International Patent Classification: G06Q 50/22 (2012.01) H04B 5/00 (2006.01)

International Application Number: PCT/US2013/065469

International Filing Date: 17 October 2013 (17.10.2013)

Filing Language: English
Publication Language: English

Priority Data:
13/665,234 31 October 2012 (31.10.2012) US

Applicant: ABBOTT DIABETES CARE INC., [US]; 1360 South Loop Road, Alameda, California 94502 (US).

Inventors: SLOAN, Mark; c/o Abbott Diabetes Care Inc., 1360 South Loop Road, Alameda, California 94502 (US).

BERMAN, Glenn; c/o Abbott Diabetes Care Inc., 1360 South Loop Road, Alameda, California 94502 (US).

DINH, John; c/o Abbott Diabetes Care Inc., 1360 South Loop Road, Alameda, California 94502 (US).


Title: WIRELESS COMMUNICATION AUTHENTICATION

For Medical Monitoring Device

Abstract: Methods, systems, and devices for authenticating wireless protocol pairing are provided. Authenticated wireless protocol pairing may include detecting an analyte sample; determining an analyte concentration associated with the detected analyte sample; generating an unauthenticated pairing with an external device by initiating a pairing procedure of a wireless protocol stack with the external device; and on a condition that the wireless protocol stack issues a pairing message, suppressing the pairing message; preventing communication based on the unauthenticated pairing with the external device; generating an authenticated pairing based on the unauthenticated pairing by displaying a pairing authentication message, and in response to user input indicating that the unauthenticated pairing is an authenticated pairing, converting the unauthenticated pairing to an authenticated pairing, and transmitting an indication of the analyte concentration to the external device.

FIG. 7
WIRELESS COMMUNICATION AUTHENTICATION
FOR MEDICAL MONITORING DEVICE

TECHNICAL FIELD

[0001] The embodiments herein relate in general to a device and method for determining and reporting glucose readings in wireless personal area networks for diabetics.

BACKGROUND

[0002] The number of diagnosed cases of diabetes continues to increase in the U.S. and throughout the world, creating enormous economic and public health consequences. Devices and therapies that improve the quality of life for the diabetic patient thus are important not only for the patient, but for society at large. One area in which recently developed technologies have been able to improve the standard of care has been in the maintenance of tight control over the blood glucose levels. It is well known that if a diabetic patient's blood glucose values can be maintained in a relatively narrow and normal range of from about 80 milligrams per deciliter (mg/dL) to about 120 mg/dL, the physiologically damaging consequences of unchecked diabetes can be minimized. With better blood glucose information, diabetic patients can better exercise tight control of their blood glucose level through a variety of means, including diet, exercise, and medication. For this reason a large industry has developed to provide the diabetic population with ever more convenient and accurate ways to measure blood glucose. There are many forms of these measuring devices; one common type is represented by hand-held electronic meters which receive blood samples via enzyme-based "test strips". In using these systems, the patient lances a finger or alternate body site to obtain a blood sample, the strip is inserted into a test strip opening in the meter housing, the sample is applied to the test strip and the electronics in the meter convert a current generated by the enzymatic reaction in the test strip to a blood glucose value. The result is displayed on the (typically) liquid crystal display of the meter. Usually, this display must be large so that diabetics who often have deteriorating vision, can more easily see the result.

[0003] It is known that such hand-held meters can advantageously be manufactured to include wireless communication capability. Such capability can assist the user in downloading data to a home computer or to a handheld computing device, for example. This minimizes the
need for the user to write down data and transfer it later to an electronic record.

It is also known that hand-held meters are often given to users, so that suppliers of the strips used with the meters can generate greater strip sales. This makes the cost of the hand-held meters critical to profitability of the manufacturers. If the cost of a meter is relatively high, profits from the sale of strips will be small or worse yet, non-existent. If the cost of the meter can be reduced, profitability is improved.

Lastly, it is known that if a strip and meter system is convenient to use, patients will test more often and compliance with treatment programs will improve. Including wireless communication in the meter adds convenience, but at a cost. For these reasons, there is a continuing need for a low cost meter and strip glucose monitoring system that nevertheless has highly convenient features, including wireless communication capabilities.

BRIEF SUMMARY

In view of the foregoing, in accordance with the various embodiments of the present disclosure, there are provided methods, devices, and systems for providing wireless communication authentication for medical monitoring device.

In a first aspect, the present disclosure provides a device, including a housing, a processor coupled to the housing, a low energy wireless transmission unit, and a memory device coupled to the housing and the processor, wherein the memory device includes instructions which, when executed by the processor, cause the processor to detect an analyte sample; determine an analyte concentration associated with the detected analyte sample; generate an unauthenticated pairing between the device and an external device by causing the wireless transceiver to initiate a pairing procedure of the wireless protocol stack with the external device, and on a condition that the wireless protocol stack issues a pairing message, suppressing the pairing message, prevent communication based on the unauthenticated pairing between the device and the external device; generate an authenticated pairing based on the unauthenticated pairing by displaying a pairing authentication message, and in response to user input indicating that the unauthenticated pairing is an authenticated pairing; converting the unauthenticated pairing to an authenticated pairing; and cause the wireless transceiver to transmit an indication of the analyte concentration to the external device.

