

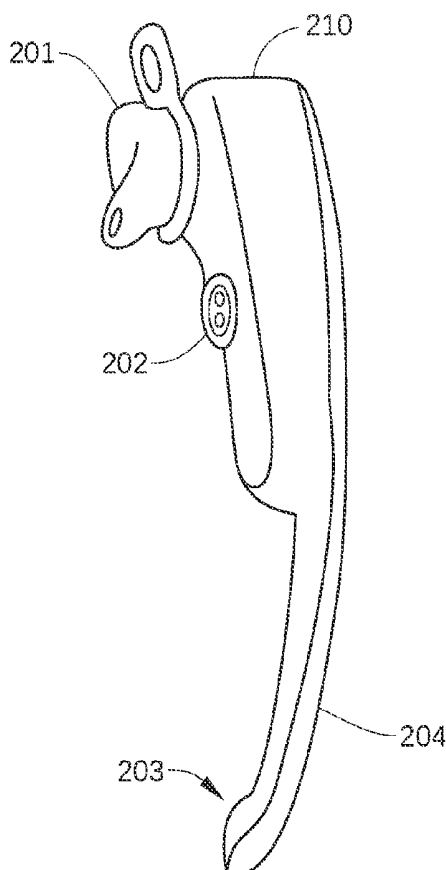


US 20170118204A1

(19) **United States**(12) **Patent Application Publication**
LAINE et al.(10) **Pub. No.: US 2017/0118204 A1**(43) **Pub. Date: Apr. 27, 2017**(54) **TECHNIQUES FOR HEARABLE
AUTHENTICATION****H04W 12/06** (2006.01)**A61B 7/04** (2006.01)(71) Applicant: **HARMAN INTERNATIONAL
INDUSTRIES, INC.**, Stamford, CT
(US)(52) **U.S. Cl.**CPC **H04L 63/0861** (2013.01); **H04W 12/06**
(2013.01); **H04L 63/10** (2013.01); **A61B**
5/04845 (2013.01); **A61B 7/04** (2013.01);
A61B 5/01 (2013.01); **A61B 5/0205** (2013.01);
A61B 5/6817 (2013.01); **A61B 5/117**
(2013.01); **A61B 5/053** (2013.01)(72) Inventors: **Heikki LAINE**, Pittstown, NJ (US);
Donald Joseph BUTTS, Westport, CT
(US)(21) Appl. No.: **14/919,555**(22) Filed: **Oct. 21, 2015****Publication Classification**(51) **Int. Cl.****H04L 29/06** (2006.01)**A61B 5/0484** (2006.01)**A61B 5/117** (2006.01)**A61B 5/01** (2006.01)**A61B 5/0205** (2006.01)**A61B 5/00** (2006.01)(57) **ABSTRACT**

The various embodiments set forth an apparatus comprising an earpiece, a sensor configured to measure an inherent attribute associated with a user, a wireless transceiver configured to communicate with a wireless access point of a wireless communication network, and a controller. The controller is configured to establish authenticated access to the wireless communication network based on the inherent attribute associated with the user. An advantage of the disclosed embodiment is that a hearable device can conveniently authenticate user access to a network with enhanced security, based on one or more inheritance factors that are measured by the hearable device.

