US 20080042806A1

(19) United States

(12) Patent Application Publication (10) Pub. No.: US 2008/0042806 A1

Wood, JR. (43) Pub. Date: Feb. 21, 2008

(54) METHOD OF ADDRESSING MESSAGES AND COMMUNICATIONS SYSTEM

(76) Inventor: **Clifton W. Wood JR.**, Boise, ID (US)

Correspondence Address:
WELLS, ST. JOHN, ROBERTS, GREGORY & MATKIN P.S.
Suite 1300
601 W. First Avenue
Spokane, WA 99204-0317 (US)

(21) Appl. No.: **11/855,855**

(22) Filed: **Sep. 14, 2007**

Related U.S. Application Data

(63) Continuation of application No. 11/416,846, filed on May 2, 2006, which is a continuation of application No. 09/820,467, filed on Mar. 28, 2001, now Pat. No. 7,315,522, which is a continuation of application No. 09/026,248, filed on Feb. 19, 1998, now Pat. No. 6,275,476.

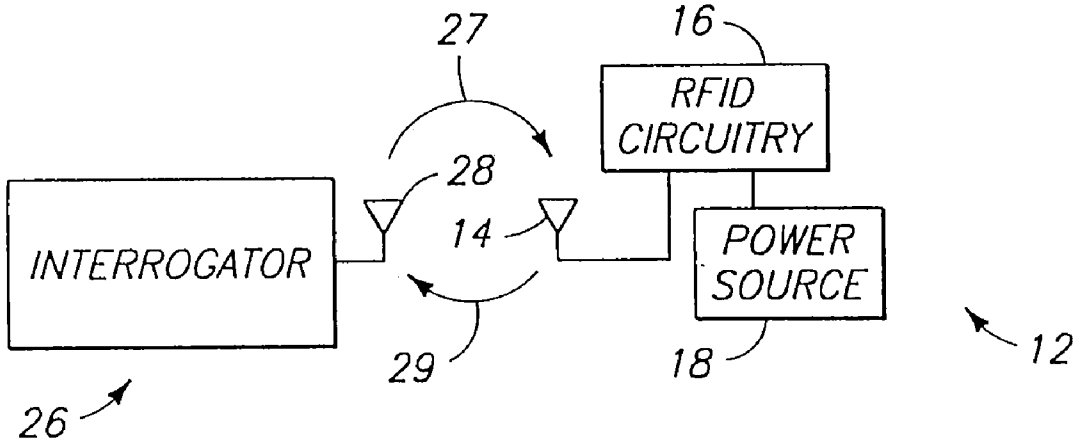
Publication Classification

(51) **Int. Cl.**
H04Q 5/22 (2006.01)

(52) **U.S. Cl.** **340/10.1**

(57) **ABSTRACT**

A method of establishing wireless communications between an interrogator and individual ones of multiple wireless identification devices, the method comprising combining tree search and Aloha methods to establish communications between the interrogator and individual ones of the multiple wireless identification devices without collision. A system comprising an interrogator, and a plurality of wireless identification devices configured to communicate with the interrogator in a wireless fashion, the respective wireless identification devices having a unique identification number, the interrogator being configured to employ tree search and Aloha techniques to determine the unique identification numbers of the different wireless identification devices so as to be able to establish communications between the interrogator and individual ones of the multiple wireless identification devices without collision by multiple wireless identification devices attempting to respond to the interrogator at the same time.



