

(51) International Patent Classification:
H04W 74/08 (2009.01)(21) International Application Number:
PCT/IB2012/052393(22) International Filing Date:
14 May 2012 (14.05.2012)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
1108509.9 20 May 2011 (20.05.2011) GB(71) Applicant (for all designated States except US): **CANON KABUSHIKI KAISHA** [JP/JP]; 3-30-2, Shimomaruko, 3-chome, Ohta-ku, Tokyo (JP).

(72) Inventors; and

(75) Inventors/Applicants (for US only): **NEZOU, Patrice** [FR/FR]; Chemin du Pré Thébault, F-35250 Saint Sulpice La Foret (FR). **SEVIN, Julien** [FR/FR]; 11 Allée du Luxembourg, F-35140 Saint Aubin du Cormier (FR). **VIGER, Pascal** [FR/FR]; Le Mesnil, F-35150 Janze (FR).(74) Agent: **SANTARELLI**; B.P. 237, 14 avenue de la Grande-Armée, F-75822 Paris Cedex 17 (FR).

(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, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, 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, 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, ML, MR, NE, SN, TD, TG).

Published:

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

(54) Title: METHOD AND DEVICE FOR OPTIMIZING ACCESS TO A MEDIUM IN A COMMUNICATION NETWORK

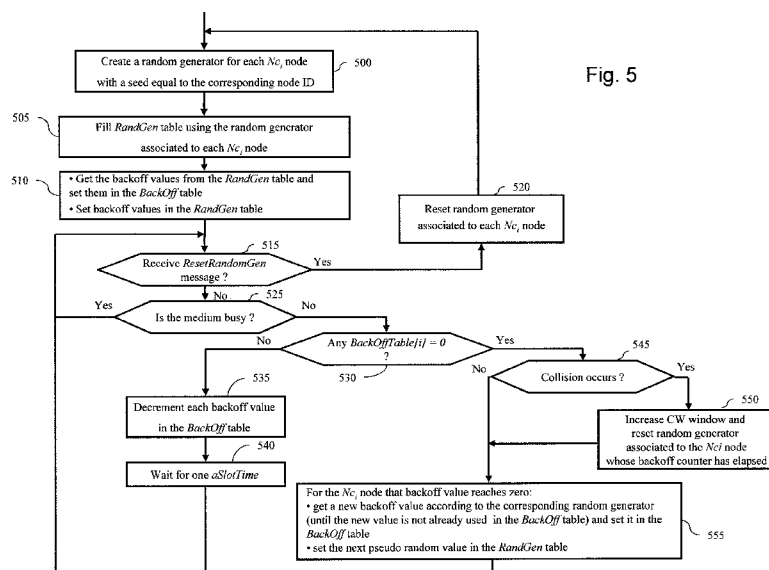


Fig. 5

(57) Abstract: The invention is directed to the optimization of an access to a medium in wireless networks which can be accessed by a plurality of nodes, each node of the plurality of nodes using a medium access mechanism of the Carrier Sense Multiple Access with Collision Avoidance type based on a computation of a backoff value. A specific value is associated with each node of a set of nodes of the plurality of nodes, the specific value of a node being known by the other nodes of the set of nodes. According to the invention, a backoff value is determined (505, 510) for each node of the set of nodes, in each node of the set of nodes, the backoff value associated with a node being determined as a function of the specific value associated with that node.

METHOD AND DEVICE FOR OPTIMIZING ACCESS TO A MEDIUM IN A COMMUNICATION NETWORK

5

The present invention relates generally to wireless communication networks and more specifically to a method and a device for optimizing sharing of backoff values for collision avoidance in wireless networks so as to optimize the medium access in a wireless communication network based on contention avoidance medium access mechanism.

10

The 802.11 MAC (acronym of *Medium Access Control*) standard supports shared accesses to a wireless medium through a technique called Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA). The 802.11 standard is mainly directed to the waiting management of nodes waiting for the medium to become idle so as to authorize access to the medium.

15

According to a communication mode of that standard, known as Distributed Coordination Function Carrier Sense Multiple Access with Collision Avoidance (DCF), a wireless channel, generically referred to as the medium, is sensed by a source node so that transmission of data packets from the source node to a destination node is permitted when the sensed wireless channel is idle. If the channel is sensed as being busy, the source node defers its transmission.

20

The backoff algorithm is a well-known method to solve contention between different source nodes that need to access a medium (typically a wireless channel) simultaneously: the method requires each of these nodes to choose a random number of time units, called backoff value or backoff period, and wait for that number of time units to elapse before accessing the medium, continuously checking (each time unit) whether or not another node accesses the medium.

25

Therefore, when the medium becomes idle, the source node waits for a random backoff period to elapse during which it continues to sense the medium. At the end of that period and if the medium is still idle, the source node

30

begins transmitting data packets. The random backoff period reduces the risk of collision between data packets transmitted by the given source node and other source nodes since the other source nodes waiting to access the medium are likely to use a different random backoff period.

5 It is to be recalled that the time unit in the 802.11 standard is the slot time generally called *aSlotTime* parameter. This parameter is specified by the physical layer (PHY). It is, for example, equal to 9 μ s for the 802.11n standard. All the dedicated time periods, for example SIFS, PIFS, and DIFS, are multiples of that time unit.

10 The Short Inter-Frame Space (SIFS) is used to separate a response frame from the frame that requested the response, for example between a data frame and the acknowledgement response. The SIFS is, for example, equal to 16 μ s according to the 802.11n standard. The PCF Inter-Frame Space (PIFS) provides the next highest access priority time space after the SIFS time ($PIFS =$
15 $SIFS + aSlotTime$). The DCF Inter-Frame Space (DIFS) defines the minimum waiting time, after detecting that a medium is idle, before a transmitting node can attempt to transmit data packets ($DIFS = SIFS + 2 \times aSlotTime$). The different inter-frame space durations provide access to a wireless medium at different priority levels.

20 Figure 1 is a time diagram illustrating the DCF and backoff access mechanism for accessing a communication medium for transmitting data packets. In the given example, three different source nodes, referred to as node A, node B, and node C, need to access the medium.

 As depicted with triangular marks, node B needs to transmit data at
25 time t_0 while node A is transmitting data packets. Similarly, node C needs to transmit data at time t_1 while node A is still transmitting data packets.

 However, a node must first sense the medium over a DIFS duration before initiating any transmission on the wireless medium. If the wireless medium is still idle at the end of the DIFS duration, the transmitting node
30 initiates its transmission process. To that end, it invokes a backoff procedure using a backoff counter to count down a backoff value (corresponding to a

number of time units) randomly obtained from a range defined by zero and a contention window (CW) value ($[0; CW]$).

