), from a target wireless access point (3), management data representative of, for respective wireless end points (4) associated with the target wireless access point (3), a received signal strength and a number of retransmissions and of, for respective neighboring wireless access points (3) detected by the target wireless access point (3), an ID, a received signal strength
10 and a channel used,
- identifying (S2) at least one wireless end point (4) affected by a hidden node problem in function of the corresponding received signal strength and number of retransmissions,
- identifying (S3) at least one potential hidden node in function of the channel used
15 and the received signal strength of a detected neighboring wireless access points (3),
- identifying (S4) a hidden node wireless access point (3) by comparing the wireless access points (3) detected by the wireless end point (4) identified as affected by a hidden node problem and the identified potential hidden node.

20

2. Method according to claim 1, wherein identifying (S2) at least one wireless end point (4) affected by a hidden node problem comprises determining whether a corresponding received signal strength is below a first threshold and whether a corresponding number of retransmissions is above a second threshold.

25

3. Method according to claim 1 or 2, wherein identifying at least one potential hidden node comprises, for a neighboring wireless access point using the same channel as the target wireless access point, determining whether the received signal strength of said neighboring wireless access point is above a third threshold.

30

4. Method according to one of claims 1 to 3, wherein identifying at least one potential hidden node comprises, for a neighboring wireless access point using a different channel than the target wireless access point, determining whether the received signal strength of said neighboring wireless access point is above a fourth threshold which depends on a channel separation.

35

5. Method according to one of claims 1 to 4, comprising controlling the identified hidden node wireless access point by reducing power (T3) and/or changing channel (T4).

- 10 -

6. Method according to claim 5, comprising, after controlling the identified hidden node wireless access point, checking (U1, U2) whether the identified wireless end point (4) is still affected by a hidden node problem, in function of the
5 corresponding received signal strength and number of retransmissions.

7. Computer program (P) comprising instructions for performing the method of one of claims 1 to 6 when said instructions are executed by a computer.

10 8. Control device (7) for controlling a wireless access point (3), comprising:
- means (5, 6, P) for receiving (S1), from a target wireless access point (3), management data representative of, for respective wireless end points (4) associated with the target wireless access point (3), a received signal strength and a number of retransmissions and of, for respective neighboring wireless access points
15 (3) detected by the target wireless access point (3), an ID, a received signal strength and a channel used,
- means (5, 6, P) for identifying (S2) at least one wireless end point (4) affected by a hidden node problem in function of the corresponding received signal strength and number of retransmissions,
20 - means (5, 6, P) for identifying (S3) at least one potential hidden node in function of the channel used and the received signal strength of a detected neighboring wireless access points (3),
- means (5, 6, P) for identifying (S4) a hidden node wireless access point (3) by comparing the wireless access points (3) detected by the wireless end point (4)
25 identified as affected by a hidden node problem and the identified potential hidden node.