In a second aspect, the present disclosure provides a method including detecting
an analyte sample; determining an analyte concentration associated with the detected analyte sample; generating an unauthenticated pairing with an external device by initiating a pairing procedure of a wireless protocol stack with the external device, and on a condition that the wireless protocol stack issues a pairing message, suppressing the pairing message; preventing communication based on the unauthenticated pairing with the external device; generating an authenticated pairing based on the unauthenticated pairing by displaying a pairing authentication message, and in response to user input indicating that the unauthenticated pairing is an authenticated pairing, converting the unauthenticated pairing to an authenticated pairing; and transmitting an indication of the analyte concentration to the external device.

[0009] It should be noted that two or more of the embodiments described herein, including those described above, may be combined to produce one or more additional embodiments which include the combined features of the individual embodiments.

[0010] These and other objects, features, and advantages of the present disclosure will become more fully apparent from the following detailed description of the embodiments, the appended claims and the accompanying drawings.

**BRIEF DESCRIPTION OF THE DRAWINGS**

[0011] The invention is best understood from the following detailed description when read in conjunction with the accompanying drawings. It is emphasized that, according to common practice, the various features of the drawings are not to-scale. On the contrary, the dimensions of the various features are arbitrarily expanded or reduced for clarity. Included in the drawings are the following figures.

[0012] FIG. 1 is a schematic view showing typical data signal flow between devices of a wireless system constructed according to one embodiment of the present invention.

[0013] FIG. 2 is a schematic view showing the client device of Fig. 1.

[0014] FIG. 3 is a schematic view showing the server device of Fig. 1.

[0015] FIG. 4 is a pictorial view showing a typical client device and typical server devices.

[0016] FIG. 5 is a perspective view showing an integrated device of an alternative embodiment.

[0017] FIG. 6 is a diagram of a health monitor device in accordance with some
embodiments of this disclosure.

Fig. 7 is a diagram of an example of wireless communication authentication for medical monitoring device in accordance with some embodiments of this disclosure.

DETAILED DESCRIPTION

Before the devices and methods of the present disclosure are described in greater detail, it is to be understood that the devices and methods are not limited to particular embodiments described, as such may, of course, vary. It is also to be understood that the terminology used herein is for the purpose of describing particular embodiments only, and is not intended to be limiting, since the scope of the sensors and methods will be limited only by the appended claims.

Unless defined otherwise, all technical and scientific terms used herein have the same meaning as commonly understood by one of ordinary skill in the art to which the methods belong. Although any methods and materials similar or equivalent to those described herein can also be used in the practice or testing of the devices and methods, representative illustrative devices, methods and materials are now described.

It is noted that, as used herein and in the appended claims, the singular forms "a", "an", and "the" include plural referents unless the context clearly dictates otherwise. It is further noted that the claims may be drafted to exclude any optional element. As such, this statement is intended to serve as antecedent basis for use of such exclusive terminology as "solely," "only" and the like in connection with the recitation of claim elements, or use of a "negative" limitation.

Referring to Fig. 1, a wireless system constructed according to a preferred embodiment of the present invention will be described. Test strip 101 electrically communicates with client device 102, which wirelessly communicates with server device 104, such as by two-way radio frequency (RF) contact, infrared (IR) contact, Bluetooth® contact or other known wireless means 103. Optionally, server device 104 can also communicate with other devices such as data processing terminal 105 by direct electronic contact, via RF, IR, Bluetooth® or other wireless means.

Test strip 101 is a commonly known electrochemical analyte test strip, such as a blood glucose test strip as described in U.S. patent application number 09/434,026 filed...
November 4, 1999 entitled "Small Volume In Vitro Analyte Sensor and Methods", incorporated herein by reference. It is mechanically received in a test strip port of a client device 102, similar to a commonly known hand-held blood glucose meter as described in the aforementioned patent application. In the preferred embodiment, client device 102 is constructed without a user interface or display to keep the size and cost of device 102 to a minimum. Client device 102 can take the form of a highlighter or easel-sized pen, as shown in Fig. 4, and can be powered by a single AA or AAA size battery.

[0024] Client device 102 wirelessly communicates with server device 104, preferably using a common standard such as 802.11 or Bluetooth® RF protocol, or an IrDA infrared protocol. Server device 104 can be another portable device, such as a Personal Digital Assistant (PDA) or notebook computer, or a larger device such as a desktop computer, appliance, etc. as shown by the examples in Fig. 4. Preferably, server device 104 does have a display, such as a liquid crystal display (LCD), as well as an input device, such as buttons, a keyboard, mouse or touch-screen. With this arrangement, the user can control client device 102 indirectly by interacting with the user interface(s) of server device 104, which in turn interacts with client device 102 across wireless link 103.

[0025] Server device 104 can also communicate with another device 105, such as for sending glucose data from devices 102 and 104 to data storage in device 105, and/or receiving instructions or an insulin pump protocol from a health care provider computer 105. Examples of such communication include a PDA 104 synching data with a personal computer (PC) 105, a mobile phone 104 communicating over a cellular network with a computer 105 at the other end, or a household appliance 104 communicating with a computer system 105 at a physician's office.

[0026] Referring to Fig. 2, internal components of a blood glucose meter 102 of the preferred embodiment are shown. Alternatively, user input 202, such as push button(s), and other sections can be eliminated to reduce size and cost of client device 102. The glucose meter housing may contain any glucose sensing system of the type well known in the art that can be configured to fit into a small profile. Such a system can include, for example, the electrochemical glucose strip and meter sensing system sold by TheraSense, Inc. of Alameda, California under the FreeStyle® brand, or other strip and meter glucose measuring systems. The housing may thus encompass the sensor electronics and a strip connector, which connector is accessed via a test
strip port opening in the housing. The housing will typically also include a battery or batteries.