It is to be noted that when the wireless medium goes from a busy to an idle state, several nodes may be ready to send data packets. To minimize collisions, the nodes that need to initiate data transfers select a random backoff value and defer communication for the corresponding number of time units. The random backoff value is generally a pseudo-random integer determined according to a uniform distribution over the range $[0, CW]$. The contention window (CW) parameter varies from a minimum value (CW_{min}) to a maximum value (CW_{max}). According to the backoff mechanism, the contention window (CW) parameter is increased on each erroneous transmission, that is to say on each collision on the medium, until it reaches the CW_{max} value. It is reset to the CW_{min} value after each successful data transmission.

To begin the random backoff procedure in a node, the latter selects a random backoff value in the range $[0, CW]$. All backoff slots (of length $aSlotTime$) occur in the backoff window or contention window following a DIFS duration during which the medium is sensed to be idle. During each backoff slot, the node continues to sense the wireless medium. If the wireless medium becomes busy during a backoff slot, the backoff procedure is frozen until the wireless medium again becomes idle. The backoff counter is then resumed after a DIFS duration.

Accordingly, returning to Figure 1, node B is sensing the medium from time t_0 to detect its idle state. Likewise, node C is sensing the medium from time t_1 . At time t_2 , both nodes B and C determine that the medium is no longer busy. Therefore, at time t_3 , that is to say after having determined that the medium is still idle at the end of the DIFS duration, the backoff value associated with each node waiting to transmit data (i.e., nodes B and C) is decreased until one of the values reaches zero. When a backoff value reaches zero, the corresponding node initiates a transmission.

When it is detected that the medium is no longer in its idle state, counting down the backoff value is suspended in each of those waiting nodes.

As shown in Figure 1, the backoff values of nodes B and C are decreased from time t_3 until the medium is no longer in an idle state (or until one of the backoff values reaches zero since, in such a case, one of those waiting nodes accesses the medium that consequently is no longer in the idle state).

- 5 For the sake of illustration, it is assumed that the backoff value associated with node C reaches zero at time t_4 . Accordingly, node C can access the medium for transmitting data while counting down the backoff value associated with node B is suspended.

- 10 If collision occurs at time t_3 , the transmitting node invokes a new backoff procedure by increasing the range of the collision window to determine a new number of backoff time units (such procedure is called Exponential Backoff Algorithm in the standard).

- 15 Time t_5 designates here the time at which the backoff value associated with node B would have reached zero if it had not been suspended at time t_4 . The value of the backoff value associated with node B at time t_4 is called the remaining backoff value.

- 20 When node C ceases to use the medium, at time t_6 , node B determines that the medium is in an idle state. Accordingly, after the following DIFS duration (i.e. at time t_7), the backoff mechanism is invoked and the backoff value associated with node B is decreased (starting from its remaining value as illustrated) so that node B can access the medium if it is still in an idle state when the backoff value reaches zero (time t_8).

- 25 According to the example given with reference to Figure 1, the node having the smallest backoff value (node C) wins the contention resolution mechanism and transmits its data packets first. The remaining nodes suspend their backoff procedure and resume with a DIFS time after the medium goes idle again. The node with the next smallest backoff value (node B) counts down the remaining backoff value and is the next to win the medium access.

- 30 In a network using a CSMA/CA medium access mechanism, it is not possible to guarantee medium access. This may lead to difficulties in transporting data such as video streams requiring low latency.

There exist solutions that cope with such a problem. For example, the system disclosed in US Patent Application No. 2009/0141738 uses a reservation-based distributed collision avoidance channel access in a wireless area network. By advertising the future channel access parameters in advance, nodes reduce the number of collisions. At the end of a data transmission, the corresponding node publishes its future backoff value and all other nodes store the published backoff value in a reservation table so as to avoid collision for its own future medium access attempts. If a node detects that a collision would occur with another node having published its next backoff value, it reschedules its next access attempts.

However, although such a solution may solve the above mentioned problem, its protocol requires heavy message exchanges for the distribution of backoff values. It requires a node to obtain channel access before advertising its backoff value. It is also sensitive to transmission errors and requires a bandwidth overhead.

Therefore, there is a need to provide a method and a device for improving network access using a CSMA/CA medium access mechanism.

Thus, it is a general object of the invention to remedy the shortcomings of the prior art as described here above.

To that end, the present invention concerns, in particular, a method for optimizing access to a medium in a communication network which can be accessed by a plurality of nodes, each node of the plurality of nodes using a medium access mechanism of the Carrier Sense Multiple Access with Collision Avoidance type based on a computation of a backoff value, a specific value being associated with each node of a set of nodes of the plurality of nodes, the specific value of a node being known by the other nodes of the set of nodes, the method being such that a step of determining a backoff value for each node of the set of nodes is carried out in each node of the set of nodes, the backoff value associated with a node being determined as a function of the specific value associated with that node.

Therefore, according to the method of the invention, the backoff values of the nodes of a privileged set of nodes are known by each node of the

privileged set of nodes and thus, the access to the medium is optimized for the nodes of the set of privileged nodes, even if the communication network is overcrowded. Accordingly, the bandwidth usage is optimized for the nodes of the set of privileged nodes. According to the invention, no medium access
5 collision may normally occur among the nodes of the set of privileged nodes and a master node is not required.

In a particular embodiment, the method further comprises a step of decrementing the backoff value associated with each node of the set of nodes if all the backoff values associated with the nodes of the set of nodes are different
10 from zero, the step of decrementing the backoff values being carried out in each node of the set of nodes. Accordingly, each node of the set of privileged nodes is able to determine when a node of the set of privileged nodes is contending for the medium access. In that case, each node of the set of privileged nodes knows implicitly if a peer has been granted the medium successfully.

Still in a particular embodiment, the method further comprises a step of determining whether or not a collision would occur according to the medium access mechanism if the backoff value associated with a node of the set of nodes reaches zero, the step of determining if a collision would occur being
15 carried out in each node of the set of nodes, for identifying a medium access collision between a node of the set of privileged nodes and another node. Therefore, standard node, for example nodes conforming to 802.11 standard, can access the medium without any modification regarding their backoff algorithm.
20

Advantageously, the method further comprises, if a collision would occur, a step of increasing the value of a contention window used for
25 determining the backoff value for each node of the set of nodes, the step of increasing the value of the contention window being carried out in each node of the set of nodes, the step of determining a backoff value being carried out again in each node of the set of nodes, for the node of the set of nodes at the origin of the collision, after the value of the contention window is increased. Accordingly,
30 a new backoff value is associated with the node of the set of privileged nodes contending for the medium access.

Preferably, the method further comprises the following steps if no collision would occur,

- transmitting data through the communication network, the step of transmitting data being carried out by the node of the set of nodes whose associated backoff value is equal to zero; and,

- determining a new backoff value for the node of the set of nodes whose associated backoff value is equal to zero,
the step of determining a new backoff value for the node of the set of nodes whose associated backoff value is equal to zero being carried out in each node of the set of nodes.

Therefore, according to the invention, not any specific messaging protocol is required for the nodes to access the medium while avoiding medium access collision among the nodes of the set of privileged nodes.