92



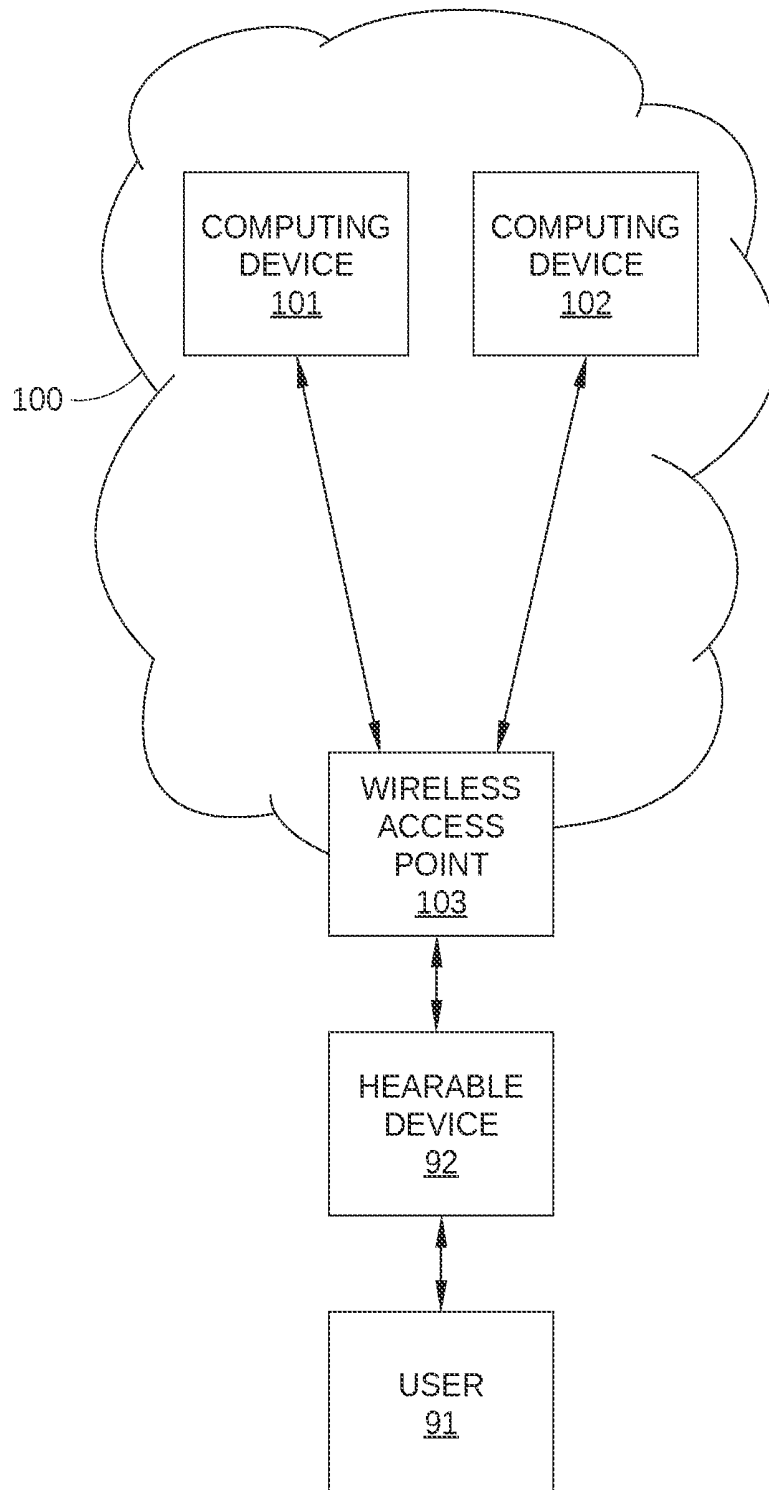


FIG. 1

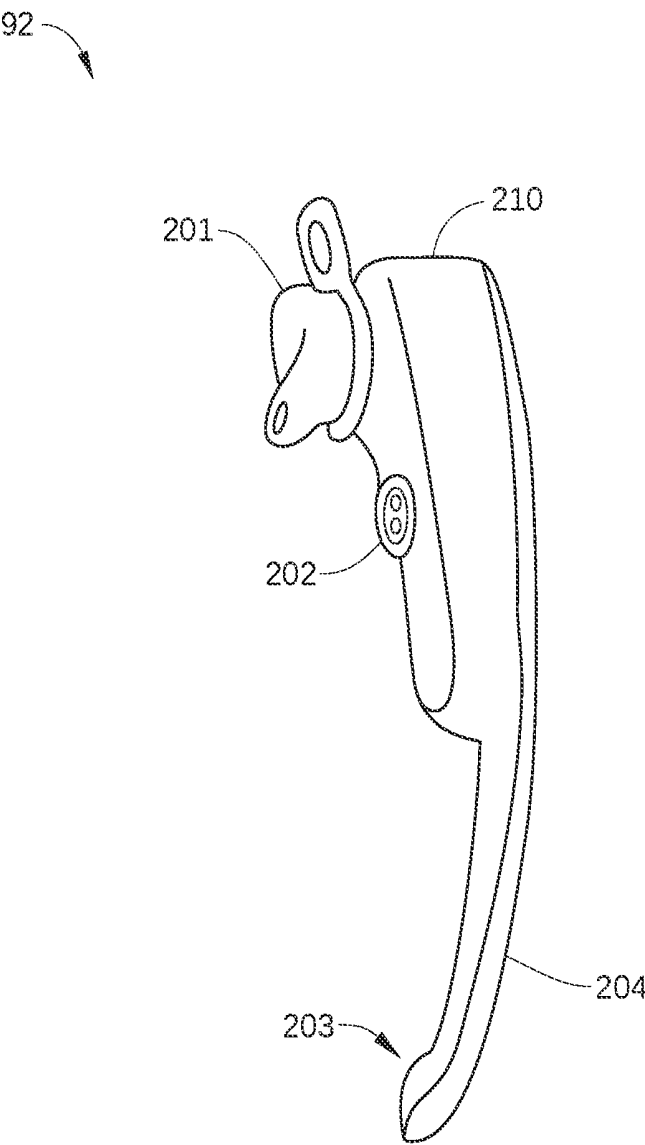


FIG. 2A

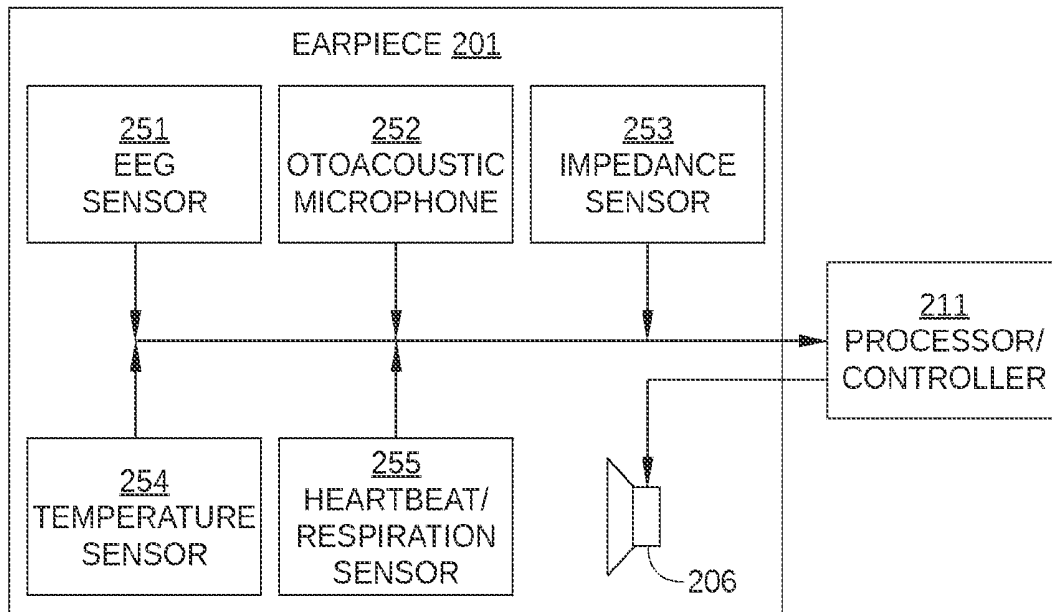


FIG. 2B

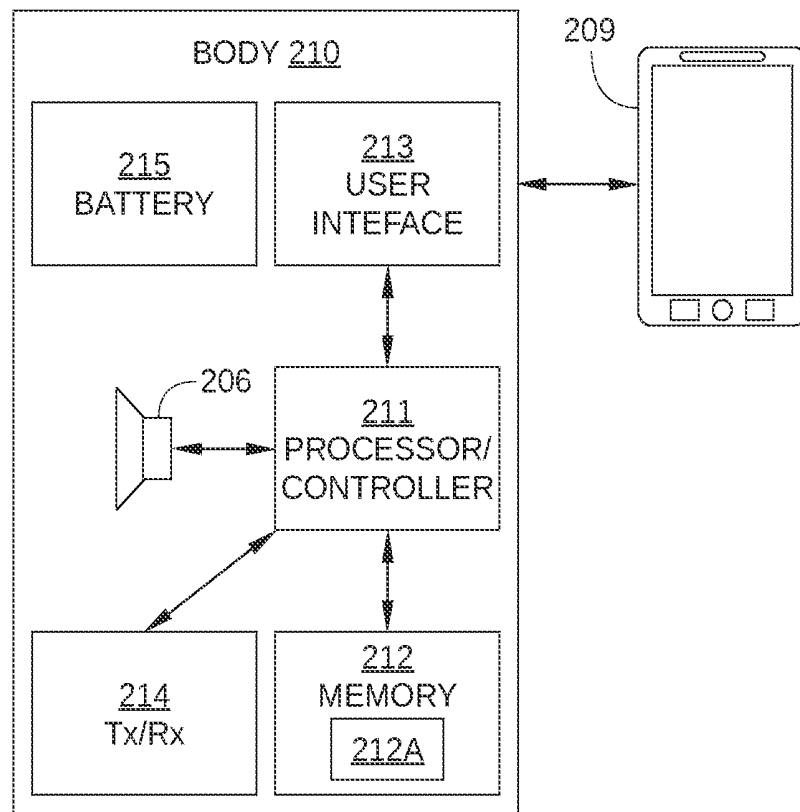


FIG. 2C

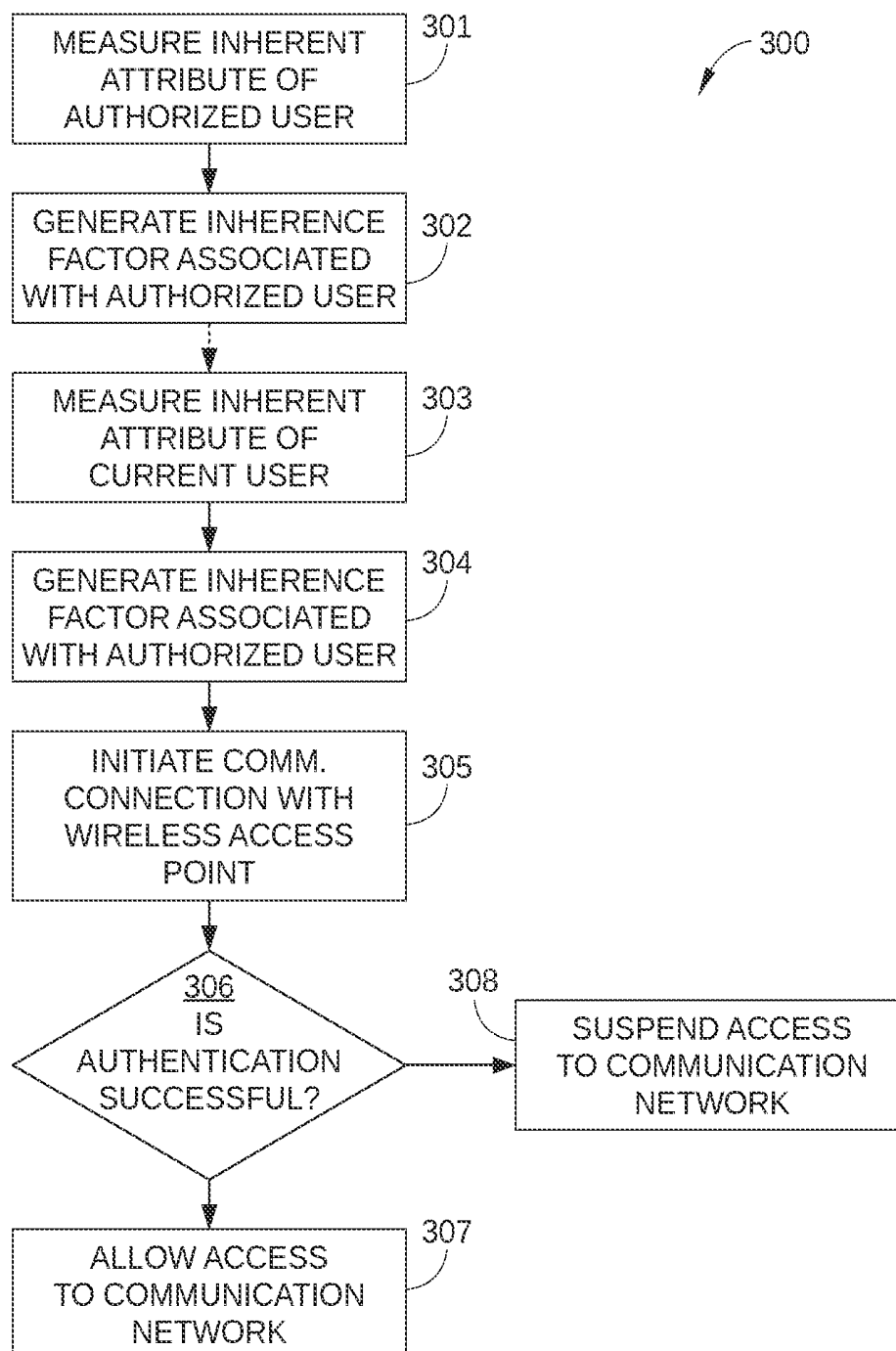


FIG. 3

TECHNIQUES FOR HEARABLE AUTHENTICATION

BACKGROUND

[0001] Field of the Various Embodiments

[0002] The various embodiments relate generally to hearable electronic devices and, more specifically, to techniques for hearable authentication.

[0003] Description of the Related Art

[0004] It has become common practice for individual consumers to use telecommunications systems for conducting financial transactions, consumer-based transactions, and other types of transactions involving the use of sensitive information. For example, wireless communication devices, either alone or in conjunction with the Internet, are frequently used for point-of-sale (POS) and on-line transactions, such as banking, retail, and other similar transactions, where credit card information, debit card information, and/or other types of account information is transmitted between or among devices. In addition, wireless communication devices, more generally, are increasingly employed for accessing various networks, other wireless devices, and the like, as part of more routine day-to-day activities. However, such devices, and the access codes associated with such devices, are routinely exposed to