



US 20110019824A1

(19) **United States**
(12) **Patent Application Publication**
Sattiraju et al.

(10) **Pub. No.: US 2011/0019824 A1**
(43) **Pub. Date: Jan. 27, 2011**

(54) **LOW POWER RADIOFREQUENCY (RF) COMMUNICATION SYSTEMS FOR SECURE WIRELESS PATCH INITIALIZATION AND METHODS OF USE**

Related U.S. Application Data

(60) Provisional application No. 60/982,225, filed on Oct. 24, 2007.

(75) Inventors: **Venkateswara R. Sattiraju**, Union City, CA (US); **Ali Niknejad**, Berkeley, CA (US); **Louis Yun**, Los Altos, CA (US)

Publication Classification

(51) **Int. Cl.**
H04W 52/02 (2009.01)
H04K 1/00 (2006.01)
(52) **U.S. Cl.** **380/270; 370/311**

Correspondence Address:
WILSON, SONSINI, GOODRICH & ROSATI
650 PAGE MILL ROAD
PALO ALTO, CA 94304-1050 (US)

(57) **ABSTRACT**

Provided herein is a wireless healthcare system comprising at least one sensor and a base unit adaptable to be in communication with the sensor. The sensor can be is adaptable to communicate with the base unit at a first power during formation of a communication link and is further adaptable to communicate with the base unit at a second power after the communication link has been formed, and wherein the sensor and base unit are components of a wireless healthcare system. The sensor can be a patch adaptable to be positioned on the surface of a patient. Further provided herein is a method of using the wireless healthcare system and kit.

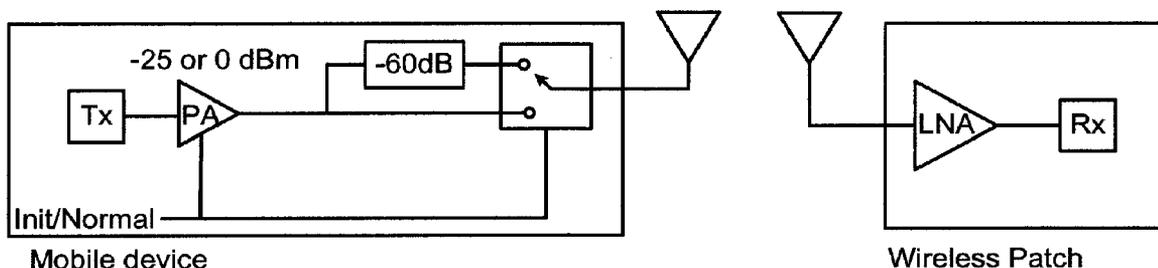
(73) Assignee: **HMICRO, INC.**, Los Altos, CA (US)