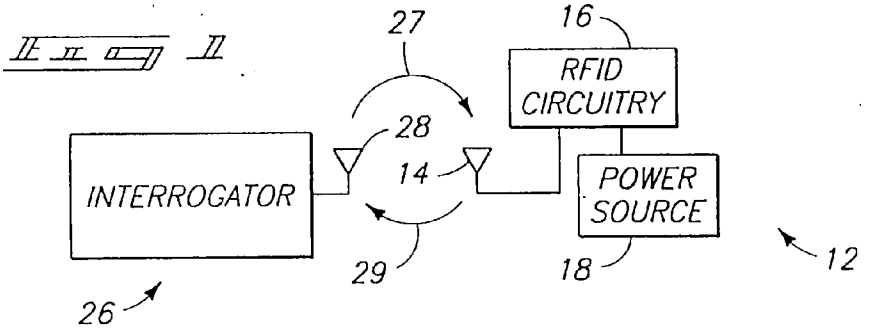


Fig. 1

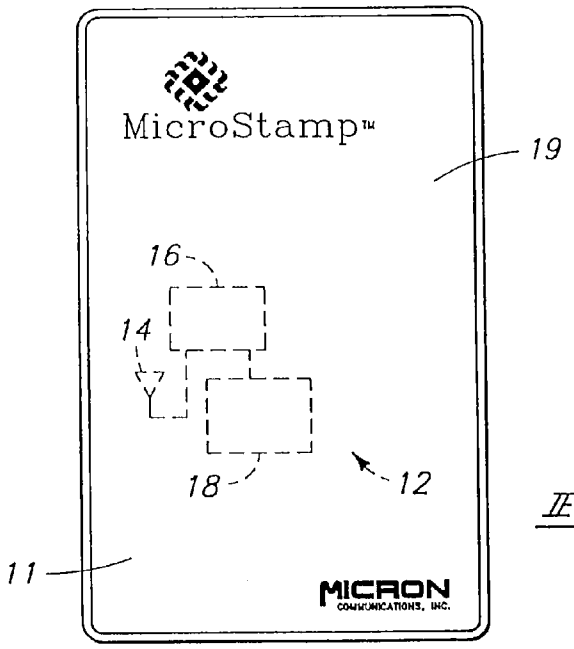


Fig. 2

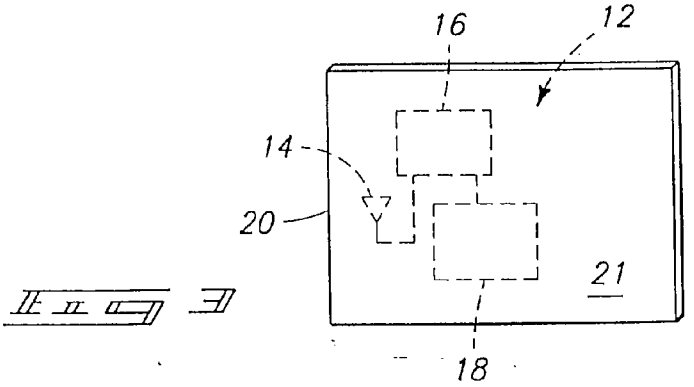


Fig. 3

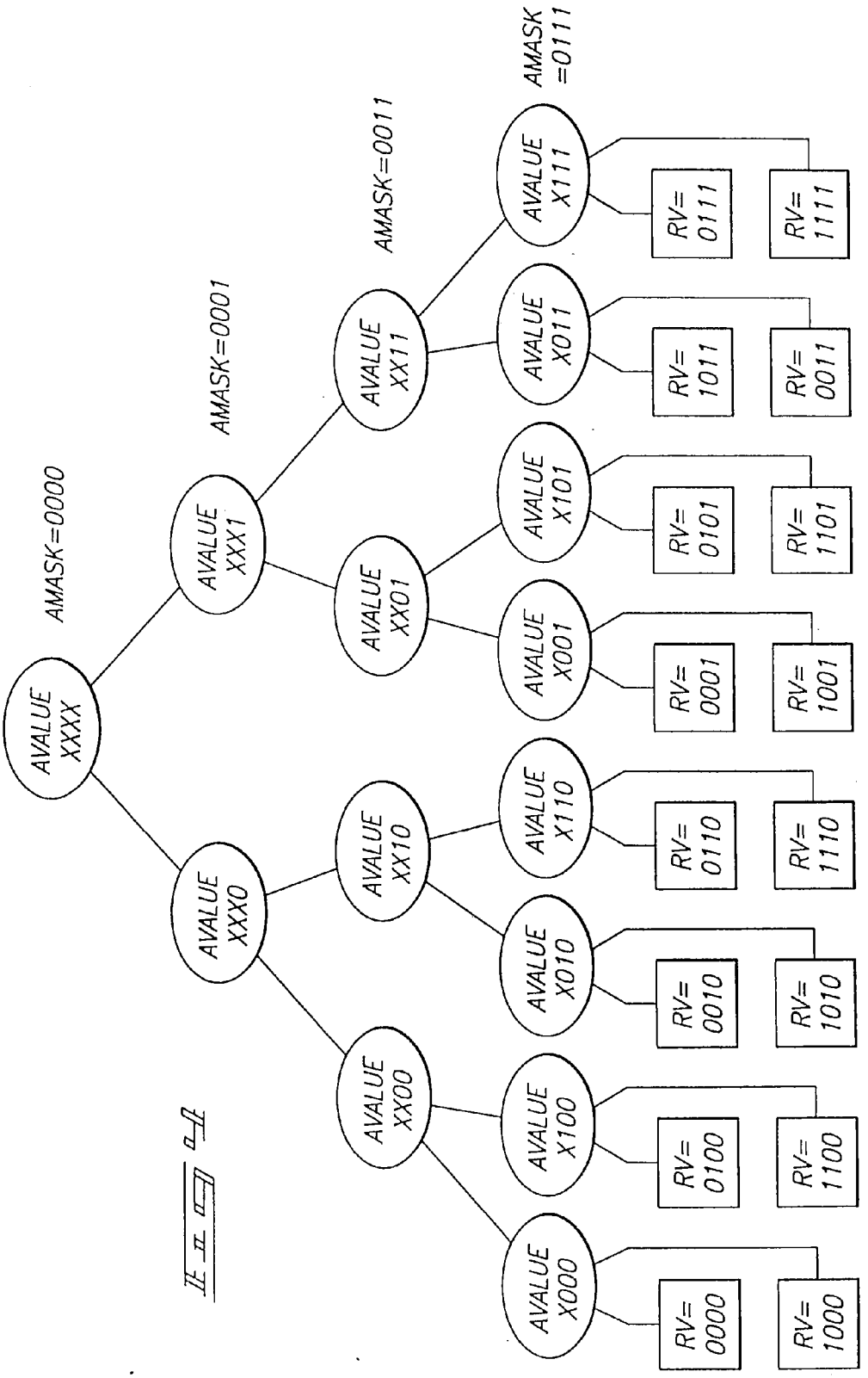

AMASK=0000
AMASK=0001
AMASK=0011
AMASK =0111
AVALUE XXXX
AVALUE XXX0
AVALUE XXX1
AVALUE XX00
AVALUE XX10
AVALUE XX01
AVALUE XX11
AVALUE X000
AVALUE X100
AVALUE X010
AVALUE X110
AVALUE X001
AVALUE X101
AVALUE X011
AVALUE X111
RV= 0000
RV= 1000
RV= 0100
RV= 1100
RV= 0010
RV= 1010
RV= 0110
RV= 1110
RV= 0001
RV= 1001
RV= 0101
RV= 1101
RV= 1011
RV= 0011
RV= 0111
RV= 1111