Referring to Fig. 3, internal components of a server device 104 of the preferred embodiment are shown. Note that a redundant test strip interface 301 can be provided if desired for receiving test strips 101. Device 104 can be a proprietary unit designed specifically for use with blood glucose meters, or can be a generic, multipurpose device such as a standard PDA. An example of a similar device designed for blood glucose testing is disclosed in U.S. Patent No. 6,560,471 issued May 6, 2003 to TheraSense, Inc. entitled "Analyte Monitoring Device and Methods of Use", incorporated herein by reference.

Figure 4 shows examples of the devices to and from which the meter of the invention can communicate. Such devices will become part of an individual's personal area network and each becomes enabled with short range wireless communication capabilities. Desktop, laptop and handheld computers, as well as printers can be so enabled and will provide displays and printouts valuable as records for the diabetic. Telephones will also be enabled in this fashion and can be used for displaying glucose data as well as further transmitting the data over larger networks. Many of these devices can assist the diabetic by responding to glucose levels by providing alarms, or suggesting that action be taken to correct a hypo or hyperglycemic condition, or to call necessary medical assistance. Diabetics are aware of the risks involved in driving when glucose levels are out of range and particularly when they are too low. Thus, the navigation computer in the diabetic's car may become part of the local area network and will download glucose data from the meter when the diabetic enters the car. For safety sake, the car computer system may be programmed to require that the diabetic perform a glucose test before driving, and more specifically the car may be disabled unless the diabetic takes the test and the result is in an appropriate range.

The pen shaped client device 102 shown in Fig. 4 preferably has a test strip port 201 (not shown in Fig. 4) located on its distal end. Because the sensitive analog "front end" circuitry associated with measuring the very small electrochemistry currents from test strips 101 is located adjacent strip port 201, it is advisable to not design a wireless link antenna too close to this distal end as it may interfere with the proper operation of the glucose sensing circuitry. On the other hand, if the wireless link antenna is located at the proximal end of the client device 102, it will likely be covered by the hand of the user holding it, which may limit the range of the low transmission power device to an unacceptable distance. Accordingly, it is preferable to design
the layout of client device 102 such that an internal antenna is located in a middle section of the
device away from the distal and proximal ends.

[0030] Referring to Fig. 5, an alternative embodiment of the present invention is shown. Due to the reduced size of a blood glucose meter 102 when it does not include a display or push buttons, it can be combined with a lancing device to form an integrated unit 102'. Test strip port 201 can be located in the side of integrated device 102' or wherever there is room available. A test strip storage compartment can also be located within integrated device 102' and accessed through a flip-lid 220 or other suitable closure means. If room permits, a second test strip storage compartment (not shown) can be included so that fresh strips and used strips can be separately stored. Preferably, a desiccant is provided in one of the storage compartments to preserve the fresh strips. The design and use of lancing devices is described in U.S. Patent Number 6,283,982 issued to TheraSense, Inc. on September 4, 2001 entitled "Lancing Device and Method of Sample Collection", incorporated herein by reference. By integrating these features together in a single device without a user interface, the typical test kit that is carried around by people with diabetes can be made much smaller, easier to handle, and less costly.

[0031] Thus, one of the important features of the invention is reliance of the "displayless" glucose meter unit on a separate display device in order to minimize the complexity and cost of the meter unit. This permits the user to use the larger display units within his or her personal area network, all of which can be synchronized as they interact and communicate with the wireless enabled meter. When the meter is used, the sequences through which the user must "step" to complete the test are readily viewed on the larger display units (e.g. entering the calibration code, prompting application of the sample). At the same time the meter unit is simplified, smaller and less expensive to manufacture. Additionally, control buttons that are found on typical glucose meters can be eliminated, saving additional size and cost, since the user can rely on the user in out features of the server device instead. It is expected that the simplified, wireless enabled meters of the invention may ultimately become inexpensive enough to make them disposable after a specified number of uses, permitting the producer to routinely upgrade as appropriate.

[0032] Additionally, the system permits the user to include security coding at any time the meter unit accesses a display device, so that the user's data is secure. That is, it is considered an important feature of the invention that when the "client" meter of the invention is used, that
the system will require the user to enter an identity code in order to verify that the person handling the meter is indeed an authorized user. Of course, it is possible for the system to permit more than one user if the meter owner so desires. Moreover, the user's data may optionally be encrypted prior to wireless transmission and thereafter respectively decrypted upon wireless reception.

While the module need not include a large or expensive display, it may nevertheless be advantageous to include some ability to advise the user of a glucose level which is determined when the module is used as a "stand-alone" unit. For example, the module could include a very low cost, small three digit LCD display. Alternatively, the module could include LED indicator lights (e.g. red for out of desired range, green for within desired range). Other possibilities include a red LED for below range, a green LED for within range, and a yellow LED for above range, or a column of LEDs or an electroluminescent strip (similar to those used on common batteries to indicate battery life) to indicate approximate or relative glucose levels.

FIG. 6 shows a diagram of a health monitor device 600 in accordance with some embodiments of this disclosure. The health monitor device 600 may be used for determining a concentration of an analyte in blood or interstitial fluid. For example, the health monitor device 600 may be an analyte test meter, such as a glucose test meter that may be used for determining an analyte concentration, such as a blood glucose concentration, of a sample for determination of a blood glucose level of a patient, such as a patient with Type-1 or Type-2 diabetes. In some embodiments, the health monitor device 600 may be a blood glucose meter, a continuous monitor, an insulin pump, a blood pressure meter, a heart rate monitor, a thermometer, or any other health monitor device capable of measuring, monitoring, or storing raw or analyzed medical data electronically.