- 1/1 -

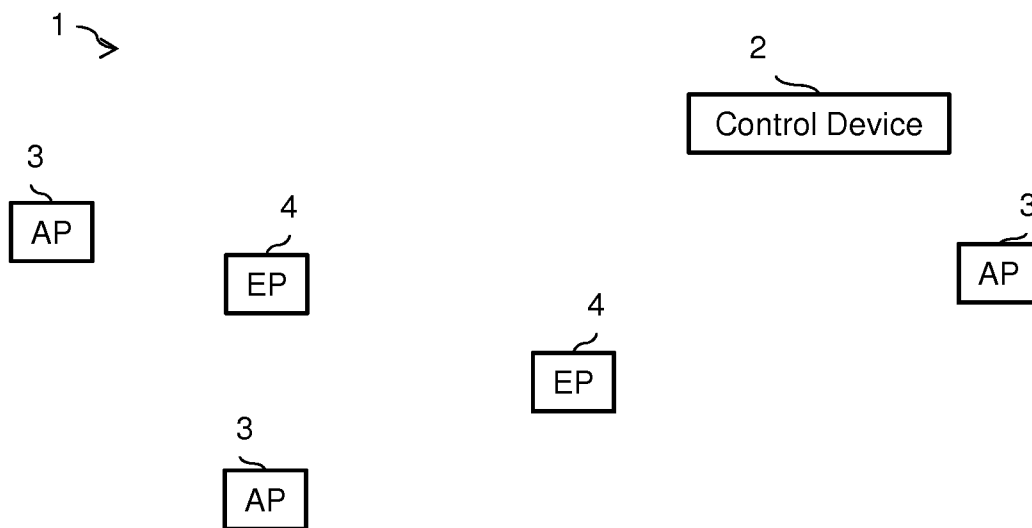


FIG. 1

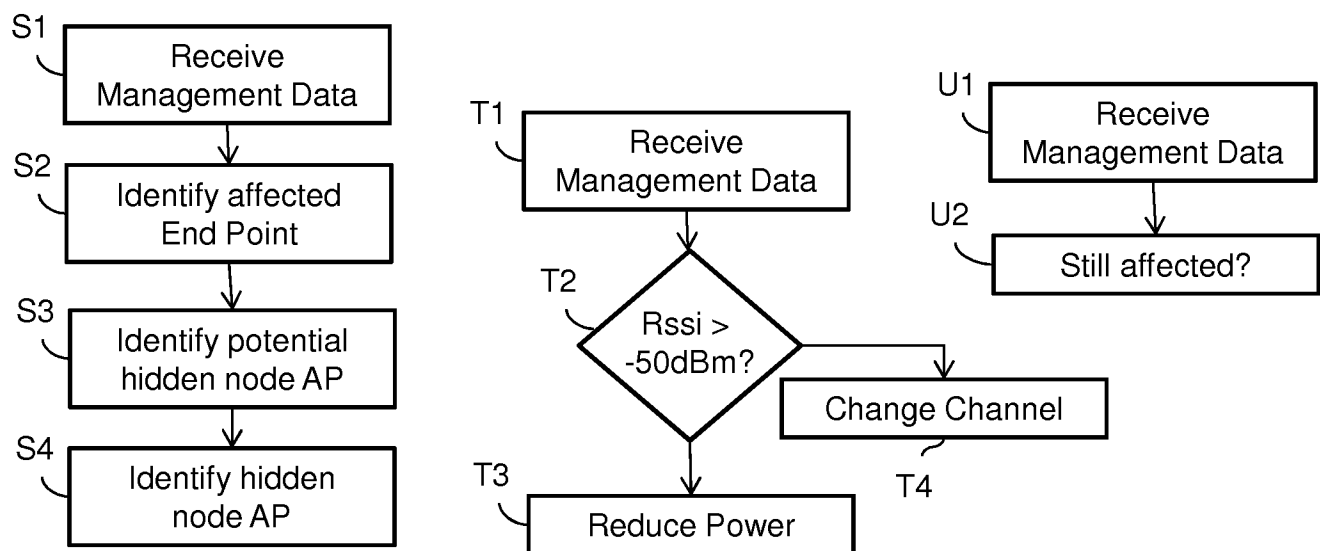


FIG. 2

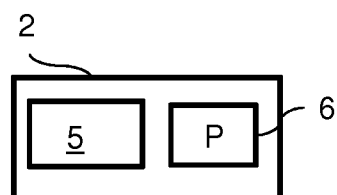


FIG. 3

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2017/066880

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04W16/14
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04W

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EP0-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 2016/086985 A1 (NOKIA SOLUTIONS & NETWORKS OY [FI]) 9 June 2016 (2016-06-09) abstract; claims 1,2 ----- -/--	1-8



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

28 August 2017

Date of mailing of the international search report

04/09/2017

Name and mailing address of the ISA/

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040,
Fax: (+31-70) 340-3016

Authorized officer

Schweitzer, J

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2017/066880

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	SHO MOTEGI ET AL: "A directional MAC protocol with the DATA-frame fragmentation and short busy advertisement signal for mitigating the directional hidden node problem", 2012 IEEE 23RD INTERNATIONAL SYMPOSIUM ON PERSONAL, INDOOR AND MOBILE RADIO COMMUNICATIONS (PIMRC 2012) : SYDNEY, AUSTRALIA, 9 - 12 SEPTEMBER 2012, IEEE, PISCATAWAY, NJ, 9 September 2012 (2012-09-09), pages 393-398, XP032273009, DOI: 10.1109/PIMRC.2012.6362817 ISBN: 978-1-4673-2566-0 the whole document -----	1,7,8
A	TIM FARNHAM: "REM based approach for hidden node detection and avoidance in cognitive radio networks", GLOBAL COMMUNICATIONS CONFERENCE (GLOBECOM), 2012 IEEE, IEEE, 3 December 2012 (2012-12-03), pages 1391-1397, XP032374865, DOI: 10.1109/GLOCOM.2012.6503308 ISBN: 978-1-4673-0920-2 the whole document -----	1,7,8
A	WO 2015/081990 A1 (ERICSSON TELEFON AB L M [SE]) 11 June 2015 (2015-06-11) abstract; claim 1 -----	1,7,8

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/EP2017/066880

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2016086985 A1	09-06-2016	CN 107079302 A WO 2016086985 A1	18-08-2017 09-06-2016
WO 2015081990 A1	11-06-2015	NONE	