In a particular embodiment, the function applied on the specific value associated to each node of the set of nodes is a pseudo-random generator taking the associated specific value as a seed, the pseudo-random generators used in each node of the set of nodes being preferably based on a same random value computation algorithm. Accordingly, each node of the set of privileged nodes is able to determine a new backoff value associated with a node of the set of privileged nodes, the backoff values determined in each node of the set of privileged being the same.

Still in a particular embodiment, the method further comprises a step of verifying that the backoff value determined for a node of the set of nodes is different from the backoff value determined for each other node of the set of nodes, another backoff value being determined if a backoff value determined for a node of the set of nodes is equal to the backoff value determined for another node of the set of nodes, the verifying step being carried out in each node of the set of nodes. Accordingly, the backoff values associated to the nodes of the set of privileged nodes are different, avoiding medium access collision among the nodes of the set of privileged nodes.

Still in a particular embodiment, the step of determining a backoff value for each node of the set of nodes is carried out again in each node of the

set of nodes upon reception of a specific message generated when a new node is added to the set of nodes. Therefore, the set of privileged nodes can be easily modified.

Still in a particular embodiment, the specific values associated with
5 the nodes of the set of nodes are node identifiers.

Another object of the invention is a computer program comprising instructions for carrying out each step of the method described above when the program is loaded and executed by a programmable apparatus, and an information storage means readable by a computer or a microprocessor storing
10 instructions of a computer program, characterized in that it makes it possible to implement a method of optimizing access to a medium as described above.

It is still another object of the invention to provide a device for a node for optimizing access to a medium in a communication network that can be accessed by a plurality of nodes, each node of the plurality of nodes using a
15 medium access mechanism of the Carrier Sense Multiple Access with Collision Avoidance type based on a computation of a backoff value, a specific value being associated with each node of a set of nodes of the plurality of nodes, the specific value of a node being known by the other nodes of the set of nodes, the device comprising means for determining a backoff value for each node of the
20 set of nodes, the backoff value associated with a node being determined as a function of the specific value associated with that node.

Therefore, according to the device of the invention, the backoff values of nodes of a privileged set of nodes are known by each node of the privileged set of nodes, the access to the medium being optimized for the nodes
25 of the set of privileged nodes, even if the communication network is overcrowded. Accordingly, the bandwidth usage is optimized for the nodes of the set of privileged nodes. According to the invention, no medium access collision may normally occur among the nodes of the set of privileged nodes and a master node is not required.

30 In a preferred embodiment, the device further comprises means for decrementing the backoff value associated with each node of the set of nodes if all the backoff values associated with the nodes of the set of nodes are different

from zero. Accordingly, each node of the set of privileged nodes is able to determine when a node of the set of privileged nodes is contending for the medium access.

Still in a preferred embodiment, the device further comprises means
5 for determining whether or not a collision would occur according to the medium access mechanism if the backoff value associated with a node of the set of nodes reaches zero, and preferably means for increasing the value of a contention window used for determining the backoff value for each node of the set of nodes, if a collision would occur, the means for determining a backoff
10 value being invoked by the means for increasing the value of the contention window, for determining a backoff value for the node of the set of nodes at the origin of the collision. Therefore, standard node, for example nodes conforming to 802.11 standard, can access the medium without any modification regarding their backoff algorithm.

Advantageously, the device further comprises means for verifying
15 that the backoff value determined for a node of the set of nodes is different from the backoff value determined for each other node of the set of nodes and for determining another backoff value if a backoff value determined for a node of the set of nodes is equal to the backoff value determined for another node of
20 the set of nodes. Accordingly, the backoff values associated to the nodes of the set of privileged nodes are different, avoiding medium access collision among the nodes of the set of privileged nodes.

Further advantages of the present invention will become apparent to
the ones skilled in the art upon examination of the drawings and detailed
25 description. It is intended that any additional advantages be incorporated herein.

Figure 1 is a time diagram illustrating the DCF and backoff access
mechanism for accessing a communication medium for transmitting data
packets;

30 Figure 2 is an example of a communication system where the present invention can be implemented;

Figure 3 is a block diagram illustrating schematically the architecture of a node adapted to incorporate the invention, for example a node Nc_i of Figure 2;

Figure 4 is a block diagram illustrating steps of an example of an algorithm used during an initialization phase when a new node is added to a set of nodes considered as privileged;

Figure 5 is a block diagram illustrating steps of an example of an algorithm carried out by the backoff management block 330 of Figure 3 according to the invention; and,

Figure 6, comprising Figure 6a and Figure 6b, illustrates an example of *BackOff* and *RandGen* tables, respectively, that are stored in each node of the set of privileged nodes.

According to an embodiment of the invention, a set of nodes of a communication sub-network, using a CSMA/CA access mechanism, is identified as a set of privileged nodes that try to contend continuously for the communication medium of the sub-network. Accordingly, the nodes of the set of privileged nodes use a dedicated shared backoff time calculation method for collision avoidance within the sub-network so as to decrease the medium access time for these nodes. According to a particular embodiment, each node of the set of privileged nodes owns a unique node identifier that is used by the shared backoff time calculation algorithm for determining a backoff value associated with each of these nodes, the backoff value being most of the time different for each of these nodes. Alternatively, other values, specific to each node of the set of privileged nodes and known by these nodes may be used.

As described below, a pseudo-random generator is preferably used in each node of the set of privileged nodes to determine a backoff value for each of these nodes. A seed of such a pseudo-random generator is the node identifier (or a value that is unique to each node of the set of privileged nodes and known by all of these nodes) of the corresponding node.

When a new node is added to the set of privileged nodes, the current used backoff values of all the nodes of the set of privileged nodes are synchronized as described herein below.

According to an embodiment of the invention, each node of the set of privileged nodes checks if another node of this set uses the backoff value provided by its own pseudo-random generator.

For each time unit during which the backoff algorithm conforming to
5 the invention is invoked, each node of the set of privileged nodes updates internally the current backoff value of all of the set of privileged nodes.

Figure 2 is an example of a communication system 100 where the present invention can be implemented. The communication system 100 comprises a transmission medium 105 allowing several nodes to exchange data
10 packets. Such a transmission medium may drop or corrupt transmitted data packets. The transmission medium 105 conforms to the CSMA/CA channel access mechanism. For the sake of illustration, transmission medium 105 can be a wireless network implementing the 802.11 standard.

The nodes of the communication system 100 may be divided in two
15 sets: a set of privileged nodes and a set of nodes implementing the 802.11 standard. According to the given example, the set of privileged nodes comprises the nodes 110-1 to 110-3, referred to as Nc_i nodes, while the set of nodes implementing the 802.11 standard comprises the nodes 115-1 to 115-4, referred to as Nb_i nodes.

For the sake of illustration, all data exchanges between nodes of the
20 communication system 100, that is to say nodes Nc_i and nodes Nb_i , are managed through the standardized 802.11n MAC/PHY layers.

Figure 3 is a block diagram illustrating schematically the architecture of a node 300 adapted to carry out, at least partially, the invention, for example
25 a node Nc_i of Figure 2. As illustrated, node 300 comprises a physical (PHY) layer block 305, a MAC layer block 310, and an application layer block 315.