potentially malicious or otherwise unauthorized users, which can compromise the security of any network accessible by these devices. Such malicious and unauthorized users are becoming more and more aggressive in trying to exploit any weaknesses in the security of networked devices or the networks associated with those devices. Consequently, developing robust security and authentication procedures for wireless communication devices has become all the more important.

[0005] As an example, smart phones with two-factor authentication can be compromised quite easily. First, when a user authorizes access to a wireless network by entering a personal identification number (PIN) via a smartphone, the PIN may be intercepted electronically, or simply procured by someone watching and memorizing the PIN during PIN entry. Either way, the knowledge authentication factor associated with the smartphone (i.e., the PIN), can be readily obtained by a malicious user. Similarly, the possession authentication factor associated with the smartphone (i.e., physical control of the smartphone) can be obtained by a malicious user by simply stealing or gaining temporary electronic access to the smartphone.

[0006] In sum, the convenience afforded by using a wireless communication device to perform secure transactions and to access networks and other devices can be easily outweighed by the added security risks associated with using wireless communication device for these purposes. Accordingly, what would be useful are techniques for more securely accessing networks via wireless communication devices.

SUMMARY

[0007] The various embodiments set forth an apparatus comprising an earpiece, a sensor configured to measure an inherent attribute associated with a user, a wireless transceiver configured to communicate with a wireless access point of a wireless communication network, and a controller. The controller is configured to establish authenticated access to the wireless communication network based on the inherent attribute associated with the user.

[0008] At least one advantage of the disclosed embodiments is that a hearable device can conveniently authenticate user access to a network with enhanced security, based on one or more inference factors that are measured by the hearable device.

BRIEF DESCRIPTION OF THE SEVERAL VIEWS OF THE DRAWINGS

[0009] So that the manner in which the above recited features of the various embodiments can be understood in detail, a more particular description of the various embodiments, briefly summarized above, may be had by reference to embodiments, some of which are illustrated in the appended drawings. It is to be noted, however, that the appended drawings illustrate only typical embodiments and are therefore not to be considered limiting of its scope, for the various embodiments may admit to other equally effective embodiments.