The health monitor device 600 may communicate in a wireless communication system, such as the wireless system shown in Fig. 1. For example, the health monitor device 600 may receive fluid samples, or sample data, from a sensor device 602, such as the test strip 101 shown in Fig. 1, and may wirelessly transmit data to an external device 604, such as the server device 104 shown in Fig. 1. The health monitor device 600 may include a housing 610, a processor 620, a sensor interface 630, a user interface 640, a clock 650, a data storage unit 660, a power supply 670, and a communication interface 680.

The housing 610 may physically enclose one or more of the processor 620, the
sensor interface 630, the user interface 640, the clock 650, the data storage unit 660, the power supply 670, or the communication interface 680, and may be configured to fit into a small profile. Although the housing 610 is shown a single physical unit, the housing 610 may be implemented as one or more physical units that may be physically or electronically connected. Although not shown in Fig. 6, the housing 610 may include one or more ports, such as a test strip port, a power port, an audio connection port, or a data connection port. For example, the housing 610 may include a test strip port configured to receive a test strip, which may include a fluid sample, and may be connected to the sensor interface 630.

[0037] The processor 620 may include any device capable of manipulating or processing a signal or other information, including an optical processor, a quantum processor, a molecular processor, or a combination thereof. For example, the processor 620 may include a general purpose processor, a central processing unit (CPU), a special purpose processor, a plurality of microprocessors, a controller, a microcontroller, an Application Specific Integrated Circuit (ASIC), a Field Programmable Gate Array (FPGA), a programmable logic array, programmable logic controller, microcode, firmware, any type of integrated circuit (IC), a state machine, or any combination thereof. As used herein, the term "processor" includes a single processor or multiple processors. The processor 620 may be operatively coupled to the sensor interface 630, the user interface 640, the clock 650, the data storage unit 660, the power supply 670, or the communication interface 680.

[0038] In some embodiments, the sensor interface 630 may receive a fluid sample, such as a fluid sample transported via the test strip 101 shown in Fig. 1, and the processor 620 may control the sensor interface 630 to analyze the fluid sample to determine an associated analyte level. In some embodiments, the sensor interface 630 may receive raw or analyzed data indicating an analyte level associated with a fluid sample analyzed at an external measurement device, such as a continuous analyte monitoring device, via a wireless communication medium, such as radio frequency identification (RFID). For example, the continuous analyte monitoring device may include a transcutaneously implanted sensor, such as an implantable glucose sensor, that may continually or substantially continually measure an analyte concentration of a bodily fluid. In some embodiments, the sensor interface 630 may receive analyte related data from the external measurement device periodically, based on a transmission schedule, or may request the data from the external measurement device.
The user interface 640 may include a display unit and one or more input elements, such as buttons, jogs, or dials. The user interface 640, or a portion thereof, may be integrated with the housing 610. For example, the user interface 640 may form a part of an external surface of the housing 610. The user interface 640, or a portion thereof, may be configured to allow a user of the health monitor device 600 to receive information, input information, or otherwise interact, with the health monitor device 600. For example, the user of the health monitor device 600 may operate the one or more input buttons to enter a calibration code associated with a test strip or other fluid sample reception device. In another example, the user interface 640 may present visual, tactile, or auditory information indicating, for example, a blood glucose measurement to the user. In some embodiments, the display unit may include a graphical display unit, such as a LCD or an LED display, an auditory display unit, such as speaker, or both a graphical display and an audio display. In some embodiments, the user interface 640 may include a touch screen display. In some embodiments, the display unit, the input elements, or both may be omitted from the user interface 640.

The clock 650 may be operatively coupled to the processor 620 and may provide a clock signal at discreet clock frequencies to the processor 620. For example, the clock may include an oscillator, such as a quartz crystal oscillator, or any other device capable of producing a clock signal for indicating a real time clock.

The data storage unit 660 may store raw data, analyzed data, or both. In some embodiments, the data storage unit 660 may store instructions that may be executed by the processor to, for example, perform analysis, such as analyte concentration analysis and medication dosage calculation. The data storage unit 660 may include any non-transitory computer-readable or computer-readable medium, such as any tangible device that can, for example, contain, store, communicate, or transport instructions, or any information associated therewith, for use by or in connection with the processor 620. The non-transitory computer-readable or computer-readable medium may be, for example, a solid state drive, a memory card, removable media, a read only memory (ROM), a random access memory (RAM), any type of disk including a hard disk, a floppy disk, an optical disk, a magnetic or optical card, an application specific integrated circuits (ASICs), or any type of non-transitory media suitable for storing electronic information, or any combination thereof. The data storage unit 660 may be operatively connected to, for example, the processor 620 through, for example, a memory bus.
The power supply 670 may be any suitable device for powering the health monitor device 600, or any portion thereof. For example, the power supply 670 may include a wired power source; one or more dry cell batteries, such as nickel-cadmium (NiCd), nickel-zinc (NiZn), nickel metal hydride (NiMH), lithium-ion (Li-ion); solar cells; fuel cells; or any other device capable of powering the health monitor device 600. The processor 620, the sensor interface 630, the user interface 640, the clock 650, the data storage unit 660, or the communication interface 680, may have a lower duty cycle and may actively operate less frequently, for shorter periods of using the device 600, for example, using a wireless communication protocol, such as Bluetooth® RF protocol, a cellular protocol, or any other wireless protocol. In some embodiments, the communication interface 680 may include a receiver, a transmitter, or a transceiver. For example, the communication interface 680 may include a wireless transmission unit, such as a Bluetooth® low energy wireless transmission unit. Although not expressly shown in Fig. 6, the communication interface 680 may include a wireless antenna, a wired communication port, such as an Ethernet port, an infrared port, a serial port, or any other wired or wireless unit capable of interfacing with a wired or wireless electronic communication medium. In some embodiments, the health monitor device 600 may communicate with the external device 604 indirectly via another device, or series of devices. For example, the health monitor device 600 may communicate with the external device 604 via a network, wherein the health monitor device 600 may transmit signals to, for example, an access point (not shown), and the access point may transmit the signals to the external device 604, in the same or a different format, via one or more other devices in a network.