The PHY layer block 305 (here a 802.11 standardized PHY layer) is in charge of formatting and sending data packets on the medium used (e.g. a wireless medium) as well as receiving data packets from that medium. The
30 MAC layer block 310 comprises a standard MAC 802.11 layer 320 and two additional blocks 325 and 330 for carrying out, at least partially, the invention. According to a particular embodiment, the initialization block 325 is in charge of

initiating the shared backoff time calculation procedure while the backoff management block 330 is in charge of managing the backoff values used by the nodes of the set of privileged nodes, according to the invention. Finally, the application layer block 315 implements an application generating and receiving data packets, for example data packets of a video stream.

Accordingly, the node 300 comprises means to transmit data packets in a network using a CSMA/CA medium access mechanism as well as means to receive data packets in a network using a CSMA/CA medium access mechanism. Moreover, according to an implemented standard, for example the 802.11 standard, the node 300 comprises means to allocate, in cooperation with other nodes linked to node 300, node identifiers. The initialization and backoff management blocks 325 and 330 provide means for the node 300 to generate a pseudo-random value using a node identifier as seed in order to compute a backoff value, means for comparing a computed backoff value with backoff values used by a set of nodes, means for regenerating a new pseudo-random value if the computed backoff value is already used, and means for updating the backoff values used by a set of nodes.

It is to be noted that the means for pseudo-random generation in the backoff management block 330 are similar for all the nodes of the set of privileged nodes. In other words, all the nodes of the set of privileged nodes implement the same pseudo-random generator algorithm. As a consequence, knowing the seed of the generator allows exactly the same series of random values to be retrieved in different nodes.

Figure 4 is a block diagram illustrating steps of an example of an algorithm used during an initialization phase when a new node is added to a set of privileged nodes (nodes N_{c_i} of Figure 2), according to the invention. The steps depicted on Figure 4 are typically executed by the initialization block 325 of the node 300 represented in Figure 3.

A first step to be carried out when a new node is to be added in a network conforming the 802.11 standard is the identification of a right channel frequency. This is typically done during the booting of the node by scanning the

available frequencies. Next, the new node requests other nodes of the set of privileged nodes to subscribe to that set (step 400).

Following the transmission of such a request, the new node receives a node identifier (step 405), referred to as *nodeID* below, which is determined, for example, according to the 802.11 standard MAC protocol. Such a *nodeID* may be for example, the MAC address of the node or a function of the MAC address. As described above, the node identifiers are used as a seed of a pseudo-random generator for determining a backoff value for each corresponding node of the set of privileged nodes. It is to be noted that, as mentioned above, the *nodeID* can be, in the meaning of the invention, any value that is specific to a node and that is known by the other nodes.

A following step of the initialization phase is to synchronize, in all the nodes of the set of privileged nodes, the next backoff value to be used by each node of the set of privileged nodes. Several embodiments can be implemented to perform that step.

In one embodiment using the 802.11 standard MAC protocol, the new node can send a particular message (step 410), referred to as *ResetRandomGen* message below, to all nodes of the set of privileged nodes, specifying that the pseudo-random generators of all of these nodes must be reinitialized after the end of the next transmission on the medium.

According to another embodiment, the *ResetRandomGen* message can contain a timestamp specifying the date at which the pseudo-random generators of all nodes of the set of privileged nodes must be reinitialized. It should be noted that all these nodes must use a synchronization mechanism whose precision of the clock drift is not greater than the half duration of a *aSlotTime* time. The synchronization mechanism specified in the 802.11 standard, called the Timing Synchronization Function (TSF), provides for this requirement for a network containing no more than 10 nodes.

Figure 5 is a block diagram illustrating steps of an example of an algorithm that may be carried out by the backoff management block 330 of Figure 3 according to the invention. As described above, the backoff management block 330 is in charge of controlling the medium access of the

node and updating the backoff value for each node of the set of privileged nodes. This algorithm is executed by each node of the set of privileged nodes.

According to a particular embodiment, the backoff values associated with each node of the set of privileged nodes and stored in each of these nodes are managed and stored using two tables. A first table, referred to as *BackOff*, is used for storing the current backoff value used by each node of the set of privileged nodes (*BackOff[i]* is the current backoff value used by the node N_{c_i} of the set of privileged nodes). A second table, referred to as *RandGen*, is used for storing the initial backoff value used by each node of the set of privileged nodes for a next transmission.

Figure 6, comprising Figure 6a and Figure 6b, illustrates an example of the *BackOff* and *RandGen* tables, respectively, that are stored in each node of the set of privileged nodes. It is to be observed that since these tables are managed similarly in each node of the set of privileged nodes, the values memorized in these tables are the same in each of these nodes. The *BackOff* and *RandGen* tables each comprise n columns corresponding to the n nodes of the set of privileged nodes.

Returning to Figure 5, a first step consists in creating a pseudo-random generator for each node N_{c_i} of the set of privileged nodes, with a seed equal to the corresponding *nodeID* (step 500). It is observed that since *nodeIDs* are known by all the nodes of the set of privileged nodes, using a *nodeID* as the seed of a pseudo-random generator means that the resulting lists of backoff values are precisely known by all N_{c_i} nodes without any message exchange.

The pseudo-random generators are advantageously set in such a way that the generated pseudo-random values are comprised within the range $[0; CW]$.

Creating a pseudo-random generator for each node N_{c_i} of the set of privileged nodes means, in the context of the invention, preparing a pseudo-random function having a specific seed so that the function yields a pseudo-random value each time it is called. Accordingly, the pseudo-random value obtained by the function executed in a node with a specific seed, after having been called a number j of times, is the same as the pseudo-random value

obtain by the same function executed in another node with the same specific seed, after having been called the same number j of times.

Next, the *RandGen* table is initialized using the pseudo-random generator associated with each node of the set of privileged nodes (step 505).

5 To that end, each pseudo-random generator is selected to generate a pseudo-random value that is considered as a backoff value and stored as such in the *RanGen* table. If one of the obtained backoff values is equal to another obtained backoff value, another one is obtained to replace the one that is equal to the other one. This is repeated until each backoff value is different from all the other
10 backoff values.

The stored backoff values represent the initial backoff values for the next transmission by each node of the set of privileged nodes. Accordingly, these backoff values are copied in the *BackOff* table representing the current backoff values and new pseudo-random values are obtained from the random
15 generators and stored in the *RandGen table* (step 510), these new values representing the initial backoff value for the next transmission of each node of the set of privileged nodes.

A test is then performed to determine whether or not a *ResetRandomGen* message has been received (step 515), such a message
20 being received each time a new node is added in the set of privileged nodes. If a *ResetRandomGen* message has been received, a synchronization step of the nodes of the set of privileged nodes is carried out (step 520). Such a step may consist, for example, in resetting the pseudo-random generator associated with each node of the set of privileged nodes so as to create a new pseudo-random
25 generator for each node of the set of privileged nodes (comprising the new node) at step 500. Consequently, each node of the set of privileged nodes knows the backoff values of all the others nodes of the set of privileged nodes (for the reasons described above) and is precisely synchronized. Since, each node of the set of privileged nodes knows when the value of the backoff counter
30 of each of these nodes reaches zero, collision among these nodes is avoided.