FIG 4

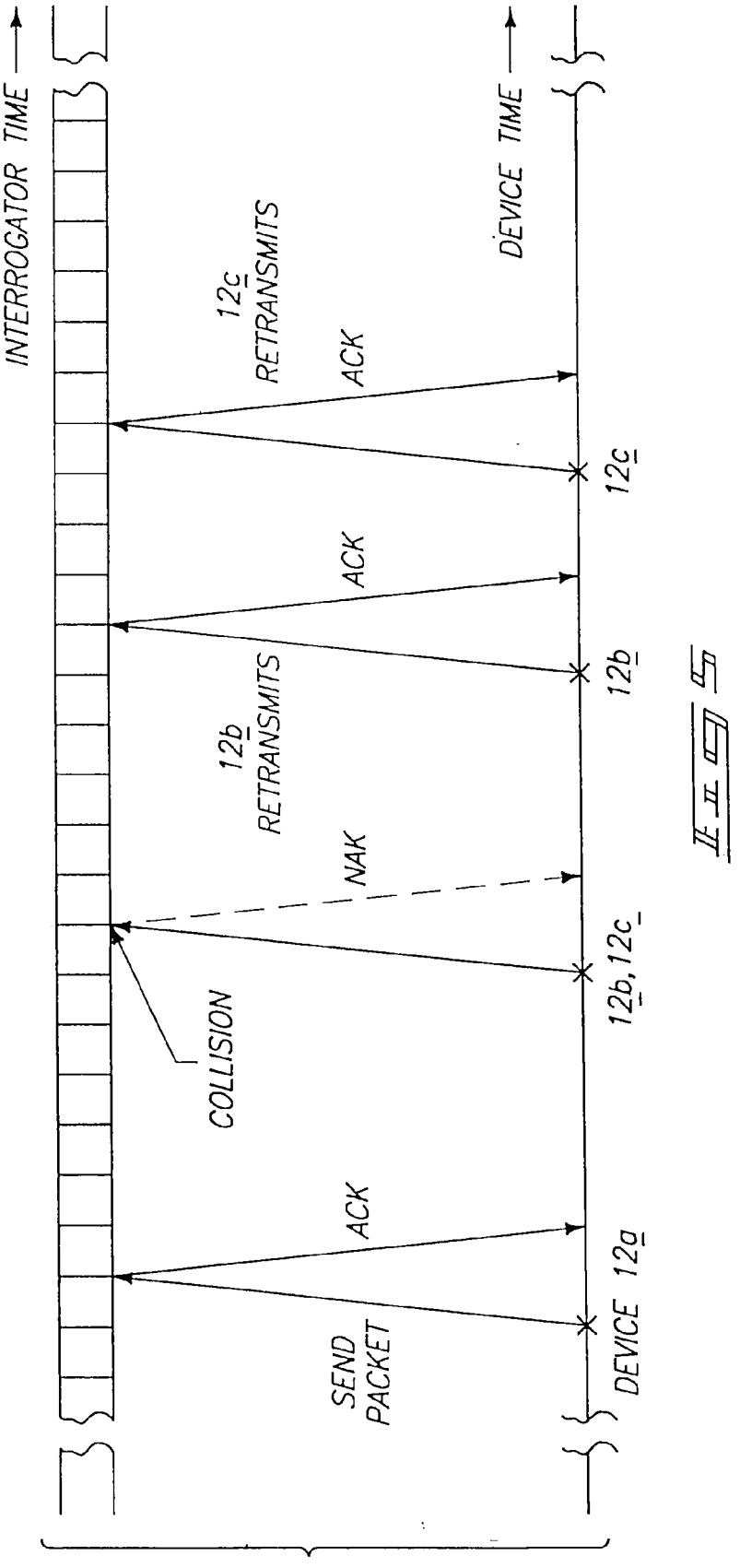

INTERROGATOR TIME
DEVICE TIME
SEND PACKET
DEVICE 12a
ACK
COLLISION
12b, 12c
NAK
12b RETRANSMITS
12b
ACK
12c RETRANSMITS
12c
ACK

FIG 5

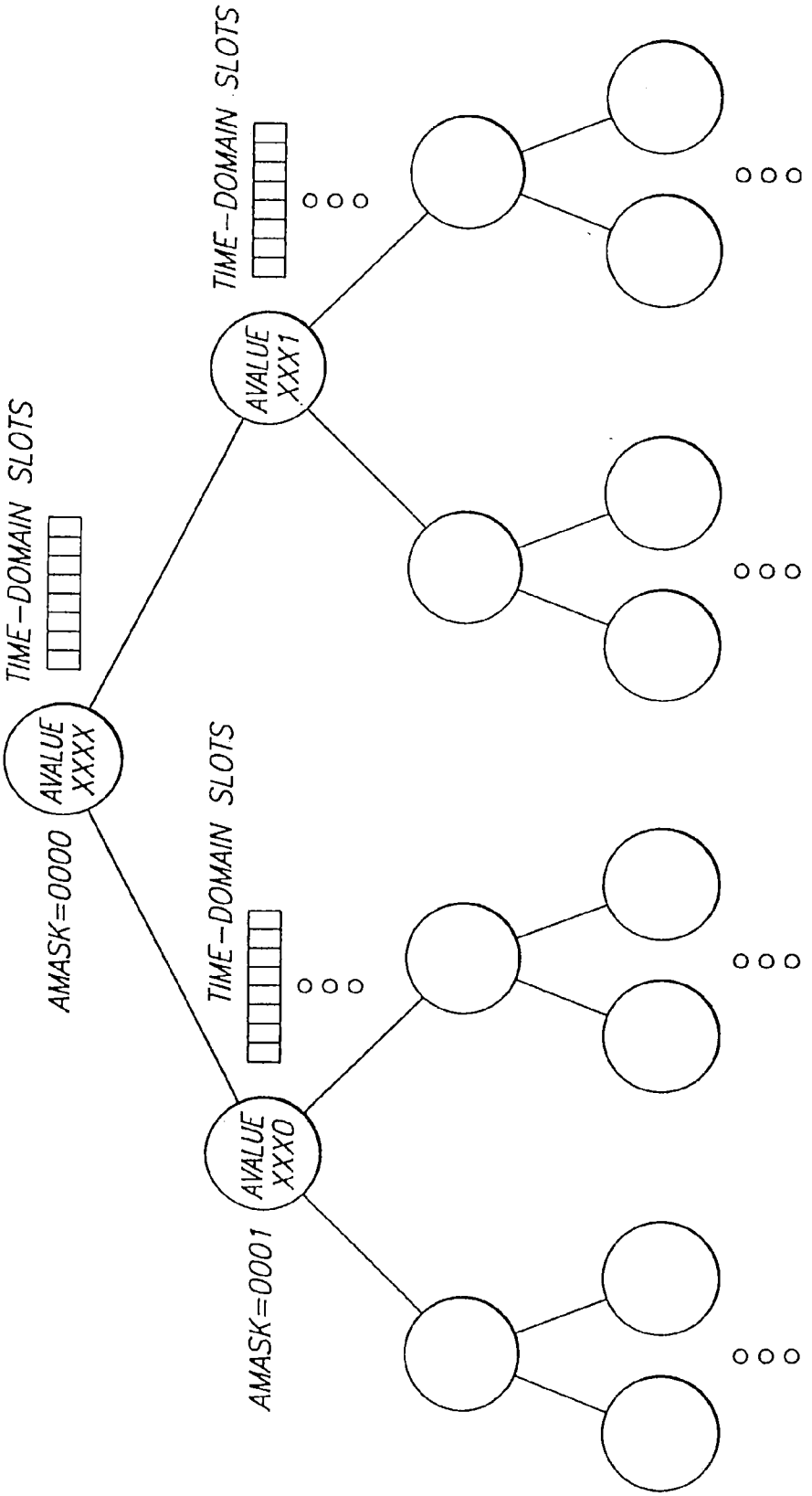

AMASK=0000
AVALUE XXXX
TIME-DOMAIN SLOTS
AMASK=0001
AVALUE XXXO
TIME-DOMAIN SLOTS
AVALUE XXX1
TIME-DOMAIN SLOTS

FIG 5

METHOD OF ADDRESSING MESSAGES AND COMMUNICATIONS SYSTEM

TECHNICAL FIELD

[0001] This invention relates to communications protocols and to digital data communications. Still more particularly, the invention relates to data communications protocols in mediums such as radio communication or the like. The invention also relates to radio frequency identification devices for inventory control, object monitoring, determining the existence, location or movement of objects, or for remote automated payment.

BACKGROUND OF THE INVENTION

[0002] Communications protocols are used in various applications. For example, communications protocols can be used in electronic identification systems. As large numbers of objects are moved in inventory, product manufacturing, and merchandising operations, there is a continuous challenge to accurately monitor the location and flow of objects. Additionally, there is a continuing goal to interrogate the location of objects in an inexpensive and streamlined manner. One way of tracking objects is with an electronic identification system.