(21) Appl. No.: **12/739,549**

(22) PCT Filed: **Oct. 22, 2008**

(86) PCT No.: **PCT/US08/80716**

§ 371 (c)(1),
(2), (4) Date: **Oct. 11, 2010**



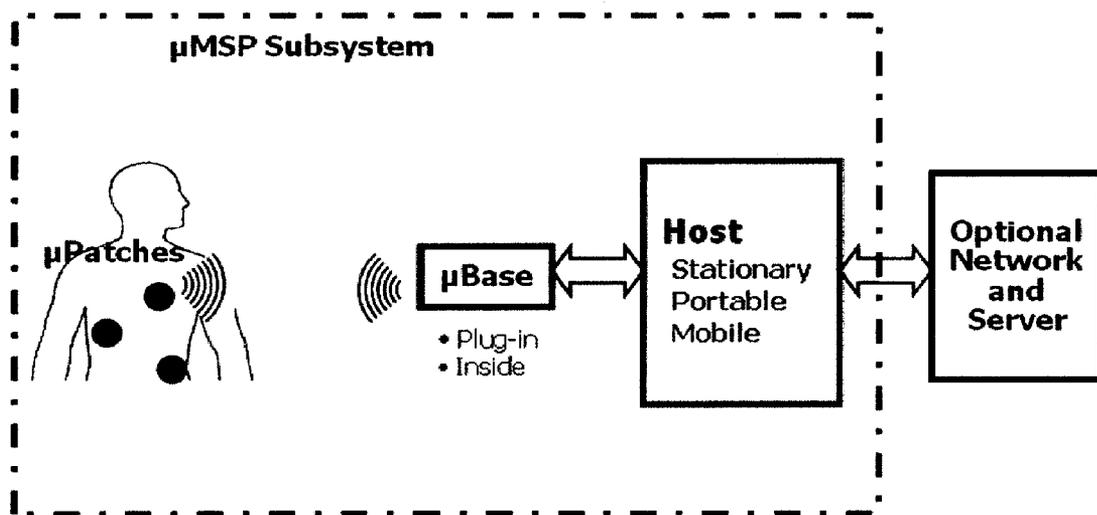


FIG. 1

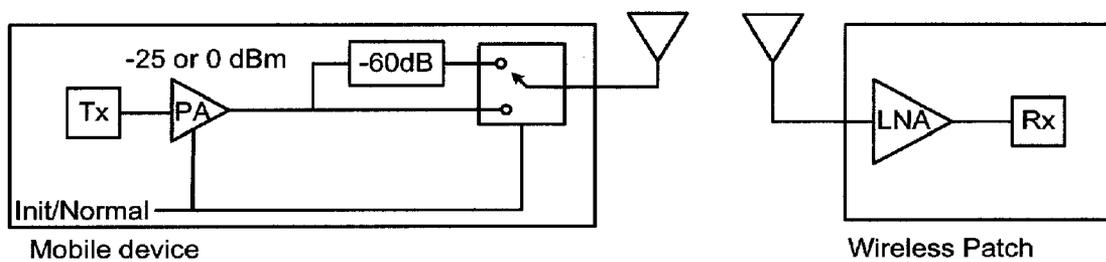


FIG. 2

**LOW POWER RADIOFREQUENCY (RF)
COMMUNICATION SYSTEMS FOR SECURE
WIRELESS PATCH INITIALIZATION AND
METHODS OF USE**

CROSS-REFERENCE

[0001] This application claims the benefit of U.S. Provisional Application No. 60/982,225, filed Oct. 24, 2007, which application is incorporated herein by reference in its entirety.

BACKGROUND OF THE INVENTION

[0002] Wireless healthcare systems are being increasingly used to help reduce healthcare cost, increase patient independence and provide better outcomes. A typical wireless healthcare system includes sensors, a host device or relay station, and a remote server. The sensors typically sense physiological signals from the body and wirelessly transmit them to a nearby host device or relay station. The host device receives the signals from the sensors and can then process and relay them to the remote server. The signal can be relayed using a cellular or other suitable type of network.

[0003] One critical aspect of remote monitoring of human physiological signals is to ensure that the privacy of the patient is maintained. Wireless transmission of these physiological signals needs to be protected against unauthorized detection of the signals. One method that can be used to ensure that patient information remains confidential includes encrypting data transmission with a 128-bit or better advanced encryption standard (AES) encryption scheme. Such a scheme involves sharing of private keys between the wireless patches and the host device prior to transmission. In order to accomplish this, sharing of private keys between the wireless patches and the host device prior to transmission can be done. This is feasible when the sensors and the host device could be purchased by patients at the same time, and also the host device could be reused with the same patch at different times. Another method is to ensure private key exchange by allowing the host device to program the keys into the sensors using near field communication so that nearby detectors cannot listen to the transmissions as the near field communication's range is only about 20 cm. Such a method can be used when it is practical to have an additional wireless method (magnetic field induction using 13.56 MHz bandwidth) that is different from the ones used by the wireless healthcare systems (radio frequency (RF) bands in the hundreds of MHz and in GHz) in the wireless patches and host device.

[0004] Therefore, a wireless healthcare system that is capable of eliminating detection of patient information by devices external to the system by operating at a low-power RF mode during the key-exchange period would be useful.