If a *ResetRandomGen* message has not been received, another test is performed to determine whether or not the medium is busy (step 525). If the

medium is busy, the backoff counter is frozen and the process branches at step 515 to check for the possible reception of a *ResetRandomGen* message.

When the medium becomes idle (step 525), another test is performed to determine whether or not a backoff counter of a node of the set of privileged nodes elapses (which happens when the corresponding backoff value reaches zero), that is to say if there is an index value i such that $BackOff[i]=0$ (step 530). If no backoff counter of the nodes of the set of privileged nodes has elapsed, the backoff counter of each node of the set of privileged nodes is decreased by one (step 535), that is to say that each value of the *BackOff* table is decreased by one, a waiting time of one *aSlotTime* is performed (step 540), and the process branches to step 515 wherein it is determined whether or not a *ResetRandomGen* message has been received.

If the backoff value of one of the nodes of the set of privileged nodes reaches zero (step 530), another test is performed to determine whether or not a collision would occur between a node of the set of privileged nodes trying to transmit data packets and another node (step 545) not belonging to the set of privileged nodes (for example nodes Nb_i of Figure 2). If a collision would occur, the *CW* value is increased, preferably as specified by the 802.11 standard, the pseudo-random generator associated with the node of the set of privileged nodes, whose backoff counter has elapsed, is reset (step 550), and the process branches to step 555 described hereafter.

If no collision would occur (step 545), the node whose backoff value reaches zero accesses the medium for transmitting data packets (not represented). It is to be noted that since the process described by reference to Figure 5 is carried out by each node of the set of privileged nodes, each of these nodes may determine which node is accessing the medium.

The backoff procedure of the node accessing the medium is reinitialized (step 555). Such a reinitialization step may consist in getting a new backoff value for the node whose backoff value has just reached zero. Such new backoff value is obtained from the pseudo-random generator associated with the corresponding node. If the new backoff value is equal to a backoff value of the *BackOff* table, another new backoff value is obtained similarly. This

is repeated until the new backoff value is different from all the backoff values. The obtained new backoff value is stored in the *BackOff* table and the next backoff value is obtained (still from the pseudo-random generator associated with the node whose backoff value reaches zero) and stored in the *RanGen* table.

Again, it is to be noted that because the process is carried out in each node of the set of privileged nodes, the coherency of the *BackOff* and *RandGen* tables of these nodes is maintained.

It is to be noted that if the number of nodes of the set of privileged nodes is greater than the *CW* value, it is impossible to allocate a different backoff value for each of these nodes. Accordingly, the value of *CW* is advantageously chosen so as to be greater than the number of nodes of the set of privileged nodes. In such a case, the access delay may be increased but the solution remains fair for all the nodes of the network.

It is also noted that each node of the set of privileged nodes must be directly seen by all others nodes of that set because of the synchronization of the backoff values of the nodes of the set of privileged nodes that is directly linked to the medium status.

Naturally, in order to satisfy local and specific requirements, a person skilled in the art may apply, to the solution described above, many modifications and alterations all of which, however, are included within the scope of protection of the invention as defined by the following claims.

CLAIMS

5 1. A method for optimizing access to a medium in a communication network which can be accessed by a plurality of nodes, each node of the plurality of nodes using a medium access mechanism of the Carrier Sense Multiple Access with Collision Avoidance type based on a computation of a backoff value, the method being characterized in that a specific value is
10 associated with each node of a set of nodes of the plurality of nodes, the specific value of a node being known by the other nodes of the set of nodes, and in that a step of determining a backoff value for each node of the set of nodes is carried out in each node of the set of nodes, the backoff value associated with a node being determined as a function of the specific value
15 associated with that node.

 2. The method according to claim 1 further comprising a step of decrementing the backoff value associated with each node of the set of nodes if all the backoff values associated with the nodes of the set of nodes are different from zero, the step of decrementing the backoff values being carried out in each
20 node of the set of nodes.

 3. The method of claim 1 or of claim 2 further comprising a step of determining whether or not a collision would occur according to the medium access mechanism if the backoff value associated with a node of the set of nodes reaches zero, the step of determining if a collision would occur being
25 carried out in each node of the set of nodes.

 4. The method according to claim 3 further comprising, if a collision would occur, a step of increasing the value of a contention window used for determining the backoff value for each node of the set of nodes, the step of increasing the value of the contention window being carried out in each node of
30 the set of nodes, the step of determining a backoff value being carried out again in each node of the set of nodes, for the node of the set of nodes at the origin of the collision, after the value of the contention window is increased.

5. The method according to claim 3 or claim 4 further comprising the following steps if no collision would occur,

- transmitting data through the communication network, the step of transmitting data being carried out by the node of the set of nodes whose
5 associated backoff value is equal to zero; and,

- determining a new backoff value for the node of the set of nodes whose associated backoff value is equal to zero,

the step of determining a new backoff value for the node of the set of nodes whose associated backoff value is equal to zero being carried out in each node
10 of the set of nodes.

6. The method according to any one of claims 1 to 5 wherein the function applied on the specific value associated to each node of the set of nodes is a pseudo-random generator taking the associated specific value as a seed.

15 7. The method according to claim 6 wherein the pseudo-random generators used in each node of the set of nodes are based on a same random value computation algorithm.

8. The method according to any one of claims 1 to 7 further comprising a step of verifying that the backoff value determined for a node of
20 the set of nodes is different from the backoff value determined for each other node of the set of nodes, another backoff value being determined if a backoff value determined for a node of the set of nodes is equal to the backoff value determined for another node of the set of nodes, the verifying step being carried out in each node of the set of nodes.

25 9. The method according to any one of the preceding claims wherein the step of determining a backoff value for each node of the set of nodes is carried out again in each node of the set of nodes upon reception of a specific message generated when a new node is added to the set of nodes.

30 10. The method according to any one of the preceding claims wherein the specific values associated with the nodes of the set of nodes are node identifiers.

11. A computer program comprising instructions for carrying out each step of the method according to any one of the preceding claims when the program is loaded and executed by a programmable apparatus.

12. An information storage means readable by a computer or a
5 microprocessor storing instructions of a computer program, characterized in that it makes it possible to implement a method of optimizing access to a medium according to any one of claims 1 to 10.

13. A device for a node for optimizing access to a medium in a communication network that can be accessed by a plurality of nodes, each
10 node of the plurality of nodes using a medium access mechanism of the Carrier Sense Multiple Access with Collision Avoidance type based on a computation of a backoff value, the device being characterized in that a specific value is associated with each node of a set of nodes of the plurality of nodes, the specific value of a node being known by the other nodes of the set of nodes,
15 and in that the device comprises means for determining a backoff value for each node of the set of nodes, the backoff value associated with a node being determined as a function of the specific value associated with that node.