[0003] One presently available electronic identification system utilizes a magnetic coupling system. In some cases, an identification device may be provided with a unique identification code in order to distinguish between a number of different devices. Typically, the devices are entirely passive (have no power supply), which results in a small and portable package. However, such identification systems are only capable of operation over a relatively short range, limited by the size of a magnetic field used to supply power to the devices and to communicate with the devices.

[0004] Another wireless electronic identification system utilizes a large active transponder device affixed to an object to be monitored which receives a signal from an interrogator. The device receives the signal, then generates and transmits a responsive signal. The interrogation signal and the responsive signal are typically radio-frequency (RF) signals produced by an RF transmitter circuit. Because active devices have their own power sources, and do not need to be in close proximity to an interrogator or reader to receive power via magnetic coupling. Therefore, active transponder devices tend to be more suitable for applications requiring tracking of a tagged device that may not be in close proximity to an interrogator. For example, active transponder devices tend to be more suitable for inventory control or tracking.

[0005] Electronic identification systems can also be used for remote payment. For example, when a radio frequency identification device passes an interrogator at a toll booth, the toll booth can determine the identity of the radio frequency identification device, and thus of the owner of the device, and debit an account held by the owner for payment of toll or can receive a credit card number against which the toll can be charged. Similarly, remote payment is possible for a variety of other goods or services.

[0006] A communication system, such as a wireless identification system, typically includes two transponders: a commander station or interrogator, and a responder station or transponder device which replies to the interrogator.

[0007] If the interrogator has prior knowledge of the identification number of a device which the interrogator is looking for, it can specify that a response is requested only from the device with that identification number. Sometimes, such information is not available. For example, there are occasions where the interrogator is attempting to determine which of multiple devices are within communication range.

[0008] When the interrogator sends a message to a transponder device requesting a reply, there is a possibility that multiple transponder devices will attempt to respond simultaneously, causing a collision, and thus an erroneous message to be received by the interrogator. For example, if the interrogator sends out a command requesting that all devices within a communications range identify themselves, and gets a large number of simultaneous replies, the interrogator may not able to interpret any of these replies. Thus, arbitration schemes are employed to permit communications free of collisions.

[0009] In one arbitration scheme or system, described in commonly assigned U.S. Pat. Nos. 5,627,544; 5,583,850; 5,500,650; and 5,365,551, all to Snodgrass et al. and all incorporated herein by reference, the interrogator sends a command causing each device of a potentially large number of responding devices to select a random number from a known range and use it as that device's arbitration number. By transmitting requests for identification to various subsets of the full range of arbitration numbers, and checking for an error-free response, the interrogator determines the arbitration number of every responder station capable of communicating at the same time. Therefore, the interrogator is able to conduct subsequent uninterrupted communication with devices, one at a time, by addressing only one device.

[0010] Another arbitration scheme is referred to as the Aloha or slotted Aloha scheme. This scheme is discussed in various references relating to communications, such as *Digital Communications: Fundamentals and Applications*, Bernard Sklar, published January 1988 by Prentice Hall. In this type of scheme, a device will respond to an interrogator using one of many time domain slots selected randomly by the device. A problem with the Aloha scheme is that if there are many devices, or potentially many devices in the field (i.e. in communications range, capable of responding) then there must be many available slots or many collisions will occur. Having many available slots slows down replies. If the magnitude of the number of devices in a field is unknown, then many slots are needed. This results in the system slowing down significantly because the reply time equals the number of slots multiplied by the time period required for one reply.

[0011] An electronic identification system which can be used as a radio frequency identification device, arbitration schemes, and various applications for such devices are described in detail in commonly assigned U.S. patent application Ser. No. 08/705,043, filed Aug. 29, 1996, and incorporated herein by reference.

SUMMARY OF THE INVENTION

[0012] The invention provides a wireless identification device **1**, configured to provide a signal to identify the device in response to an interrogation signal.

[0013] One aspect of the invention provides a method of establishing wireless communications between an interro-

gator and individual ones of multiple wireless identification devices. Tree search and Aloha methods are combined to establish communications between the interrogator and individual ones of the multiple wireless identification devices without collision.

[0014] One aspect of the invention provides a method of addressing messages from an interrogator to a selected one or more of a number of communications devices. A first predetermined number of bits are established to be used as unique identification numbers. Unique identification numbers respectively having the first predetermined number of bits are established for respective devices. A second predetermined number of bits are established to be used for random values. The devices are caused to select random values. Respective devices choose random values independently of random values selected by the other devices. The interrogator transmits a command requesting devices having random values within a specified group of random values to respond, the specified group being less than or equal to the entire set of random values. Devices receiving the command respectively determine if their chosen random values fall within the specified group and, if so, send a reply to the interrogator within a randomly selected time slot of a number of slots. If not, they do not send a reply. The interrogator determines if a collision occurred between devices that sent a reply and, if so, creates a new, smaller, specified group.

[0015] One aspect of the invention provides a communications system comprising an interrogator, and a plurality of wireless identification devices configured to communicate with the interrogator in a wireless fashion. The respective wireless identification devices have a unique identification number. The interrogator is configured to employ tree search and Aloha techniques to determine the unique identification numbers of the different wireless identification devices so as to be able to establish communications between the interrogator and individual ones of the multiple wireless identification devices without collision by multiple wireless identification devices attempting to respond to the interrogator at the same time.

[0016] Another aspect of the invention provides a system comprising an interrogator configured to communicate to a selected one or more of a number of communications devices, and a plurality of communications devices. The devices are configured to select random values. Respective devices choose random values independently of random values selected by the other devices. The interrogator is configured to transmit a command requesting devices having random values within a specified group of random values to respond, the specified group being less than or equal to the entire set of random values. Devices receiving the command are configured to respectively determine if their chosen random values fall within the specified group and, if so, send a reply to the interrogator within a randomly selected time slot of a number of slots. If not, they do not send a reply. The interrogator is configured to determine if a collision occurred between devices that sent a reply and, if so, create a new, smaller, specified group.

[0017] One aspect of the invention provides a radio frequency identification device comprising an integrated circuit including a receiver, a transmitter, and a microprocessor. In one embodiment, the integrated circuit is a monolithic single die single metal layer integrated circuit including the receiver, the transmitter, and the microprocessor. The device of this embodiment includes an active transponder, instead of a transponder which relies on magnetic coupling for power, and therefore has a much greater range.

BRIEF DESCRIPTION OF THE DRAWINGS

[0018] Preferred embodiments of the invention are described below with reference to the following accompanying drawings.

[0019] FIG. **1** is a high level circuit schematic showing an interrogator and a radio frequency identification device embodying the invention.

[0020] FIG. **2** is a front view of a housing, in the form of a badge or card, supporting the circuit of FIG. **1** according to one embodiment the invention.

[0021] FIG. **3** is a front view of a housing supporting the circuit of FIG. **1** according to another embodiment of the invention.