[0010] FIG. 1 is a schematic diagram illustrating a wireless communication network configured to implement one or more aspects of the various embodiments;

[0011] FIG. 2A is a schematic diagram of the hearable device of FIG. 1, according to the various embodiments;

[0012] FIG. 2B is a more detailed block diagram of the earpiece of FIG. 2A, according to the various embodiments;

[0013] FIG. 2C is a more detailed block diagram of the body of FIG. 2A, according to the various embodiments; and

[0014] FIG. 3 sets forth a flowchart of method steps for securely accessing a wireless network, according to the various embodiments.

[0015] For clarity, identical reference numbers have been used, where applicable, to designate identical elements that are common between figures. It is contemplated that features of one embodiment may be incorporated in other embodiments without further recitation.

DETAILED DESCRIPTION

[0016] FIG. 1 is a schematic diagram illustrating a wireless communication network 100, configured to implement one or more aspects of the various embodiments. Also shown in FIG. 1 is a user 91 and a hearable device 92 configured to authenticate access to wireless communication network 100 by user 91. Wireless communication network 100 may include, without limitation, computing devices 101 and 102 and a wireless access point 103. Wireless communication network 100 may be any technically feasible type of communications network that allows data to be exchanged between computing device 101, computing device 102, and other entities or devices, such as a web server or another networked computing device. For example, wireless communication network 100 may include a wide area network (WAN), a local area network (LAN), a wireless (WiFi) network, and/or the Internet, among others. In some embodiments, wireless communication network 100 may include multiple network entry points, but for clarity, only a single wireless access point 103 is depicted in FIG. 1.

[0017] Each of computing devices 101 and 102 may be any stand-alone computing device operable to communicate via wireless communication network 100, including, without limitation, a desktop computer, a laptop computer, a smart phone, a personal digital assistant (PDA), a tablet computer, an automated teller machine or point-of-sale device configured with smartphone authentication, and the

like. Alternatively or additionally, one or more of computing devices **101** and **102** may be a computing device operable to communicate via wireless communication network **100** and incorporated into an electronic device, consumer product, vehicle, or other apparatus, including, without limitation, a video game console, a set top console, a digital video recorder, a digital video disk player, a vehicle information system for a particular vehicle, and the like.

[0018] Wireless access point **103** is configured to authenticate access requests and provide authenticated access to wireless communication network **100**. In some embodiments, wireless access point **103** may be a software interface associated with a specific computing device within wireless communication network **100**, such as computing device **101** or **102**. Alternatively, wireless access point **103** may be an interface associated with a stand-alone computing device within wireless communication network **100**, such as a gateway computer or the like. Thus, when user **91** attempts to access a particular computing device within wireless communication network **100** via hearable device **92**, wireless access point **103** may operate as part of the particular computing device, or may be a separate entity that authorizes user access to the particular computer device. In operation, wireless access point **103** may serve as an authorization entity for access to wireless communication network **100**, receiving and authorizing requests to access computing device **101** and/or computing device **102**, for example from hearable device **92**.

[0019] Hearable device **92** may be any wearable electronic device that includes an earpiece or other audio interface configured for insertion in the ear canal of a user. For example, hearable device **92** may include an earpiece or audio earbud that is Bluetooth®-capable. In such embodiments, the earpiece or audio earbud may be configured to wirelessly communicate with an external computing device, such as a smartwatch, a smartphone, an electronic table, and the like. The external computing device may provide more processing power, greater memory, and/or a more ergonomic user interface than may be practicable in an earpiece or earbud form-factor. Alternatively or additionally, the earpiece or earbud may be configured with a wired connection to the external computing device. One embodiment of hearable device **92** is illustrated in FIGS. 2A-2C.

[0020] FIG. 2A is a schematic diagram of hearable device **92**, configured according to the various embodiments. Hearable device **92** may include, without limitation, an earpiece **201**, a connection terminal **202**, and a microphone **203** that is disposed on an end of a mic boom **204**, all coupled to a body **210**. FIG. 2B is a more detailed block diagram of earpiece **201**, configured according to the various embodiments, and FIG. 2C is a more detailed block diagram of body **210**, configured according to the various embodiments.

[0021] As shown in FIGS. 2A and 2B, earpiece **201** is an earpiece configured for insertion at least partially in the ear canal of a user. In some embodiments, earpiece **201** is a custom-fit earpiece specifically designed to conform to at least a portion of the ear canal of the particular user, thereby substantially isolating the ear canal of the user acoustically from the surroundings. For example, earpiece **201** may be formed based on a laser scan, digital image or other three-dimensional scan, or physical mold of the ear canal of the particular user. Consequently, a suitable contact patch is generally formed between earpiece **201** and the ear canal of a user when hearable device **92** is worn by the particular user

for whom earpiece **201** is constructed. Earpiece **201** may include, without limitation, one or more of an electroencephalogram (EEG) sensor **251**, an otoacoustic microphone **252**, an impedance sensor **253**, a temperature sensor **254**, and a heartbeat/respiration sensor **255**, all of which are coupled to a processor **211** (described below in conjunction with FIG. 2C). In some embodiments, a loudspeaker **206** may also be included in earpiece **201**, whereas in other embodiments, loudspeaker **206** may be disposed in body **210** of hearable device **92**.