14. The device of claim 13 further comprising means for decrementing the backoff value associated with each node of the set of nodes if
20 all the backoff values associated with the nodes of the set of nodes are different from zero.

15. The device of claim 13 or of claim 14 further comprising means for determining whether or not a collision would occur according to the medium access mechanism if the backoff value associated with a node of the set of
25 nodes reaches zero.

16. The device of claim 15 further comprising means for increasing the value of a contention window used for determining the backoff value for each node of the set of nodes, if a collision would occur, the means for determining a backoff value being invoked by the means for increasing the
30 value of the contention window, for determining a backoff value for the node of the set of nodes at the origin of the collision.

17. The device according to any one of claims 13 to 16 further comprising means for verifying that the backoff value determined for a node of the set of nodes is different from the backoff value determined for each other node of the set of nodes and for determining another backoff value if a backoff
5 value determined for a node of the set of nodes is equal to the backoff value determined for another node of the set of nodes.

18. A method, device, information storage means or computer program for optimizing access to a medium in a communication network substantially as herein described with reference to, and as shown in, each of
10 Figures 2 to 6 of the accompanying drawings.

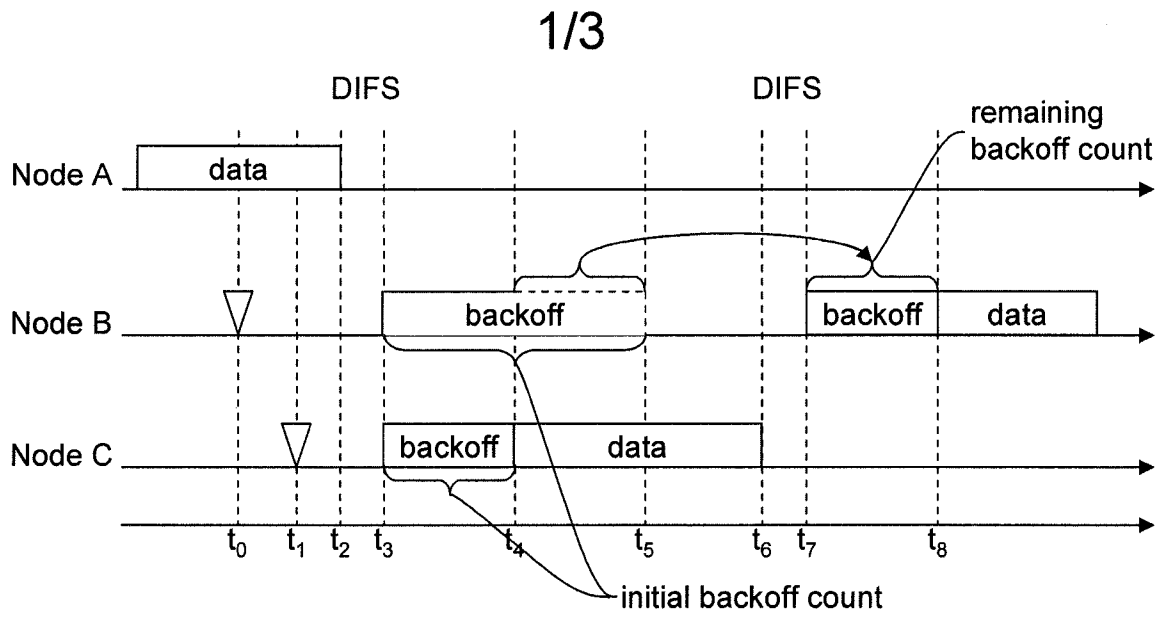


Fig. 1 (prior art)