[0022] FIG. **4** is a diagram illustrating a tree splitting sort method for establishing communication with a radio frequency identification device in a field of a plurality of such devices, without collisions.

[0023] FIG. **5** is a time line plot illustrating operation of a slotted Aloha scheme.

[0024] FIG. **6**. is a diagram illustrating using a combination of a tree splitting sort method with an Aloha method for establishing communication with a radio frequency identification device in a field of a plurality of such devices.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

[0025] This disclosure of the invention is submitted in furtherance of the constitutional purposes of the U.S. Patent Laws "to promote the progress of science and useful arts" (Article 1, Section 8).

[0026] FIG. **1** illustrates a wireless identification device **12** in accordance with one embodiment of the invention. In the illustrated embodiment, the wireless identification device is a radio frequency data communication device **12**, and includes RFID circuitry **16**. In the illustrated embodiment, the RFID circuitry is defined by an integrated circuit as described in the above-incorporated patent application Ser. No. 08/705,043, filed Aug. 29, 1996. Other embodiments are possible. A power source **18** is connected to the integrated circuit **16** to supply power to the integrated circuit **16**. In one embodiment, the power source **18** comprises a battery. The device **12** further includes at least one antenna **14** connected to the circuitry **16** for wireless or radio frequency transmission and reception by the circuitry **16**.

[0027] The device **12** transmits and receives radio frequency communications to and from an interrogator **26**. An exemplary interrogator is described in U.S. patent application Ser. No. 08/907,689, filed Aug. 8, 1997 and incorporated herein by reference. Preferably, the interrogator **26** includes an antenna **28**, as well as dedicated transmitting and receiving circuitry, similar to that implemented on the integrated circuit **16**.

[0028] Generally, the interrogator **26** transmits an interrogation signal or command **27** via the antenna **28**. The device **12** receives the incoming interrogation signal via its antenna **14**. Upon receiving the signal **27**, the device **12** responds by generating and transmitting a responsive signal or reply **29**. The responsive signal **29** typically includes information that uniquely identifies, or labels the particular device **12** that is transmitting, so as to identify any object or person with which the device **12** is associated.

[0029] Although only one device **12** is shown in FIG. **1**, typically there will be multiple devices **12** that correspond with the interrogator **26**, and the particular devices **12** that are in communication with the interrogator **26** will typically change over time. In the illustrated embodiment in FIG. **1**, there is no communication between multiple devices **12**. Instead, the devices **12** respectively communicate with the interrogator **26**. Multiple devices **12** can be used in the same field of an interrogator **26** (i.e., within communications range of an interrogator **26**). Similarly, multiple interrogators **26** can be in proximity to one or more of the devices **12**.

[0030] The radio frequency data communication device **12** can be included in any appropriate housing or packaging. Various methods of manufacturing housings are described in commonly assigned U.S. patent application Ser. No. 08/800,037, filed Feb. 13, 1997, and incorporated herein by reference.

[0031] FIG. **2** shows but one embodiment in the form of a card or badge **19** including the radio frequency data communication device **12**, and a housing **11** including plastic or other suitable material. In one embodiment, the front face of the badge has visual identification features such as graphics, text, information found on identification or credit cards, etc.

[0032] FIG. **3** illustrates but one alternative housing supporting the device **12**. More particularly, FIG. **3** shows a miniature housing **20** encasing the device **12** to define a tag which can be supported by an object (e.g., hung from an object, affixed to an object, etc.). Although two particular types of housings have been disclosed, the device **12** can be included in any appropriate housing.

[0033] If the power source **18** is a battery, the battery can take any suitable form. Preferably, the battery type will be selected depending on weight, size, and life requirements for a particular application. In one embodiment, the battery **18** is a thin profile or button-type cell forming a small, thin energy cell more commonly utilized in watches and small electronic devices requiring a thin profile. A conventional cell has a pair of electrodes, an anode formed by one face and a cathode formed by an opposite face. In an alternative embodiment, the power source **18** comprises to a series connected pair of cells. Instead of using a battery, any suitable power source can be employed.

[0034] The circuitry **16** further includes a backscatter transmitter and is configured to provide a responsive signal to the interrogator **26** by radio frequency. More particularly, the circuitry **16** includes a transmitter, a receiver, and memory such as is described in U.S. patent application Ser. No. 08/705,043.

[0035] Radio frequency identification has emerged as a viable and affordable alternative to tagging or labeling small to large quantities of items. The interrogator **26** communicates with the devices **12** via an RF link, so all transmissions by the interrogator **26** are heard simultaneously by all devices **12** within range.

[0036] If the interrogator **26** sends out a command requesting that all devices **12** within range identify themselves, and gets a large number of simultaneous replies, the interrogator **26** may not be able to interpret any of these replies. Therefore, arbitration schemes are provided.

[0037] If the interrogator **26** has prior knowledge of the a identification number of a device **12** which the interrogator **26** is looking for, it can specify that a response is requested only from the device **12** with that identification number. To target a command at a specific device **12**, (i.e., to initiate point-on-point communication), the interrogator **26** must send a number identifying a specific device **12** along with the command. At start-up, or in so a new or changing environment, these identification numbers are not known by the interrogator **26**. Therefore, the interrogator **26** must identify all devices **12** in the field (within communication range) such as by determining the identification numbers of the devices **12** in the field. After this is accomplished, point-to-point communication can proceed as desired by the interrogator **26**.

[0038] Generally speaking, RFID systems are a type of multiaccess communication system. The distance between the interrogator **26** and devices **12** within the field is typically fairly short (e.g., several meters), so packet transmission time is determined primarily by packet size and baud rate. Propagation delays are negligible. In RFID systems, there is a potential for a large number of transmitting devices **12** and there is a need for the interrogator **26** to work in a changing environment, where different devices **12** are swapped in and out frequently (e.g., as inventory is added or removed). The inventors have determined that, in such systems, the use of random access methods work effectively for contention resolution (i.e., for dealing with collisions between devices **12** attempting to respond to the interrogator **26** at the same time).

[0039] RFID systems have some characteristics that are different from other communications systems. For example, one characteristic of the illustrated RFID systems is that the devices **12** never communicate without being prompted by the interrogator **26**. This is in contrast to typical multiaccess systems where the transmitting units operate more independently. In addition, contention for the communication medium is short lived as compared to the ongoing nature of the problem in other multiaccess systems. For example, in a RFID system, after the devices **12** have been identified, the interrogator can communicate with them in a point-to-point fashion. Thus, arbitration in a RFID system is a transient rather than steady-state phenomenon. Further, the capability of a device **12** is limited by practical restrictions on size, power, and cost. The lifetime of a device **12** can often be measured in terms of number of transmissions before battery power is lost. Therefore, one of the most important measures of system performance in RFID arbitration is total time required to arbitrate a set of devices **12**. Another measure is power consumed by the devices **12** during the process. This is in contrast to the measures of throughput and packet delay in other types of multiaccess systems.