[0022] EEG sensor **251** may include any technically feasible sensor or sensors operable to non-invasively detect electrical activity of a user's brain, particularly in response to an acoustic trigger generated by loudspeaker **206**. For example, in some embodiments, EEG sensor **251** may include one or more electrodes disposed on a surface of earpiece **201** and configured to contact one or more surfaces of the ear canal of a specific user when hearable device **92** is worn by the particular user for whom earpiece **201** is constructed. Such electrodes may be configured to measure voltage fluctuations resulting from ionic current within the neurons of the user's brain in response to the acoustic trigger generated by loudspeaker **206**. Because the spontaneous electrical activity (i.e. neural oscillations) are unique to an individual, the signals detected by EEG sensor **251** may be considered a biometric signature, similar to a fingerprint. Consequently, in some embodiments, such detected signals may be employed as an inference factor for secure authentication, i.e., an inherent attribute of a user, such as something unique that a user is or does. The EEG signature associated with the authorized user may be stored locally in hearable device **92**, for example in a one-time programmable memory **212A** (described below in conjunction with FIG. 2C), and/or in wireless communication network **100**, for example in wireless access point **103**.

[0023] Otoacoustic microphone **252** may include any technically feasible sensor or sensors operable to reliably detect otoacoustic emission (OAE) from the ear of the user, particularly in response to an acoustic trigger generated by loudspeaker **206**. OAE is a sound that is emitted from within the inner ear, and evoked OAEs (EOAEs) are sounds emitted from within the inner ear when sound waves are incident on the ear. In some embodiments, otoacoustic microphone **252** is configured to detect EOAEs that are stimulated by an acoustic trigger, typically generated by loudspeaker **206**. The outer hair cells of the inner ear function as actuators that add energy to incoming sound waves, for example the sound waves associated with the acoustic trigger generated by loudspeaker **206**. Recent studies have validated that EOAEs may be used as a biometric signature, since EOAEs are unique for every person. Thus, in some embodiments, such detected signals may be employed as an inference factor for secure authentication. The otoacoustic signature associated with the authorized user may be stored locally in hearable device **92**, for example in one-time programmable memory **212A**, and/or in wireless communication network **100**, for example in wireless access point **103**.

[0024] Impedance sensor **253** may include any technically feasible sensor or sensors operable to reliably measure a "contact impedance," i.e., the electrical impedance of a contact patch between earpiece **201** and one or more surfaces of the ear canal of user **91**. Because contact impedance is highly dependent on the fit of earpiece **201** with the ear canal in which earpiece **201** is fitted, contact impedance

detected by impedance sensor 253 may be employed as an inference factor associated with the current user. Specifically, contact impedance exceeding a specific threshold indicates that earpiece 201 is either inserted incorrectly in the ear canal of the user for whom earpiece 201 is constructed, or is inserted in the ear canal of an unauthorized user, i.e., any user that is not the user for whom earpiece 201 is constructed. Thus, in some embodiments, the inability of a user to position earpiece 201 in such a way that contact impedance associated with earpiece 201 is less than a threshold value indicates that an unauthorized user is attempting to use hearable device 92. Consequently, in some embodiments, contact impedance, as measured by impedance sensor 253, may be employed as an inference factor for secure authentication. In some embodiments, contact impedance may be employed by hearable device 92 to indicate that the authorized user of hearable device 92 has not properly seated earpiece 201 in the ear canal, and/or that earpiece 201 has been removed by a user. The contact impedance associated with the authorized user may be stored locally in hearable device 92, for example in one-time programmable memory 212A, and/or in wireless communication network 100, for example in wireless access point 103.

[0025] Temperature sensor 254 may include any technically feasible sensor or sensors operable to measure a body temperature of user 91, such as a thermistor or a thermocouple. The body temperature measured in the ear canal of a user by temperature sensor 254 may, in some embodiments, be employed to confirm that a user is wearing hearable device 92. Thus, in some embodiments, the current body temperature may be used as an inference security factor for authentication of the user of hearable device 92. For example, when a user attempts to access wireless communication network 100 in FIG. 1, authentication of the identity of the user may depend in part on the current body temperature measured by temperature sensor 254 to confirm that earpiece 201 has not been removed by a user.

[0026] Heartbeat/respiration sensor 255 may include any technically feasible sensor or sensors operable to monitor heartbeat and/or respiration rate of a user 91. In some embodiments, heartbeat/respiration sensor 255 may use audio input from otoacoustic microphone 252, whereas in other embodiments, heartbeat/respiration sensor 255 may include a dedicated microphone. Because heartbeat and respiration of each person is substantially unique, a heartbeat measured in the ear canal of a user by heartbeat/respiration sensor 254 may, in some embodiments, be employed to confirm that the user wearing hearable device 92 is the authorized user of hearable device 92. Thus, in some embodiments, a heartbeat signature may be used as an inference security factor for authentication of the user of hearable device 92. For example, when a user attempts to access wireless communication network 100 in FIG. 1, authentication of the identity of the user may depend in part on whether the heartbeat signature measured by heartbeat/respiration sensor 255 matches a heartbeat signature associated with the authorized user of hearable device 92. The heartbeat signature associated with the authorized user may be stored locally in hearable device 92, for example in one-time programmable memory 212A, and/or in wireless communication network 100, for example in wireless access point 103. In some embodiments, the absence of heartbeat or respiration may be employed by hearable device 92 to indicate that earpiece 201 has been removed by a user.