SUMMARY OF THE INVENTION

[0005] 1. Provided herein is a wireless healthcare system comprising at least one sensor and a base unit adaptable to be in communication with the sensor in a wireless healthcare system. The sensor can be adaptable to communicate with the base unit at a first power during formation of a communication link. In some embodiments, the sensor can be in wireless communication with the base unit. The sensor can be further adaptable to communicate with the base unit at a second power after the communication link has been formed between the base unit and the sensor. The sensor can be a patch. In some embodiments, the patch can be positioned on the sur-

face of a patient. The sensor can be adaptable to communicate with the base unit at a first power, where the first power is a low power mode. Additionally, the wireless healthcare system can comprise a sensor adaptable to sense, detect, measure, and/or monitor at least one physiological parameter from a patient. Furthermore, the wireless healthcare system can be in communication with a network server. In some embodiments, the wireless healthcare system can be in wireless communication with a network server. The wireless healthcare system can further comprise more than one sensor. The base unit can further comprise a power-amplifier. In some embodiments, the wireless healthcare system comprises a base unit wherein the base unit is adaptable to select a first power output level of -25 dBm (Decibel referenced to milliwatt) for the power amplifier and is further adaptable to attenuate the output signal by another 60 dB (Decibel). Furthermore, the base unit can further comprise an antenna. In some embodiments, the antenna can be adaptable to transmit power during the initialization phase from about -60 dBm to about -100 dBm. In some embodiments, the antenna can be adaptable to transmit power during the initialization phase of about -85 dBm. The sensor can also comprise a power-amplifier. The sensor can be adaptable to select a first power level output level of -25 dBm for the power amplifier and is further adaptable to attenuate the output signal by another 60 dB. The sensor can also comprise an antenna adaptable to transmit power during the initialization phase of about -85 dBm.

[0006] Further provided herein is a method for encrypting data sent between a base unit and at least one sensor of a wireless healthcare system comprising: bringing the at least one sensor of the wireless healthcare system proximate to the base unit of the wireless healthcare system when a communication link between base unit and the sensor is in low power mode; establishing an encrypted link between the sensor and the base unit; and increasing the power level to a higher power after the encrypted link has been formed between the sensor and the base unit. In some embodiments of the method, the wireless healthcare system comprises more than one sensor. The method can further comprise the step of establishing an encrypted link between the base and the more than one sensor. The method can further comprise transmitting patient information from the sensor to the base unit. The establishing step can further comprise selecting an initial low power level and attenuating the output level. In some embodiments of the method, the establishing step of the method can further comprise the steps of: (a) sending a beacon from the base unit to the at least one sensor to establish the communication link; (b) receiving the beacon with the at least one sensor; (c) sending a key continuously from the at least one sensor; (d) receiving the key with the base unit; (e) sending the key from the base unit to the at least one sensor; (f) receiving the key with the at least one sensor and notifying the base unit to encrypt the communication link; and (g) receiving the notification from the base unit and switching the base unit from the at least one sensor communication link to the encrypted link. The key can be selected from a phone number, retinal scan, finger print, or any other suitable biometric information, or combination thereof. The method provided herein can further comprise the step of transmitting patient information to a network server.

[0007] Further provided herein are kits for transmitting sensitive physiological data from a patient to a host device comprising at least one sensor adaptable to be positioned on a patient and a base unit in communication with the at least one sensor, wherein the sensor is adaptable to communicate

with the base unit at a first power during formation of a communication link and is further adaptable to communicate with the base unit at a second power after the communication link has been formed, and wherein the sensor and base unit are components of a wireless healthcare system. The kit can comprise more than one sensor.

INCORPORATION BY REFERENCE

[0008] All publications, patents, and patent applications mentioned in this specification are herein incorporated by reference to the same extent as if each individual publication, patent, or patent application was specifically and individually indicated to be incorporated by reference.

BRIEF DESCRIPTION OF THE DRAWINGS

[0009] The novel features of the invention are set forth with particularity in the appended claims. A better understanding of the features and advantages of the present invention will be obtained by reference to the following detailed description that sets forth illustrative embodiments, in which the principles of the invention are utilized, and the accompanying drawings of which:

[0010] FIG. 1 illustrates one embodiment of a wireless healthcare system; and

[0011] FIG. 2 illustrates the components of one embodiment of a low power-RF transmitter and one embodiment of a receiver.