In some embodiments, the communication interface 680 may communicate with the external device 604 using a low energy wireless communication protocol, such as Bluetooth® low energy. Communicating using a low energy wireless communication protocol may allow the communication interface 680 to use substantially less power than communicating using other wireless communication protocols, such as other versions of Bluetooth®. For example, using a low energy wireless communication protocol, the communication interface 680 may have a lower duty cycle and may actively operate less frequently, for shorter periods of
time, or both.

[0045] In some embodiments, the processor 610, the communication interface 680, or a
combination of the processor 610 and the communication interface 680, may determine whether
to use a wireless communication protocol, such as Bluetooth®, or a low energy wireless
communication protocol, such as Bluetooth® low energy. For example, the processor 610 may
determine which wireless communication protocol to use based on network conditions, battery
conditions, sensed data, or a combination thereof.

[0046] In some embodiments, the health monitor device 600 may audibly present
information, such as information indicating an analyte concentration, information indicating a
rate of change of an analyte concentration, or information indicating the exceeding of a threshold
of an analyte concentration, which may indicate, for example, hypo- or hyperglycemia. For
example, the user interface 640 may include a speaker, and the health monitor device 600 may
present the audio signal via the speaker. In some embodiments, the health monitor device 600
may transmit raw or analyzed analyte information to the external device 604 and the external
device 604 may generate an audio signal for presentation. In some embodiments, the health
monitor device 600 may generate an audio signal indicating the information and may transmit
the audio indication to the external device 604 for audio presentation.

[0047] Although shown as separate elements, the processor 620, the sensor interface 630,
the user interface 640, the clock 650, the data storage unit 660, the power supply 670, the
communication interface 680, or any combination thereof, may be integrated in one or more
electronic units, circuits, or chips.

[0048] Fig. 7 shows an example of wireless communication authentication in accordance
with some embodiments of this disclosure. In some embodiments, a health monitor device, such
as the health monitor device 600 shown in Fig. 6, may perform wireless communication
authentication to establish an authenticated wireless communication link with an external device
to transmit an audio indication of health monitoring information, such as analyte information, to
the external device. Wireless communication authentication may include detecting a sample at
710, analyzing the sample at 720, determining an analyte concentration at 730, storing analyte
information at 740, generating an unauthenticated pairing at 750, preventing communication
using the pairing at 760, generating an authenticated pairing at 770, transmitting an indication of
the analyte concentration at 780, or a combination thereof. Although wireless communication
authentication is described with reference to detecting and transmitting analyte information, wireless communication authentication may be used to pair a health monitor device with an external device independently of detecting and transmitting analyte information.

[0049] A sample, such as a blood sample, may be identified at 710. For example, the health monitor device may include a sensor interface, such as the sensor interface 630 shown in Fig. 6, configured to receive a fluid sample, such as a fluid sample transported via a test strip, such as the test strip 101 shown in Fig. 1. In some embodiments, the sample may be identified by an external measurement device, such as a continuous analyte monitoring device, configured to communicate with the health monitor device using, for example, a short range wireless communication method, such as RFID. For example, the continuous analyte monitoring device may include a transcutaneously implanted sensor that may continually or substantially continually measure an analyte concentration of a bodily fluid.

[0050] The sample may be analyzed to determine a corresponding analyte level, such as a glucose level, at 720. For example, the health monitor device may include a processor, such as the processor 620 shown in Fig. 6, configured to analyze the sample. In some embodiments, the sample may be analyzed by an external analysis device, such as a continuous analyte monitoring device, configured to communicate with the health monitor device.

[0051] An analyte concentration may be identified at 730. For example, the analyte concentration may be identified based on the sample analysis at 720. In some embodiments, the analyte concentration may be received from an external analysis device, such as a continuous analyte monitoring device, configured to communicate with the health monitor device. In some embodiments, the analyte concentration may be identified based on stored information, such as previously stored raw or analyzed sample data.

[0052] In some embodiments, raw or analyzed analyte information, such the analyte concentration identified at 730, may be stored at 740. For example, health monitor device may include a data storage unit, such as the memory 660 shown in Fig. 6, a processor, such as the processor 620 shown in Fig. 6, a sensor interface, such as the sensor interface 630 shown in Fig. 6, or a combination thereof, and the processor, the sensor interface, or a combination thereof, may identify the analyte concentration based on raw or analyzed analyte data stored on the data storage unit.

[0053] An unauthenticated wireless communications pairing may be generated at 750.
Generating the unauthenticated wireless communications pairing may include performing a wireless protocol stack pairing procedure at 752, suppressing a pairing message at 754, completing the pairing procedure at 756, or a combination thereof.