[0040] FIG. **4** illustrates one arbitration scheme that can be employed for communication between the interrogator and

devices **12**. Although the arbitration system is being described in connection with a wireless identification system or RFID system, this and other arbitration schemes disclosed herein can be employed in any communication system. Generally, the interrogator **26** sends a command causing each device **12** of a potentially large number of responding devices **12** to select a random number from a known range and use it as that device's arbitration number. By transmitting requests for identification to various subsets of the full range of arbitration numbers, and checking for an error-free response, the interrogator **26** determines the arbitration number of every responder station capable of communicating at the same time. Therefore, the interrogator **26** is able to conduct subsequent uninterrupted communication with devices **12**, one at a time, by addressing only one device **12**.

[**0041**] Three variables are used: an arbitration value (AVALUE), an arbitration mask (AMASK), and a random value ID (RV). The interrogator sends a command causing each device of a potentially large number of responding devices to select a random number from a known range and use it as that device's arbitration number. The interrogator sends an arbitration value (AVALUE) and an arbitration mask (AMASK) to a set of devices **12**. The receiving devices **12** evaluate the following equation:

[**0042**] (AMASK & AVALUE)==(AMASK & RV) wherein "&" is a bitwise AND function, and wherein "==" is an equality function. If the equation evaluates to "1," (TRUE), then the device **12** will reply. If the equation evaluates to "0" (FALSE), then the device **12** will not reply. By performing this in a structured manner, with the number of bits in the arbitration mask being increased by one each time, eventually a device **12** will respond with no collisions. Thus, a binary search tree methodology is employed.

[**0043**] An example using actual numbers will now be provided using only four bits, for simplicity, reference being made to FIG. **4**. In one embodiment, sixteen bits are used for AVALUE and AMASK, respectively. Other numbers of bits can also be employed depending, for example, on the number of devices **12** expected to be encountered in a particular application, on desired cost points, etc.

[**0044**] Assume, for this example, that there are two devices **12** in the field, one with a random value (RV) of 1100 (binary), and another with a random value (RV) of 1010 (binary). The interrogator is trying to establish communications without collisions being caused by the two devices **12** attempting to communicate at the same time.

[**0045**] The interrogator sets AVALUE to 0000 (or all "don't care", indicated by the character "X" in FIG. **4**) and AMASK to 0000. The interrogator transmits a command to all devices **12** requesting that they identify themselves. Each of the devices **12** evaluate (AMASK & AVALUE)== (AMASK & RV) using the random value RV that the respective devices **12** selected. If the equation evaluates to "1" (TRUE), then the device **12** will reply. If the equation evaluates to "0" (FALSE), then the device **12** will not reply. In the first level of the illustrated tree, AMASK is 0000 and anything bitwise ANDed with all zeros results in all zeros, so both the devices **12** in the field respond, and there is a collision.

[**0046**] Next, the interrogator sets AMASK to 0001 and AVALUE to 0000 and transmits an identify command. Both devices **12** in the field have a zero for their least significant bit, and (AMASK & AVALUE)==(AMASK & RV) will be true for both devices **12**. For the device **12** with a random value of 1100, the left side of the equation is evaluated as follows (0001 & 0000)=0000. The right side is evaluated as (0001 & 1100)=0000. The left side equals the right side, so the equation is true for the device **12** with the random value of 1100. For the device **12** with a random value of 1010, the left side of the equation is evaluated as (0001 & 0000)= 0000. The right side is evaluated as (0001 & 1010)=0000. The left side equals the right side, so the equation is true for the device **12** with the random value of 1010. Because the equation is true for both devices **12** in the field, both devices **12** in the field respond, and there is another collision.

[**0047**] Recursively, the interrogator next sets AMASK to 0011 with AVALUE still at 0000 and transmits an identify command. (AMASK & AVALUE)-==(AMASK & RV) is evaluated for both devices **12**. For the device **12** with a random value of 1100, the left side of the equation is evaluated as follows (0011 & 0000)=0000. The right side is evaluated as (0011 & 1100)=0000. The left side equals the right side, so the equation is true for the device **12** with the random value of 1100, so this device **12** responds. For the device **12** with a random value of 1010, the left side of the equation is evaluated as (0011 & 0000)=0000. The right side is evaluated as (0011 & 1010)=0010. The left side does not equal the right side, so the equation is false for the device **12** with the random value of 1010, and this device **12** does not respond. Therefore, there is no collision, and the interrogator can determine the identity (e.g., an identification number) for the device **12** that does respond.

[**0048**] De-recursion takes place, and the devices **12** to the right for the same AMASK level are accessed by setting AVALUE at 0010 and using the same AMASK value 0011.

[**0049**] The device **12** with the random value of 1010 receives a command and evaluates the equation (AMASK & AVALUE)-==(AMASK & RV). The left side of the equation is evaluated as (0011 & 0010)=0010. The right side of the equation is evaluated as (0011 & 1010)=0010. The right side equals the left side, so the equation is true for the device **12** with the random value of 1010. Because there are no other devices **12** in the subtree, a good reply is returned by the device **12** with the random value of 1010. There is no collision, and the interrogator can determine the identity (e.g., an identification number) for the device **12** that does respond.

[**0050**] By recursion, what is meant is that a function makes a call to itself. In other words, the function calls itself within the body of the function. After the called function returns, de-recursion takes place and execution continues at the place just after the function call; i.e. at the beginning of the statement after the function call.

[**0051**] For instance, consider a function that has four statements (numbered 1, 2, 3, 4) in it, and the second statement is a recursive call. Assume that the fourth statement is a return statement. The first time through the loop (iteration 1) the function executes the statement 2 and (because it is a recursive call) calls itself causing iteration 2 to occur. When iteration 2 gets to statement 2, it calls itself making iteration 3. During execution in iteration 3 of statement 1, assume that the function does a return. The information that was saved on the stack from iteration 2 is

loaded and the function resumes execution at statement 3 (in iteration 2), followed by the execution of statement 4 which is also a return statement. Since there are no more statements in the function, the function de-recurses to iteration 1. Iteration 1, had previously recursively called itself in statement 2. Therefore, it now executes statement 3 (in iteration 1). Following that it executes a return at statement 4. Recursion is known in the art.