DETAILED DESCRIPTION OF THE INVENTION

[0012] Provided herein is a wireless healthcare system comprising at least one sensor and a base unit adaptable to be in communication with the sensor in a wireless healthcare system. The sensor can be adaptable to communicate with the base unit at a first power during formation of a communication link. In some embodiments, the sensor can be in wireless communication with the base unit. The sensor can be further adaptable to communicate with the base unit at a second power after the communication link has been formed between the base unit and the sensor. The sensor can be a patch. In some embodiments, the patch can be positioned on the surface of a patient. The sensor can be a wearable garment wearable by the patient that can detect signals from the patient. The sensor can be adaptable to communicate with the base unit at a first power, where the first power is a low power mode. Additionally, the wireless healthcare system can comprise a sensor adaptable to sense, detect, measure, and/or monitor at least one physiological parameter from a patient. Furthermore, the wireless healthcare system can be in communication with a network server. In some embodiments, the wireless healthcare system can be in wireless communication with a network server. The wireless healthcare system can further comprise more than one sensor. The base unit can further comprise a power-amplifier. In some embodiments, the wireless healthcare system comprises a base unit wherein the base unit is adaptable to select a first power output level of -25 dBm for the power amplifier and is further adaptable to attenuate the output signal by another 60 dB. Furthermore, the base unit can further comprise an antenna. In some embodiments, the antenna can be adaptable to transmit power during the initialization phase from about -60 dBm to about -100 dBm. In some embodiments, the antenna can be adaptable to transmit power during the initialization phase of about -85 dBm. The sensor can also comprise a power-amplifier.

The sensor can be adaptable to select a first power level output level of -25 dBm for the power amplifier and is further adaptable to attenuate the output signal by another 60 dB. The sensor can also comprise an antenna adaptable to transmit power during the initialization phase of about -85 dBm.

I. Systems

[0013] Provided herein is a wireless healthcare system for use in transmitting patient information in a secure fashion using a wireless communication device. The device provided herein includes a sensor for transmitting a signal to a base unit using a key-exchange program to encrypt the signal, thereby preventing devices external to the system, but in range of the signal, from detecting the signal transmitted between the sensor and the base unit. For a wireless healthcare system to be used for private key exchange, the radio radiofrequency (RF) power of the base unit transmitter needs to be reduced close to the sensitivity of the wireless sensor receiver so that the transmitter and receiver could be brought close to each other and still maintain a wireless link. An additional external electrical device not part of the system but capable of detecting the electrical signal between the sensor and base unit, or eavesdropping, positioned one meter away from the system will only detect a signal significantly below the receiver sensitivity. For example purposes only, an external device near the system described herein will detect a signal with at least a 40 dB of free space loss, making reception by the external device nearly impossible.

[0014] In some embodiments, the initial placement of the patches on the human body is followed by a wireless initialization sequence at very low power by bringing the base unit and the sensor in proximity to each other. Normal data transmission of a signal from the sensors from the sensors to the base unit can then occur following the initialization at normal power-level and range of operation. This ability to bring the sensors and the base unit close to each other distinguishes the wireless healthcare system from a generic wireless network where bringing the sensor and the base unit in close proximity might not be possible. The ability to bring the sensor and base unit close together can simplify the complexity and operation of the system, and can reduce the cost of the system.

[0015] FIG. 1 illustrates one embodiment of a wireless healthcare system. The wireless healthcare system can comprise at least one sensor and a base unit. In some embodiments, multiple sensors are used. The sensor can be positioned on a patient as shown in FIG. 1. The sensor can be a wireless sensor. Alternatively, the sensor can be in the form of a patch. Alternatively, the sensor can be in the form of a wearable garment. The sensor can be a wired sensor, where the sensor is wired to a base unit. In some embodiments, the sensor can be a wireless sensor in wireless communication with the base unit. When the sensor is ready for use, the sensor can be powered up. During the power up processes, the sensor undergoes a boot-up process. During this time, an attempt can be made to form a connection between the sensor and the base unit. The sensor can wait to receive commands from the base unit to establish wireless link parameters to transmit data. In order to establish a wireless link, the sensor either listens in a predetermined "broadcast channel" or alternatively, the sensor can scan multiple channels where the host device may be transmitting beacons for the sensor. In some embodiments, the sensor itself could give an indication that the sensor is ready to be initialized. The patch or wearable item could also give an indication that the sensor is ready to be initialized. The

sensor can give an audio indication that the sensor is ready to be initialized. Alternatively, the sensor can give a visual indication that the sensor is ready to be initialized.