A wireless protocol stack pairing, or bonding, procedure may be performed at 752 to establish a relationship (bond or pairing) between the health monitor device and the external device. In some embodiments, the wireless protocol stack pairing procedure may be omitted if the health monitor device previously established an authenticated communication link with the external device. Performing the wireless protocol stack pairing procedure may include generating a shared secret key (link key) at the health monitor device and the external device.

In some embodiments, the wireless protocol stack pairing procedure may include displaying a pairing message at the health monitor device, the external device, or both. For example, the wireless protocol stack pairing procedure may request user input of a pin code or passkey, such as an alphanumeric string. Implementations of the pairing message may vary among devices, which may cause the wireless protocol stack pairing procedure to fail, or may make the wireless protocol stack pairing procedure difficult for users to understand.

The pairing message may be suppressed at 754. For example, the wireless protocol stack pairing procedure may be a Bluetooth® pairing procedure and the pairing message may include one or more Bluetooth® pairing confirmation messages. In some embodiments, the wireless protocol stack pairing procedure may not include pairing messages and suppressing the complex pairing message may be omitted. For example, the wireless protocol stack pairing procedure may be a simplified Bluetooth® pairing procedure that does request user input and suppressing the pairing procedure may be omitted.

The wireless protocol stack pairing procedure may be completed at 756. Completing the wireless protocol stack pairing procedure may include storing an unauthenticated wireless protocol bond or pairing. In some embodiments, the health monitor device, the external device, or both, may store an indication of the unauthenticated wireless protocol bond.

In some embodiments, communication of health related information between the health monitor device and the external device may be prevented at 760. For example, communication may be prevented where a wireless protocol bond (pairing) does not exist, or where an established wireless protocol bond is an unauthenticated pairing.

An authenticated pairing may be generated at 760. Generating an authenticated
pairing may include performing a pairing authentication procedure at 772, converting the unauthenticated pairing to an authenticated pairing at 774, or a combination thereof.

[0060] Performing the pairing authentication procedure at 772 may include performing an application layer authentication, which may include displaying authentication information at the health monitor device, the external device, or both.

[0061] A user may confirm the authentication at the health monitor device, the external device, or both, and the unauthenticated pairing may be converted to an authenticated pairing at 774. For example, confirming the authentication may include requesting user input at the health monitor device, the external device, or both, to authenticate the wireless communication protocol bond between the health monitor device and the external device. User input authenticating the wireless protocol bond may be received at the health monitor device, the external device, or both.

In some embodiments, converting the unauthenticated pairing to an authenticated pairing may include storing an indication that the wireless protocol bond is authenticated, or removing an indication that the wireless protocol bond is not authenticated, at the health monitor device, the external device, or both.

[0062] In some embodiments, the authentication information may include a short alphanumeric string, such a four or six character string. For example, the authentication information may include, a name, or part of a name, associated with the health monitor device or the external device, such as a name of a user logged in on the external device, or a name of the device. In another example, the authentication information may include an identifier, or part of an identifier, associated with the device, such as a serial number of the health monitor device, or part of a GUID associated with the external device. In another example, the authentication information may include a phone number, associated with one or both of the devices. In another example, the authentication information may include a random or pseudorandom string.

[0063] For example, the external device may generate an authentication string, and may transmit the string to the health monitor device. In another example, the health monitor device may generate the authentication string and may transmit the string to the external device. A user may confirm the authentication string at the health monitor device, the external device, or both.

For example, the authentication string may be displayed at the health monitor device and the external device, and the user may confirm the authentication, or reject the authentication, based on a comparison of the authentication string displayed at each device.
[0064] In some embodiments, the authentication information may include an image. For example, an image may be a diagram of a simple object, such as a circle, a star, or a square; an image may be a photograph, such as a photograph of a user of the external device; or an image may be any other graphical element capable of reasonably authenticating the pairing. In some embodiments, image may be an indication of an image, such as an index of a randomly or pseudorandomly selected image from a shared source of images, such as a shared table or database of images. A user may confirm or reject the authentication based on a comparison of the authentication image displayed at each device.

[0065] For example, the health monitor device may randomly or pseudorandomly select an authentication image and may send the authentication image, or an indication of the authentication image, to the external device. In another example, the external device may randomly or pseudorandomly select an authentication image and may send the authentication image, or an indication of the authentication image, to the health monitor device.

[0066] An indication of the analyte concentration may be transmitted at 780. For example, the indication of the analyte concentration may be transmitted from the health monitor device to the external device using, for example, a Bluetooth® link established based on the bond established at 750 and authenticated at 770. In some embodiments, transmitting the indication of the analyte concentration may include transmitting raw or analyzed analyte information. In some embodiments, transmitting the indication of the analyte concentration may include transmitting health care instructions. In some embodiments, transmitting the indication of the analyte concentration may include synchronizing information between the health monitor device and the external device.

[0067] It is appreciated that certain features of the devices and methods, which are, for clarity, described in the context of separate embodiments, may also be provided in combination in a single embodiment. Conversely, various features of the devices and methods, which are, for brevity, described in the context of a single embodiment, may also be provided separately or in any suitable sub-combination. All combinations of the embodiments are specifically embraced by the present invention and are disclosed herein just as if each and every combination was individually and explicitly disclosed, to the extent that such combinations embrace operable processes and/or devices/systems/kits. In addition, all sub-combinations listed in the embodiments describing such variables are also specifically embraced by the present devices and
methods and are disclosed herein just as if each and every such sub-combination was individually and explicitly disclosed herein.