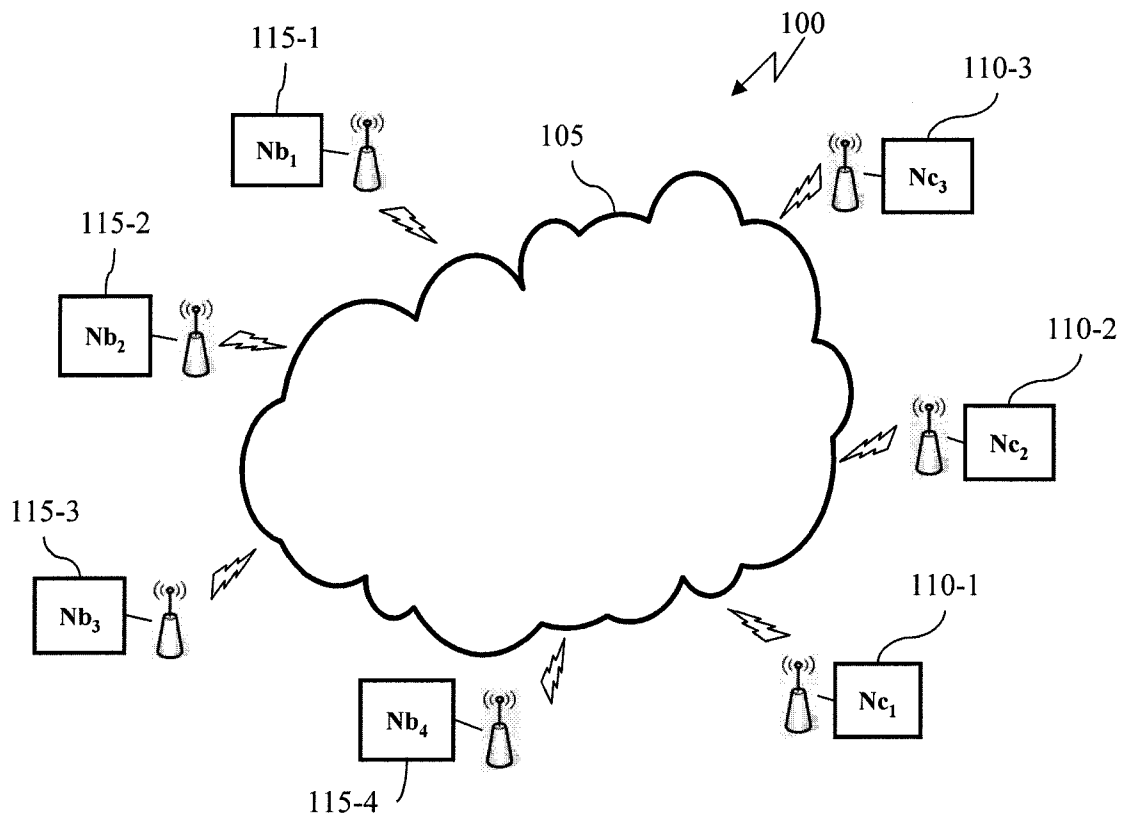


Fig. 2

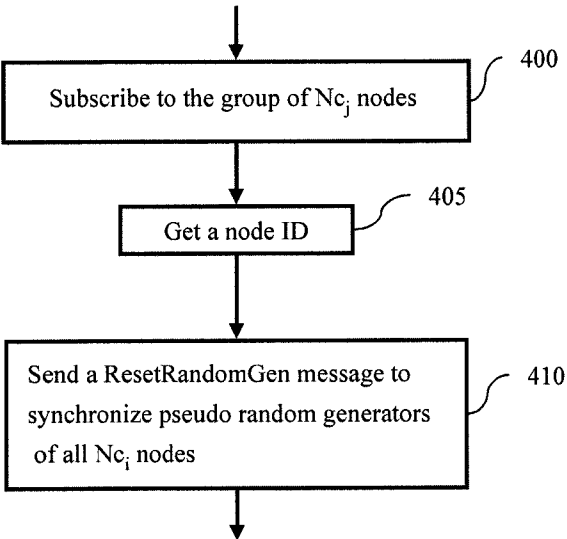
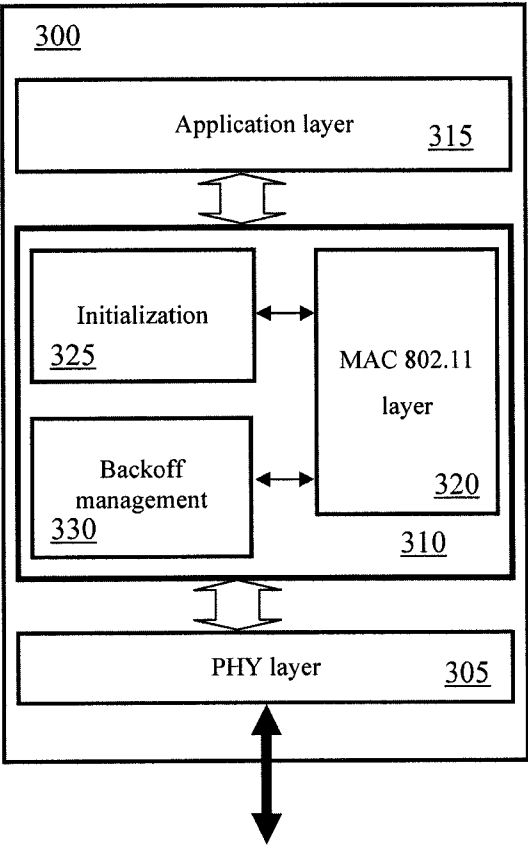


Fig. 4

Fig. 3



BackOff: current backoff value

Current backoff value N_{c_0}	Cuurent backoff value N_{c_1}	Current backoff value N_{c_2}	...	Current backoff value N_{c_i}	...	Current backoff value N_{c_n}
---------------------------------	---------------------------------	---------------------------------	-----	---------------------------------	-----	---------------------------------

Fig. 6a

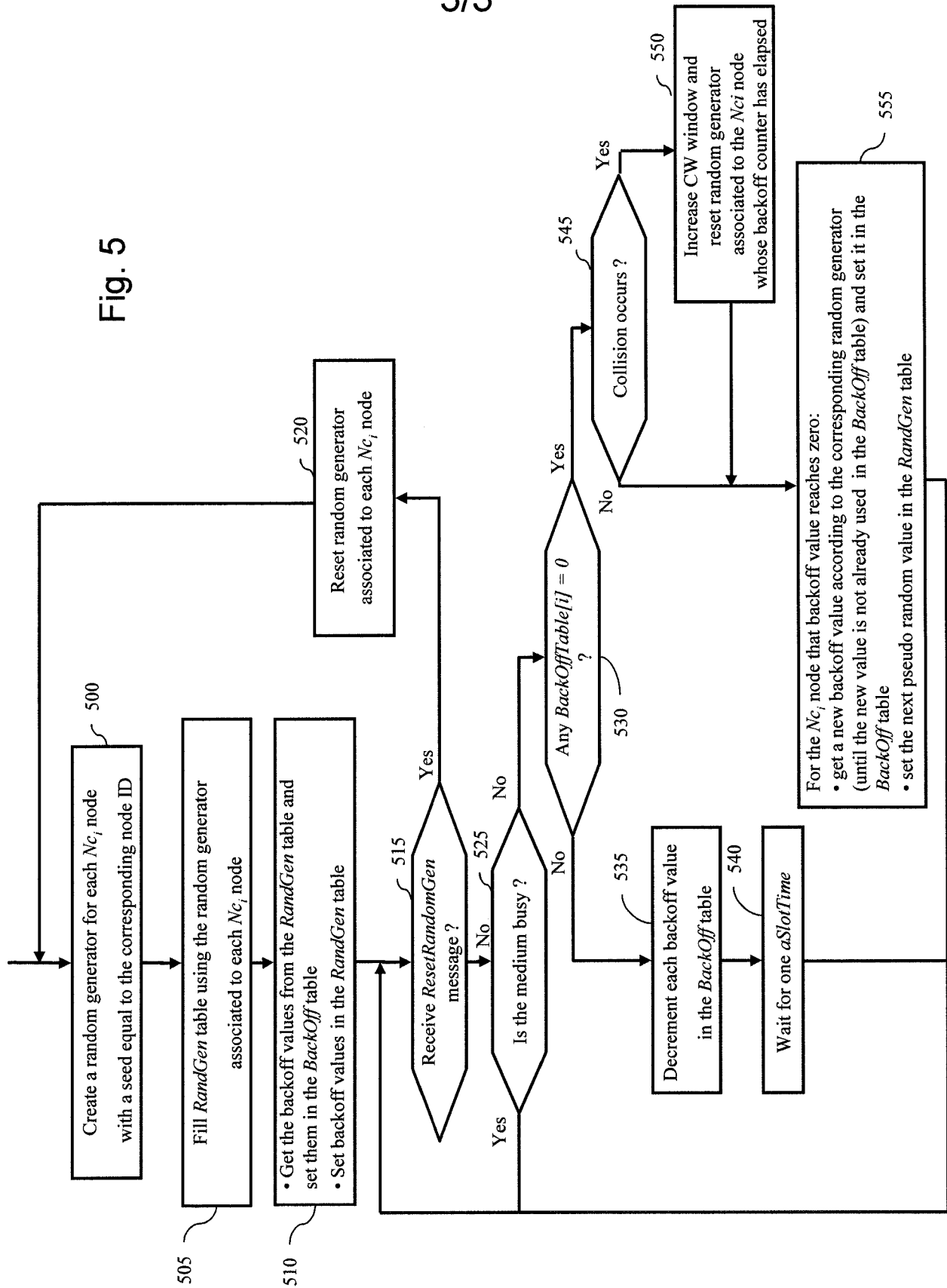
RandGen: initial backoff value for a next transmission

Next init. backoff value N_{c_0}	Next init. backoff value N_{c_1}	Next init. backoff value N_{c_2}	...	Next init. backoff value N_{c_i}	...	Next init. backoff value N_{c_n}
------------------------------------	------------------------------------	------------------------------------	-----	------------------------------------	-----	------------------------------------