[0016] The base unit can be a component of a host system. Alternatively the base unit can be a stand alone unit in communication with the sensor. FIG. 2 illustrates one embodiment of a sensor and base unit. The sensor in FIG. 2 has a sensitivity of -90 dBm. A receiver signal strength of -85 dBm is assumed to result in virtually error-free data reception during the initialization process. Any suitable signal and sensitivity level that results in error-free operation can be used.

[0017] Once the sensor has given an indication that the sensor is ready to be initialized, the end-user can then start the initialization process by bringing the base unit close to the wireless sensor. Alternatively, the wireless sensor can be brought close to the base unit. The sensor can be positioned within about 15 cm of the base unit. Additionally, the sensor can be positioned within about 10 cm of the base unit. The sensor can be positioned within about 5 cm of the base unit. In some embodiments, the sensor can be positioned within about 2 cm of the base unit.

[0018] The initialization process can then be started by the end-user. The base unit can select a low initialization power level of -25 dBm for the internal/external power-amplifier (PA) to send commands to the wireless patch to be initiated. The base unit can then further attenuate the output signal by another 60 dB by switching to an RF path that includes a 60 dB attenuator. This results in a -85 dBm radiated power at the transmit antenna. In some embodiments, the power radiated from antenna can range between about -60 dBm and -100 dBm. The close proximity of the sensor to the base unit can allow the sensor to receive the signal from the base unit reliably. The sensor can also verify that the signal is received error-free. In some embodiments, the signal can be checked for alteration using a cyclic redundancy check (CRC) of the received data packet. The sensor can then compare the signal after the CRC to the signal at the beginning of the initialization sequence. If the CRC fails, the sensor can ignore the signal from the base unit. No connection between the base unit and the sensor is formed and the sensor stays in listening mode.

[0019] The system provided herein can be a static system that establishes a link between the base and the sensor at one distance using one lower power. In some embodiments, the system can comprise a system that can be adjusted. For example, in some cases a higher complexity eavesdropping receiver with extremely low sensitivity can be in proximity to the system wherein the eavesdropping receiver can detect and demodulate transmissions at power as low as -185 dBm. The system could then lower the power transmission level to a lower level. Additionally, the base unit can be brought into closer proximity to the sensor. Using an even lower power level but having the sensor and base unit in closer proximity can help to maintain a reliable wireless link between the base unit and sensor at such low power levels.

[0020] Provided herein is one embodiment of a key-exchange program for sending encrypted data in order to establish a connection between the sensor and the base unit. The key-exchange program can comprise the base unit continuously sending out a beacon to be detected by the sensor. The wireless sensor can receive the beacon from the base unit, thereby establishing a preliminary connection between the base unit and the sensor. The sensor can then send out a key (information or a parameter that determines the functional

output of a cryptic algorithm) continuously to the base unit. The base unit then receives the key from the sensor and then sends the key continuously back to the sensor. After receiving the key, the sensor sends continuous notification to the base unit that it is permissible to switch to the encrypted channel. The sensor then listens for a signal from the base unit on the encrypted channel. The base unit can then receive the switching message from the sensor and switches to the encrypted channel. In some embodiments, the wireless sensor can send acknowledgments or other capability parameter messages to the base unit using a similar low-power mode for transmission to the host device. Together, the host device and the wireless patch can exchange encryption key information at power levels not detectable by eavesdroppers or other external devices that are within range and are of similar setup.