[0068] As will be apparent to those of skill in the art upon reading this disclosure, each of the individual embodiments described and illustrated herein has discrete components and features which may be readily separated from or combined with the features of any of the other several embodiments without departing from the scope or spirit of the present devices and methods. Any recited method can be carried out in the order of events recited or in any other order which is logically possible.

[0069] Various other modifications and alterations in the structure and method of operation of this invention will be apparent to those skilled in the art without departing from the scope and spirit of the invention. Although the invention has been described in connection with specific preferred embodiments, it should be understood that the invention as claimed should not be unduly limited to such specific embodiments. It is intended that the following claims define the scope of the present invention and that structures and methods within the scope of these claims and their equivalents be covered thereby.
What is claimed is:

1. A medical monitoring device comprising:
   a housing;
   a processor coupled to the housing;
   a wireless transceiver implementing a wireless protocol stack; and
   a memory device coupled to the housing and the processor, wherein the memory device comprises instructions which, when executed by the processor, cause the processor to:
      - detect an analyte sample,
      - determine an analyte concentration associated with the detected analyte sample,
      - generate an unauthenticated pairing between the device and an external device by:
        - causing the wireless transceiver to initiate a pairing procedure of the wireless protocol stack with the external device; and
        - on a condition that the wireless protocol stack issues a pairing message, suppressing the pairing message,
      - prevent communication based on the unauthenticated pairing between the device and the external device,
      - generate an authenticated pairing based on the unauthenticated pairing by:
        - displaying a pairing authentication message; and
        - in response to user input indicating that the unauthenticated pairing is an authenticated pairing, converting the unauthenticated pairing to an authenticated pairing, and
      - cause the wireless transceiver to transmit an indication of the analyte concentration to the external device.

2. The medical monitoring device of claim 1, wherein the memory device comprises instructions which, when executed by the processor, cause the processor to suppress the pairing message by preventing the pairing message from being displayed.
3. The medical monitoring device of claim 1, wherein the memory device comprises instructions which, when executed by the processor, cause the processor to suppress the pairing message by causing the wireless transceiver to transmit a confirmation code to the external device without user input.

4. The medical monitoring device of claim 1, wherein the memory device comprises instructions which, when executed by the processor, cause the processor to display the pairing authentication message on a condition that pairing procedure of the wireless protocol stack is complete.

5. The medical monitoring device of claim 1, wherein the memory device comprises instructions which, when executed by the processor, cause the processor to display the pairing authentication message by displaying an image, a telephone number associated with the external device, a user name received from the external device, a unique identifier associated with the device, a unique identifier associated with the external device, a portion of a unique identifier associated with the device, a portion of a unique identifier associated with the external device, a word, or a random character string.

6. The medical monitoring device of claim 1, wherein the wireless protocol stack is a Bluetooth® wireless protocol stack and the pairing procedure is a Bluetooth® pairing procedure.

7. The medical monitoring device of claim 1, wherein the memory device comprises instructions which, when executed by the processor, cause the processor to prevent communication by preventing communication of analyte information.

8. The medical monitoring device of claim 1, wherein the memory device comprises instructions which, when executed by the processor, cause the processor to generate the unauthenticated pairing by generating a pairing and generating an indication that the pairing is not authenticated.
9. The medical monitoring device of claim 1, wherein the memory device comprises instructions which, when executed by the processor, cause the processor to generate the authenticated pairing by performing an application layer authentication procedure.

10. The medical monitoring device of claim 1, the memory device comprises instructions which, when executed by the processor, cause the processor to, in response to user input indicating that the unauthenticated pairing is not an authenticated pairing, remove the unauthenticated pairing.

11. A method comprising:
   detecting an analyte sample;
   determining an analyte concentration associated with the detected analyte sample;
   generating an unauthenticated pairing with an external device by:
      initiating a pairing procedure of a wireless protocol stack with the external device, and
      on a condition that the wireless protocol stack issues a pairing message, suppressing the pairing message;
   preventing communication based on the unauthenticated pairing with the external device;
   generating an authenticated pairing based on the unauthenticated pairing by:
      displaying a pairing authentication message, and
      in response to user input indicating that the unauthenticated pairing is an authenticated pairing, converting the unauthenticated pairing to an authenticated pairing; and
   transmitting an indication of the analyte concentration to the external device.

12. The method of claim 11, wherein suppressing the pairing message includes preventing the pairing message from being displayed.
13. The method of claim 11, wherein suppressing the pairing message includes transmitting a confirmation code to the external device without user input.

14. The method of claim 11, wherein displaying the pairing authentication message is performed on a condition that pairing procedure of the wireless protocol stack is complete.

15. The method of claim 11, wherein displaying the pairing authentication message includes displaying an image, a telephone number associated with the external device, a user name received from the external device, a unique identifier associated with the device, a unique identifier associated with the external device, a portion of a unique identifier associated with the external device, a portion of a unique identifier associated with the external device, a word, or a random character string.

16. The method of claim 11, wherein the wireless protocol stack is a Bluetooth® wireless protocol stack and the pairing procedure is a Bluetooth® pairing procedure.

17. The method of claim 11, wherein preventing communication includes preventing communication of analyte information.

18. The method of claim 11, wherein generating the unauthenticated pairing includes generating a pairing and generating an indication that the pairing is not authenticated.

19. The method of claim 11, wherein generating the authenticated pairing includes performing an application layer authentication procedure.