[0052] Consider the following code, which employs recursion, and which can be used to implement operation of the method shown in FIG. **4** and described above.

```
Arbitrate(AMASK, AVALUE)
    {
        collision=IdentifyCmnd(AMASK, AVALUE)
        if (collision) then
                    {
                        /* recursive call for left side */
                    Arbitrate((AMASK<<1)+1, AVALUE)
                        /* recursive call for right side */
                Arbitrate((AMASK<<1)+1, AVALUE+(AMASK+1))
            }       /* endif */
    } /* return */
```

[0053] The symbol "<<" a represents a bitwise left shift. "<<1" means shift left by one place. Thus, 0001<<1 would be 0010. Note, however, that AMASK is originally called with a value of zero, and 0000<<1 is still 0000. Therefore, for the first recursive call, AMASK=(AMASK<<1)+1. So for the first recursive call, the value of AMASK is 0000+0001=0001. For the second call, AMASK=(0001<<1)+1=0010+1=0011. For the third recursive call, AMASK=(0011<<1)+1=0110+1=0111.

[0054] The routine generates values for AMASK and AVALUE to be used by the interrogator in an identify command "IdentifyCmnd." Note that the routine calls itself if there is a collision. De-recursion occurs when there is no collision. AVALUE and AMASK would have values such as the following assuming there are collisions all the way down to the bottom of the tree.

AVALUE	AMASK
0000	0000
0000	0001
0000	0011
0000	0111
0000	1111*
1000	1111*
0100	0111
0100	1111*
1100	1111*

[0055] This sequence of AMASK, AVALUE binary numbers assumes that there are collisions all the way down to the bottom of the tree, at which point the Identify command sent by the interrogator is finally successful so that no collision occurs. Rows in the table for which the interrogator is successful in receiving a reply without collision are marked with the symbol "*". Note that if the Identify command was successful at, for example, the third line in the table then the interrogator would stop going down that branch of the tree and start down another, so the sequence would be as shown in the following table.

AVALUE	AMASK
0000	0000
0000	0001
0000	0011*
0010	0011
...	...

[0056] This method is referred to as a splitting method. It works by splitting groups of colliding devices **12** into subsets that are resolved in turn. The splitting method can also be viewed as a type of tree search. Each split moves the method one level deeper in the tree. Either depth-first or breadth first traversals of the tree can be employed.

[0057] Another arbitration method that can be employed is referred to as the "Aloha" method. In the Aloha method, every time a device **12** is involved in a collision, it waits a random period of time before retransmitting. This method can be improved by dividing time into equally sized slots and forcing transmissions to be aligned with one of these slots. This is referred to as "slotted Aloha." In operation, the interrogator asks all devices **12** in the field to transmit their identification numbers in the next time slot. If the response is garbled, the interrogator informs the devices **12** that a collision has occurred, and the slotted Aloha scheme is put into action. This means that each device **12** in the field responds within an arbitrary slot determined by a randomly selected value. In other words, in each successive time slot, the devices **12** decide **14** to transmit their identification number with a certain probability.

[0058] The Aloha method is based on a system operated by the University of Hawaii. In 1971, the University of Hawaii began operation of a system named Aloha. A communication satellite was used to interconnect several university computers by use of a random access protocol. The system operates as follows. Users or devices transmit at any time they desire. After transmitting, a user listens for an acknowledgment from the receiver or interrogator. Transmissions from different users will sometimes overlap in time (collide), causing reception errors in the data in each of the contending messages. The errors are detected by the receiver, and the receiver sends a negative acknowledgment to the users. When a negative acknowledgment is received, the messages are retransmitted by the colliding users after a random delay. If the colliding users attempted to retransmit without the random delay, they would collide again. If the user does not receive either an acknowledgment or a negative acknowledgment within a certain amount of time, the user "times out" and retransmits the message.

[0059] In the slotted Aloha scheme, a sequence of coordination pulses is broadcast to all stations (devices). As is the case with the pure Aloha scheme, packet lengths are constant. Messages are required to be sent in a slot time between synchronization pulses, and can be started only at the beginning of a time slot. This reduces the rate of collisions because only messages transmitted in the same slot can interfere with one another. The retransmission mode of the pure Aloha scheme is modified for slotted Aloha such that if a negative acknowledgment occurs, the device retransmits after a random delay of an integer number of slot times.

[0060] FIG. **5** illustrates operation of the slotted Aloha scheme. FIG. **5** shows a packet of data bits transmitted by a

first device **12***a*, which is substantially identical to the device **12**. The interrogator **26** acknowledges receipt without collision, as indicated in FIG. **5** by the symbol ACK. FIG. **5** also shows devices **12***b* and **12***c*, also substantially identical to the device **12**, simultaneously transmitting packets of data to the interrogator **26**, resulting in a collision. The interrogator returns a negative acknowledgment, as indicated in FIG. **5** by the symbol NAK. The devices **12***b* and **12***c* then respectively select random numbers, and retransmit after a time delay corresponding to the selected random number. There is a possibility that the devices **12***b* and **12***c* will again transmit at the same times, causing another collision, but in that case they will retransmit again using newly selected random numbers until there is no collision.

[**0061**] Another form of Aloha scheme is called reservation-Aloha. The reservation-Aloha system has two basic modes: an unreserved mode, and a reserved mode.

[**0062**] In the unreserved mode, a time frame is established and divided into a number of small reservation subslots. Users (devices) use these subslots to reserve message slots. After requesting a reservation, the user (device) listens for an acknowledgment and a slot assignment.

[**0063**] In the reserved mode, a time frame is divided into a certain number of slots whenever a reservation is made. All but the last slot are used for message transmissions. The last slot is subdivided into subslots to be used for reservations. Users (devices) send message packets in their assigned portions of the slots reserved for message transmissions.

[**0064**] FIG. **6** illustrates combining a tree sort method of a type such as the one shown in FIG. **4** with an Aloha method. Combining the two methods allows a minimal number of slots to be used and a takes advantage of the conquer and divide approach of the tree sort method. The method shown in FIG. **6** proceeds in a manner similar to the manner described in connection with FIG. **4**, except that devices **12** in the field that reply for the given AMASK and AVALUE, reply within a randomly selected time slot. This significantly reduces the number of collisions. In one embodiment, the reply includes the unique identification number of the particular device **12**. In one embodiment, the reply includes the random value RV selected by the particular device **12**. In one embodiment, the reply includes both the unique identification number of the particular device **12** as well as the random value RV selected by the same device **12**.

[**0065**] In one embodiment, the same randomly selected time slot is used by a device **12** at different levels of the tree (i.e., for different values of AMASK and AVALUE). In another embodiment, different randomly selected times slots are used by a device **12** at different levels of the tree (i.e., for different values of AMASK and AVALUE). In one embodiment, a combination of these approaches is used. For example, one embodiment utilizes a method where the interrogator goes down the tree until some responses without collision are received, before the devices **12** re-randomize their Aloha random number. This can be classified as an adaptive method. Other adaptive methods are possible. For example, in one embodiment, the number of Aloha slots is reduced at lower levels of the tree. The number of slots can be reduced by the same number for each level down the tree, or by a number that varies depending on the number of levels down the tree. Thus, for example, the number of slots can remain constant through a progression down the tree until some responses without collision are received, at which point the number of slots is reduced.