[0021] After the key-exchange between the sensor and the base unit is complete, the sensor and base unit can communicate reliably with each other to establish and complete the initialization process. Any signal received by an eavesdropping device at this point suffers an additional 40 dB free-space path-loss (-135 dBm) or more, even at one meter distances from the base unit. This reduction in free-space path-loss can make it virtually impossible for an eavesdropping device to detect and demodulate the transmission signal between the sensor and the base-unit. Any similar signal attenuation mechanism can be used to achieve low-power transmissions. For example purposes only, different combinations of power amplified power and one or more attenuator stages could be used to achieve the desired power level. The initialization sequence can also be modified to follow near field communication (NFC) Forum's technical specifications. In some embodiments, an NFC transceiver can be employed in addition to a radiofrequency (RF) transceiver which would use the same RF antenna. In this case, the RF antenna tuned for RF frequencies can provide the adequate attenuation at the NFC frequency providing the desired privacy.

[0022] Additionally, any subsequent (periodic) key exchange for enhanced privacy does not need to involve low-power transmissions, as they can use the existing keys to encrypt the transmitted data containing the new keys. The key can also be the unique identification of the end-user including, but not limited to, the end user's mobile phone number, or any suitable biometric information such as finger-print, or retinal scan.

[0023] In some embodiments, multiple sensors can be used. The same authentication key can be used by the base unit in conjunction with multiple sensors that are in close proximity to each other. By issuing a single command on the host device, the end user needs to initiate the authentication process once. The base unit can then go through the above procedure with each wireless patch to authenticate all of the remaining sensors. This eliminates the need to authenticate all the sensors separately.

[0024] Once the initialization is completed successfully, subsequent transmissions between the base unit and the sensor can be encrypted. The transmit power levels are restored to normal levels by switching to higher power-levels of the power-amplifier, as well as bypassing the RF path with the 60 dB attenuation.

[0025] In some embodiments, the system can be adaptable to upload information from the base unit onto a network

server. The base unit can be hard-wired to the network server. Alternatively the base unit can be wirelessly connected to the network server.

II. Methods

[0026] Further provided herein is a method for encrypting data sent between a base unit and at least one sensor of a wireless healthcare system comprising: bringing the at least one sensor of the wireless healthcare system proximate to the base unit of the wireless healthcare system when a communication link between base unit and the sensor is in low power mode; establishing an encrypted link between the sensor and the base unit; and increasing the power level to a higher power after the encrypted link has been formed between the sensor and the base unit. In some embodiments of the method, the wireless healthcare system comprises more than one sensor. The method can further comprise the step of establishing an encrypted link between the base and the more than sensor. The method can further comprise transmitting patient information from the sensor to the base unit. The establishing step can further comprise selecting an initial low power level and attenuating the output level. In some embodiments of the method, the establishing step of the method can further comprise the steps of: (a) sending a beacon from the base unit to the at least one sensor to establish the communication link; (b) receiving the beacon with the at least one sensor; (c) sending a key continuously from the at least one sensor; (d) receiving the key with the base unit; (e) sending the key from the base unit to the at least one sensor; (f) receiving the key with the at least one sensor and notifying the base unit to encrypt the communication link; and (g) receiving the notification from the base unit and switching the base unit from the at least one sensor communication link to the encrypted link. The key can be selected from a phone number, retinal scan, finger print, or any other suitable biometric information, or combination thereof. The method provided herein can further comprise the step of transmitting patient information to a network server.

III. Kits

[0027] Further provided herein are kits for transmitting sensitive physiological data from a patient to a host device comprising: at least one sensor adaptable to be positioned on a patient; and a base unit in communication with the at least one sensor, wherein the sensor is adaptable to communicate with the base unit at a first power during formation of a communication link and is further adaptable to communicate with the base unit at a second power after the communication link has been formed, and wherein the sensor and base unit are components of a wireless healthcare system. The kit can comprise more than one sensor.

[0028] While preferred embodiments of the present invention have been shown and described herein, it will be obvious to those skilled in the art that such embodiments are provided by way of example only. Numerous variations, changes, and substitutions will now occur to those skilled in the art without departing from the invention. It should be understood that various alternatives to the embodiments of the invention described herein may be employed in practicing the invention. It is intended that the following claims define the scope of the invention and that methods and structures within the scope of these claims and their equivalents be covered thereby.