20. The method of claim 11, further comprising:
   in response to user input indicating that the unauthenticated pairing is not an authenticated pairing, remove the unauthenticated pairing.
FIG. 7

1. DETECT SAMPLE
2. ANALYZE SAMPLE
3. DETERMINE ANALYTE CONCENTRATION
4. STORE ANALYTE INFORMATION
5. GENERATE UNAUTHENTICATED PAIRING
6. WIRELESS PROTOCOL STACK PAIRING PROCEDURE
7. SUPPRESS PAIRING MESSAGE
8. COMPLETE PAIRING PROCEDURE
9. PREVENT COMMUNICATION
10. GENERATE AUTHENTICATED PAIRING
11. DISPLAY AUTHENTICATION MESSAGE
12. CONVERT PAIRING
13. TRANSMIT ANALYTE INFORMATION
A. CLASSIFICATION OF SUBJECT MATTER

G06Q 50/22(2012.01)i, H04B 5/00(2006.01)i

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)

G06Q 50/22; H04B 7/00; G05B 11/01; H04W 12/04; G06F 21/00; H04B 5/00

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

Korean utility models and applications for utility models

Japanese utility models and applications for utility models

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

eKOMPASS(KIPO internal) & Keywords: bluetooth, analyte, glucose, blood

C. DOCUMENTS CONSIDERED TO BE RELEVANT

<table>
<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>Y</td>
<td>US 2011-0063094 Al (ULF MEIJERTOBERENS et al.) 17 March 2011</td>
<td>1-20</td>
</tr>
<tr>
<td></td>
<td>See abst ract, paragraph [0065], claims 1, 6 and figure 1.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>See abst ract, paragraph [0022], [0050], claims 1, 3 and figures 2, 3.</td>
<td></td>
</tr>
<tr>
<td>A</td>
<td>US 2008-0160914 Al (MATTHEW B. MCRAE et al.) 03 July 2008</td>
<td>1-20</td>
</tr>
<tr>
<td></td>
<td>See abst ract, claim 1 and figure 2.</td>
<td></td>
</tr>
<tr>
<td>A</td>
<td>US 2008-0090524 Al (KYONG, HUN LEE et al.) 17 April 2008</td>
<td>1-20</td>
</tr>
<tr>
<td></td>
<td>See abst ract, claim 1 and figure 5.</td>
<td></td>
</tr>
<tr>
<td>A</td>
<td>US 2011-0217950 Al (ALAN KOZLAY) 08 Sept ember 2011</td>
<td>1-20</td>
</tr>
<tr>
<td></td>
<td>See abst ract, claim 1 and figure 1.</td>
<td></td>
</tr>
</tbody>
</table>

Further documents are listed in the continuation of Box C.

See patent family annex.

* Special categories of cited documents:
  "A" document defining the general state of the art which is not considered to be of particular relevance
  "E" earlier application or patent but published on or after the international filing date
  "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
  "O" document referring to an oral disclosure, use, exhibition or other means
  "P" document published prior to the international filing date but later than the priority date claimed

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search

24 January 2014 (24.01.2014)

Date of mailing of the international search report

24 January 2014 (24.01.2014)

Name and mailing address of the ISA/KR

Korean Intellectual Property Office
189 Cheongsa-ro, Seo-gu, Daegu Metropolitan City, 302-701, Republic of Korea
Facsimile No. +82-42-472-7140

Authorized officer

OH, Eung Gie
Telephone No. +82-42-481-8744

Form PCT/ISA/210 (second sheet) (July 2009)
Information on patent family members

<table>
<thead>
<tr>
<th>Patent document cited in search report</th>
<th>Publication date</th>
<th>Patent family member(s)</th>
<th>Publication date</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>CN 101821722 A</td>
<td>01/09/2010</td>
</tr>
<tr>
<td></td>
<td></td>
<td>EP 2162824 A2</td>
<td>17/03/2010</td>
</tr>
<tr>
<td></td>
<td></td>
<td>KR 10-2010-0053526 A</td>
<td>20/05/2010</td>
</tr>
<tr>
<td></td>
<td></td>
<td>wo 2009-005950 A2</td>
<td>08/01/2009</td>
</tr>
<tr>
<td></td>
<td></td>
<td>wo 2009-005950 A3</td>
<td>12/03/2009</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CN 101015173 B</td>
<td>19/06/2013</td>
</tr>
<tr>
<td></td>
<td></td>
<td>EP 1635508 Al</td>
<td>15/03/2006</td>
</tr>
<tr>
<td></td>
<td></td>
<td>EP 1792442 Al</td>
<td>06/06/2007</td>
</tr>
<tr>
<td></td>
<td></td>
<td>EP 1792442 B1</td>
<td>24/02/2010</td>
</tr>
<tr>
<td></td>
<td></td>
<td>JP 04739342 B2</td>
<td>03/08/2011</td>
</tr>
<tr>
<td></td>
<td></td>
<td>JP 2008-512891 A</td>
<td>24/04/2008</td>
</tr>
<tr>
<td></td>
<td></td>
<td>KR 10-1270039 B1</td>
<td>31/05/2013</td>
</tr>
<tr>
<td></td>
<td></td>
<td>wo 2006-027725 Al</td>
<td>16/03/2006</td>
</tr>
<tr>
<td>US 2008-0160914 Al</td>
<td>03/07/2008</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>EP 1912388 A3</td>
<td>01/08/2012</td>
</tr>
<tr>
<td></td>
<td></td>
<td>US 8045921 B2</td>
<td>25/10/2011</td>
</tr>
</tbody>
</table>

Form PCT/ISA/210 (patent family annex) (July 2009)