[**0066**] Thus, this embodiment provides the advantages of both the Aloha methods and the tree sorting methods of establishing communications without collisions.

[**0067**] In another embodiment, levels of the search tree are skipped. Skipping levels in the tree, after a collision caused by multiple devices **12** responding, reduces the number of subsequent collisions without adding significantly to the number of no replies. In real-time systems, it is desirable to have quick arbitration sessions on a set of devices **12** whose unique identification numbers are unknown. Level skipping reduces the number of collisions, both reducing arbitration time and conserving battery life on a set of devices **12**. In one embodiment, every other level is skipped. In alternative embodiments, more than one level is skipped each time.

[**0068**] The trade off that must be considered in determining how many (if any) levels to skip with each decent down the tree is as follows. Skipping levels reduces the number of collisions, thus saving battery power in the devices **12**. Skipping deeper (skipping more than one level) further reduces the number of collisions. The more levels that are skipped, the greater the reduction in collisions. However, skipping levels results in longer search times because the number of queries (Identify commands) increases. The more levels that are skipped, the longer the search times. Skipping just one level has an almost negligible effect on search time, but drastically reduces the number of collisions. If more than one level is skipped, search time increases substantially. Skipping every other level drastically reduces the number of collisions and saves battery power without significantly increasing the number of queries.

[**0069**] Level skipping methods are described in a commonly assigned patent application (attorney docket MI40-117) naming Clifton W. Wood, Jr. and Don Hush as inventors, titled "Method of Addressing Messages, Method of Establishing Wireless Communications, and Communications System," filed concurrently herewith, and incorporated herein by reference.

[**0070**] In compliance with the statute, the invention has been described in language more or less specific as to structural and methodical features. It is to be understood, however, that the invention is not limited to the specific features shown and described, since the means herein disclosed comprise preferred forms of putting the invention into effect. The invention is, therefore, claimed in any of its forms or modifications within the proper scope of the appended claims appropriately interpreted in accordance with the doctrine of equivalents.

1-40. (canceled)

41. A method for performing radio frequency communications, the method comprising:

(A) generating by a first radio frequency identification (RFID) tag a first random number;

(B) transmitting by an interrogator a first request for a first response from the first RFID tag if the first random number is within a first subgroup of possible random numbers;

(C) receiving by the first RFID tag the first request;

(D) communicating by the first RFID tag the first response when the first random number is within the first subgroup, the communicating being performed at a time based upon a second random number;

(E) redefining the first subgroup as a subset of a previous first subgroup and repeating steps B-E when a collision occurs; and

(F) redefining the first subgroup as another subgroup of possible random numbers when the first response is received by the interrogator without collision, the first response including one or more random numbers generated by the first RFID tag.

42. The method of claim 41, wherein the first request includes a selection indicator, the selection indicator identifying one or more of a plurality of RFID tags, the communicating by the first RFID tag only being performed if the selection indicator matches one or more selection bits stored on the first RFID tag.

43. The method of claim 41, further comprising setting an inventoried flag by the first RFID tag to a first state to indicate that the first RFID tag has responded to the interrogator.

44. The method of claim 41, further comprising transmitting by the interrogator a wake-up signal, the wake-up signal causing the first RFID tag to transition from a battery-saving mode to an operational mode.

45. The method of claim 41, wherein a binary search tree is used to define and redefine the first subgroup.

46. The method of claim 45, wherein the redefining further includes skipping one or more levels.

47. The method of claim 41, wherein the one or more random numbers included in the first response include the first random number.

48. The method of claim 41, wherein the first random number is different than the second random number.

49. The method of claim 41, further comprising regenerating the second random number when the first subgroup is redefined.

50. The method of claim 41, further comprising identifying by the interrogator the first RFID tag by at least one random number generated by the first RFID tag in at least one further communication.

51. The method of claim 41, wherein the communicating is performed at least in part by utilizing an ALOHA scheme to communicate the response.

52. A method for a radio frequency identification (RFID) tag to perform wireless communications, the method comprising:

receiving a request, the request including a subset of possible random numbers;

determining whether a first random number generated by the RFID tag is within the subset; and

communicating a response to the request at a time based at least in part on a second random number generated by the RFID tag.

53. The method of claim 52, wherein the request includes a selection indicator, the selection indicator identifying one or more of a plurality of RFID tags, and wherein the communicating a response is only being performed if the selection indicator corresponds with one or more selection bits stored on the RFID tag.

54. The method of claim 52, further comprising setting an inventoried flag to a first state to indicate that the RFID tag has responded.

55. The method of claim 52, further comprising receiving a wake-up signal, the wake-up signal causing the RFID tag to transition from a battery-saving mode to an operational mode.

56. The method of claim 52, wherein the first random number is different than the second random number.

57. The method of claim 52, further comprising repeating the receiving, the determining, and the communicating for each new subset received, wherein the second random number is generated for each new subset.

58. The method of claim 52, further comprising receiving at least one message that identifies the RFID tag by at least one of the first random number and the second random number.

59. The method of claim 52, wherein the RFID tag utilizes an ALOHA scheme to communicate the response.

60. A method for an interrogator to poll a plurality of radio frequency identification (RFID) tags, the method comprising:

causing each of the plurality of RFID tags to generate one or more random numbers, each random number being generated by respective ones of the plurality of RFID tags independently of other ones of the plurality of RFID tags;

defining a first subgroup of a plurality of subgroups of possible random numbers;

transmitting a request to the plurality of RFID tags for identified RFID tags having generated a random number within the first subgroup to respond;

repeatedly redefining the first subgroup to include fewer possible random numbers and transmitting a new request for identified RFID tags having a random number within the first subgroup to respond until receiving a response without a collision or receiving no response; and

repeatedly picking a different subgroup and repeating the transmitting, the receiving, and the repeatedly redefining when a valid response or no response is received until the plurality of RFID tags have been identified, the valid response including at least one random number.

61. The method of claim 60, wherein the request includes a selection indicator, the selection indicator identifying one or more of the plurality of RFID tags from which a response is being requested.

62. The method of claim 60, further comprising transmitting a wake-up signal.

63. The method of claim 60, wherein the defining and the redefining are performed at least in part in accordance with a binary search tree.

64. The method of claim 63, wherein the redefining skips one or more intermediate levels in the binary search tree.

65. The method of claim 60, wherein the at least one random number included in the valid response is the same random number used to identify the subgroup to which the RFID tag belongs.

* * * * *