Fig. 6b

3/3

Fig. 5



INTERNATIONAL SEARCH REPORT

International application No
PCT/IB2012/052393

A. CLASSIFICATION OF SUBJECT MATTER INV. H04W74/08 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 H04L 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) EPO-Internal, WPI Data											
C. DOCUMENTS CONSIDERED TO BE RELEVANT <table border="1"> <thead> <tr> <th>Category*</th> <th>Citation of document, with indication, where appropriate, of the relevant passages</th> <th>Relevant to claim No.</th> </tr> </thead> <tbody> <tr> <td>X</td> <td> KYASANUR P ET AL: "Detection and handling of MAC layer misbehavior in wireless networks", PROCEEDINGS 2003 INTERNATIONAL CONFERENCE ON DEPENDABLE SYSTEMS AND NETWORKS. DSN 2003. SAN FRANCISCO, CA, JUNE 22 - 25, 2003; [INTERNATIONAL CONFERENCE ON DEPENDABLE SYSTEMS AND NETWORKS], LOS ALAMITOS, CA : IEEE COMP. SOC, US, 22 June 2003 (2003-06-22), pages 173-182, XP010643854, DOI: 10.1109/DSN.2003.1209928 ISBN: 978-0-7695-1952-4 paragraphs [0001], [04.1] ----- </td> <td>1-17</td> </tr> <tr> <td>X</td> <td> GB 2 423 162 A (TOSHIBA RES EUROP LTD [GB]) 16 August 2006 (2006-08-16) pages 3, 15 ----- -/-- </td> <td>1-17</td> </tr> </tbody> </table>			Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.	X	KYASANUR P ET AL: "Detection and handling of MAC layer misbehavior in wireless networks", PROCEEDINGS 2003 INTERNATIONAL CONFERENCE ON DEPENDABLE SYSTEMS AND NETWORKS. DSN 2003. SAN FRANCISCO, CA, JUNE 22 - 25, 2003; [INTERNATIONAL CONFERENCE ON DEPENDABLE SYSTEMS AND NETWORKS], LOS ALAMITOS, CA : IEEE COMP. SOC, US, 22 June 2003 (2003-06-22), pages 173-182, XP010643854, DOI: 10.1109/DSN.2003.1209928 ISBN: 978-0-7695-1952-4 paragraphs [0001], [04.1] -----	1-17	X	GB 2 423 162 A (TOSHIBA RES EUROP LTD [GB]) 16 August 2006 (2006-08-16) pages 3, 15 ----- -/--	1-17
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.									
X	KYASANUR P ET AL: "Detection and handling of MAC layer misbehavior in wireless networks", PROCEEDINGS 2003 INTERNATIONAL CONFERENCE ON DEPENDABLE SYSTEMS AND NETWORKS. DSN 2003. SAN FRANCISCO, CA, JUNE 22 - 25, 2003; [INTERNATIONAL CONFERENCE ON DEPENDABLE SYSTEMS AND NETWORKS], LOS ALAMITOS, CA : IEEE COMP. SOC, US, 22 June 2003 (2003-06-22), pages 173-182, XP010643854, DOI: 10.1109/DSN.2003.1209928 ISBN: 978-0-7695-1952-4 paragraphs [0001], [04.1] -----	1-17									
X	GB 2 423 162 A (TOSHIBA RES EUROP LTD [GB]) 16 August 2006 (2006-08-16) pages 3, 15 ----- -/--	1-17									
☒ Further documents are listed in the continuation of Box C. ☒ See patent family annex.											
* Special categories of cited documents : <table border="0"> <tr> <td> "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 </td> <td> "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 </td> </tr> </table>			"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							
"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		Date of mailing of the international search report									
4 July 2012		12/07/2012									
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 Pasini, Enrico									

INTERNATIONAL SEARCH REPORT

International application No

PCT/IB2012/052393

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	SIWARUK SIWAMOGSATHAM ED - ANONYMOUS: "A novel smart-DCF scheme for high-speed WLANs", COMMUNICATIONS AND INFORMATION TECHNOLOGIES, 2007. ISCIT '07. INTERNATIONAL SYMPOSIUM ON, IEEE, PI, 1 October 2007 (2007-10-01), pages 1032-1037, XP031166613, DOI: 10.1109/ISCIT.2007.4392168 ISBN: 978-1-4244-0976-1 paragraph [0001] -----	1-17
A	MORAES R ET AL: "A TDMA-based mechanism to enforce real-time behavior in WiFi networks", FACTORY COMMUNICATION SYSTEMS, 2008. WFCS 2008. IEEE INTERNATIONAL WORKSHOP ON, IEEE, PISCATAWAY, NJ, USA, 21 May 2008 (2008-05-21), pages 109-112, XP031344939, ISBN: 978-1-4244-2349-1 paragraph [0002] -----	1-17

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IB2012/052393

Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:
2. ☒ Claims Nos.: 18
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:
see FURTHER INFORMATION sheet PCT/ISA/210
3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.
2. ☐ As all searchable claims could be searched without effort justifying an additional fees, this Authority did not invite payment of additional fees.
3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:
4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

- ☐ The additional search fees were accompanied by the applicant's protest and, where applicable, the payment of a protest fee.
- ☐ The additional search fees were accompanied by the applicant's protest but the applicable protest fee was not paid within the time limit specified in the invitation.
- ☐ No protest accompanied the payment of additional search fees.

FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 210

Continuation of Box II.2

Claims Nos.: 18

1.

The subject-matter of independent claim 18 is defined merely by a reference to the drawings. According to Rule 6.2(a) PCT, claims should not contain such references except where absolutely necessary, which is not the case here. Moreover, claim 18 leaves entirely unclear (Article 6 PCT) to which entity ("method, device, information storage means or computer") said claim is possibly meant to be directed. Finally, the vague expression "substantially as herein described with reference to and as shown in each of figures 2 to 6 of the accompanying drawing" in independent claim 18 leaves the reader in doubt as to the specific technical features to which it is, possibly, meant to refer, thereby rendering the definition of the subject-matter of said claim unclear, Article 6 PCT. 2. As a consequence, independent claim 18 is so vague and unclear in its present form that no search could be carried out and no meaningful opinion could be formed on novelty and inventive step in respect of its subject-matter (Article 34(4)(a)(ii) PCT).

The applicant's attention is drawn to the fact that claims relating to inventions in respect of which no international search report has been established need not be the subject of an international preliminary examination (Rule 66.1(e) PCT). The applicant is advised that the EPO policy when acting as an International Preliminary Examining Authority is normally not to carry out a preliminary examination on matter which has not been searched. This is the case irrespective of whether or not the claims are amended following receipt of the search report or during any Chapter II procedure. If the application proceeds into the regional phase before the EPO, the applicant is reminded that a search may be carried out during examination before the EPO (see EPO Guideline C-VI, 8.2), should the problems which led to the Article 17(2) declaration be overcome.

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/IB2012/052393

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
GB 2423162	A	16-08-2006	NONE