What is claimed is:

1. A wireless healthcare system comprising:
 - at least one sensor; and
 - a base unit adaptable to be in communication with the sensor,
 wherein the sensor is adaptable to communicate with the base unit at a first power during formation of a communication link and is further adaptable to communicate with the base unit at a second power after the communication link has been formed, and wherein the sensor and base unit are components of a wireless healthcare system.
2. The wireless healthcare system of claim 1 wherein the sensor is a patch adaptable to be positioned on the surface of a patient.
3. The wireless healthcare system of claim 1 wherein the first power is a low power mode.
4. The wireless healthcare system of claim 1 wherein the sensor is adaptable to detect at least one physiological parameter from a patient.
5. The wireless healthcare system of claim 1 wherein the base unit is further adaptable to be in external communication with a network server.
6. The wireless healthcare system of claim 1 wherein the base unit is adaptable to be in wireless communication with the sensor.
7. The wireless healthcare system of claim 1 further comprising more than one sensor.
8. The wireless healthcare system of claim 1 wherein the base unit further comprises a power-amplifier.
9. The wireless healthcare system of claim 1 wherein the base unit is adaptable to select a first power level output level of -25 dBm for the power amplifier and is further adaptable to attenuate the output signal by another 60 dB.
10. The wireless healthcare system of claim 1 wherein the base unit further comprises an antenna.
11. The wireless healthcare system of claim 10 wherein the antenna is adaptable to transmit power during the initialization phase of about -85 dBm.
12. The wireless healthcare system of claim 1 wherein the sensor further comprises a power-amplifier.
13. The wireless healthcare system of claim 1 wherein the sensor is adaptable to select a first power level output level of -25 dBm for the power amplifier and is further adaptable to attenuate the output signal by another 60 dB.
14. The wireless healthcare system of claim 1 wherein the sensor further comprises an antenna.
15. The wireless healthcare system of claim 14 wherein the antenna is adaptable to transmit power during the initialization phase of about -85 dBm.
16. A method for encrypting data sent between a base unit and at least one sensor of a wireless healthcare system comprising:
 - (a) bringing the at least one sensor of the wireless healthcare system proximate to the base unit of the wireless healthcare system when the communication link is in lower power mode;
 - (b) establishing an encrypted link between the sensor and the base unit; and
 - (c) increasing the power level to a higher power after the link has been formed between the sensor and base unit.
17. The method of claim 16 wherein the healthcare systems further comprises more than one sensor.

18. The method of claim **16** further comprising the step of establishing an encrypted link between the base and the more than one sensor.

19. The method of claim **16** further comprising the step of transmitting patient information from the sensor to the base unit.

20. The method of claim **16** wherein the establishing step comprises selecting an initial low power level and attenuating the output level.

21. The method of claim **16** wherein the establishing step further comprises the steps of:

- (a) sending a beacon from the base unit to the at least one sensor to establish a communication channel;
- (b) receiving the beacon with the at least one sensor;
- (c) sending a key continuously from the at least one sensor;
- (d) receiving the key with the base unit;
- (e) sending the key from the base unit to the at least one sensor;
- (f) receiving the key with the at least one sensor and notifying the base unit to encrypt the communication channel; and
- (g) receiving the notification from the base unit and switching the base unit to the at least one sensor communication link to the encrypted link.

22. The method of claim **21** wherein the key is selected from at least one of a phone number, retinal scan, fingerprint, or biometric information.

23. The method of claim **21** further comprising the step of transmitting patient information to a network server.

24. A kit for transmitting sensitive physiological data from a patient to a host device comprising:

- (h) at least one sensor adaptable to be positioned on a patient; and
- (i) a base unit in communication with the at least one sensor,

wherein the sensor is adaptable to communicate with the base unit at a first power during formation of a communication link and is further adaptable to communicate with the base unit at a second power after the communication link has been formed, and wherein the sensor and base unit are components of a wireless healthcare system.

25. The kit of claim **24** further comprising more than one sensor.

* * * * *