[0027] Connection terminal 202, shown in FIG. 2A, may be disposed on a side surface of body 210, and may include one or more connector plugs for charging hearable device 92 and/or for inputting external information to hearable device 92 via a wired connection (not shown). Microphone 203 may be disposed on an end of mic boom 204, and is configured for voice communication. Body 210, which is shown in FIGS. 2A and 2C, may house, without limitation, processor 211, a memory 212, a user interface 213, a transceiver (Tx/Rx) 214, and a battery 215. In some embodiments, loudspeaker 206 may also be disposed in body 210.

[0028] Processor 211 may be any suitable processor implemented as a central processing unit (CPU), an application-specific integrated circuit (ASIC), a field programmable gate array (FPGA), any other type of processing unit, or a combination of different processing units. In general, processor 211 may be any technically feasible hardware unit capable of processing data and/or executing software applications to facilitate operation of hearable device 92 as described herein. Thus, in some embodiments, processor 211 may be configured as a controller for hearable device 92.

[0029] Memory 212 may include volatile memory, such as a random access memory (RAM) module, and non-volatile memory, such as a flash memory unit, a read-only memory (ROM), or any other type of memory unit or combination thereof suitable for use in hearable device 92. Memory 212 is configured to store any software programs, operating system, drivers, and the like, that facilitate operation of hearable device 92. In some embodiments, memory 212 includes a one-time programmable memory 212A, configured to store one or more inference factors associated with the authorized user of hearable device 92. In such embodiments, only a single authorized user is typically associated with hearable device 92. However, in some embodiments, one-time programmable memory 212A may be configured to store one or more inference factors associated with multiple authorized users of hearable device 92.

[0030] User interface 213 is configured to enable user inputs to hearable device 92, such as powering hearable device on and off, initiating and ending calls, changing volume, and the like. Thus, user interface 213 may include, without limitation, one or more mechanical (rocker, up-down, toggle) buttons or touch sensors disposed on an outer surface of housing 210. In some embodiments, user interface 213 may also be configured to communication with one or more display elements or devices. In some embodiments, such display elements or devices may be associated with an external computing device 209, such as an electronic tablet or smartphone operable to communicate with hearable device 92 and display content associated with operation of hearable device 92. For example, as part of a user authentication process, user interface 213 may be configured to facilitate the entry of a PIN via an application running on such an external computing device 209.

[0031] Transceiver 214 may be any technically feasible apparatus configured to provide a wireless communications link between hearable device 92 and network wireless access point 103. For example, but without limitation, wireless transceiver 130 may be a Bluetooth® access point. Alternatively or additionally, wireless transceiver 130 may be configured with cellular communication capability, satellite telephone communication capability, a wireless wide area network communication capability, or other types of

communication capabilities that allow for communication with wireless communication network 100 and computing devices 101 and 102.

[0032] Battery 215 may be any suitable energy storage battery suitable for use in hearable device 92, is configured to provide power to hearable device 92 during operation, and is typically a rechargeable battery.

[0033] According to embodiments described herein, hearable device 92 is configured to enable a user to securely access a computing device within wireless communication network 100. Specifically, hearable device 92 enables such secure access by incorporating an inheritance factor associated with the user into the authentication process. Hearable device 92 may employ the inheritance factor either alone or in conjunction with one or more other authorization factors, such as a knowledge factor (e.g., knowledge of a PIN or password) and/or a possession factor (e.g., possession of a physical fob, key, and/or hearable device 92 itself). Suitable inheritance factors employed by hearable device 92 may include, without limitation, an EEG reading or signature measured by EEG sensor 251 or an otoacoustic signature measured by otoacoustic microphone 252. In addition to or in lieu of these biometric signatures, hearable device 92 may employ one or more other inheritance factors as an inheritance factor during an authentication process, such as earpiece fit, measured by impedance sensor 253, body temperature, measured by temperature sensor 254, or a heart beat signature, measured by heartbeat/respiration sensor 255. Any other suitable inheritance factors not directly measured by a sensor in hearable device 92, such as fingerprint or retina imagery, may also be included in such an authentication process.

[0034] Thus, when the user of hearable device 92 enters the wireless signal range of wireless communication network 100, hearable device 92 and wireless access point 103 establish a secure connection based on at least one inheritance factor associated with the user of hearable device 92 and measured by hearable device 92. In this way, a secure connection is established between hearable device 92 and wireless communication network 100 without the need for manual entry of a PIN or possession of a security fob by the user of hearable device 92. Instead, the secure connection may be established transparently. For example, in embodiments in which wireless communication network 100 is associated with a vehicle or a home network, a physical key is not needed for entry to the vehicle or home. This is because hearable device 92 determines the identity of a user by measuring one or more of the inheritance factors described above, and either provides the one or more inheritance factors to the network as part of an authentication process or simply notifies the network that the user wearing hearable device 92 is an authenticated user.

[0035] For example, in some embodiments, wireless communication network 100 may be as simple as a single computing device, such as computing device 101, and a single network entry point, such as wireless access point 103. In such an embodiment, computing device 101 may be associated with a vehicular infotainment system, a home network and entertainment system, or an individual apparatus, such as an electronic tablet, DVD player, and the like. Thus, when the user of hearable device 92 enters the wireless signal range of wireless communication network 100 (for example, the user approaches the vehicle associated with wireless communication network 100), wireless access

point 103 may query hearable device 92 whether user 91 is an authenticated user. Alternatively, wireless access point 103 may query hearable device directly for one or more specific inheritance factors to authenticate user 91. As noted, each such inheritance factor is based on an inherent attribute of the user of hearable device 92 that hearable device 92 is configured to detect, i.e., an EEG signature, an otoacoustic signature, earpiece fit/impedance, heart beat signature, and the like. Hearable device 92 then measures the appropriate inherent attribute of the user, provides the inheritance factor based thereon to wireless access point 103, and receives access to wireless communication network 100 when the inheritance factor provided is determined to be correct, thereby completing the authentication process.

[0036] In some embodiments, when hearable device 92 (and by extension user 91) receives access to wireless communication network 100, user 91 may then access communication network as a typical network user, and access the Internet, transfer data to and/or from computing devices 101 and/or 102, etc. Alternatively or additionally, in other embodiments, when hearable device 92 and user 91 receive access to wireless communication network 100, one or more automated processes may occur. For example, when computing device 101 is associated with a vehicle, computing device 101 may automatically initiate one or more vehicle-specific actions, such as unlocking and/or starting the vehicle, powering up an infotainment system associated with the vehicle, and downloading and/or implementing personalized settings for vehicle systems associated with user 91 (e.g., radio settings, mirror positions, seat adjustments, audio system settings, environmental control settings, etc.). In some embodiments, the personalized settings may be downloaded from cloud storage or from hearable device 92, via wireless communication network 100. Alternatively or additionally, such personalized settings may be stored in computing device 101. In another example, when computing device 101 is associated with a home network and entertainment system, computing device 101 may automatically initiate one or more home network-specific actions, such as deactivating a home security system, powering specific lights on or off, modifying heating and cooling setpoints, and the like.

[0037] FIG. 3 sets forth a flowchart of method steps for securely accessing a wireless network, according to the various embodiments. Although the method steps are described with respect to the systems of FIGS. 1-2C, persons skilled in the art will understand that any system configured to perform the method steps, in any order, falls within the scope of the various embodiments.

[0038] As shown, a method 300 begins at step 301, in which hearable device 92 measures one or more inherent attributes associated with an authorized user of hearable device 92, such as user 91. The one or more inherent attributes may include, without limitation, an EEG signature, an otoacoustic signature, earpiece fit or impedance, or a heart beat signature, among others. In some embodiments, measurement of the inherent attribute may involve generating an audio stimulus, for example via loudspeaker 206, and recording a response measured by a sensor included in earpiece 201. In other embodiments, the one or more inherent attributes may be measured without a triggering stimulus.

[0039] In step 302, hearable device 92 generates an inheritance factor based on the inherent attributes measured in step

301, i.e., the unique value, function, or signature that is associated with the particular user for the inherent attribute. In addition, hearable device 92 stores the inheritance factor so generated, either locally in one-time memory 212A, remotely in a computing device within wireless communication network 100, or both locally and remotely. In some embodiments, hearable device 92 is configured so that only a single authorized user may be associated with hearable device 92, and in such embodiments, one-time memory 212A is programmed accordingly. It is noted that steps 301 and 302 may be performed upon initial startup of hearable device 92, when user 91 is first established as the authorized user of hearable device 92.

[0040] In step 303, hearable device 92 measures an inherent attribute of the user currently wearing hearable device 92, for example via one or more sensors disposed within earpiece 201. As described above in step 301, measurement of the inherent attribute of the user currently wearing hearable device 92 may include generating an audio stimulus, for example via loudspeaker 206, and recording a response. In step 304, based on the inherent attribute measured in step 303, hearable device 92 generates an inheritance factor associated with the current wearer of hearable device 92, i.e., the unique value, function, or signature that is associated with the current user for the inherent attribute.

[0041] In some embodiments, steps 303 and 304 are performed in response to a user powering on hearable device 92 and/or donning hearable device 92. In such embodiments, hearable device 92 is typically configured to determine whether the current wearer of hearable device 92 is the authorized user of hearable device 92, i.e., whether the current wearer of hearable device 92 is matched to hearable device 92. Thus, in such embodiments, the authentication functionality associated with providing secure access to wireless communication network 100 typically resides in hearable device 92. In such embodiments, the donning and removal of hearable device 92 may be detected by impedance sensor 253, temperature sensor 254, and/or heartbeat/respiration sensor 255.

[0042] Alternatively, in some embodiments, steps 303 and 304 are performed in response to hearable device 92 entering the wireless signal range of wireless communication network 100 and/or receiving a query from wireless access point 103 for an inheritance factor associated with the current user of hearable device 92. For example, such a query may be received from wireless access point 103 in embodiments in which the inheritance factor associated with the authorized user of hearable device 92 is not stored locally in hearable device 92, and is only stored remotely in a computing device within wireless communication network 100. Thus, in such embodiments, the authentication functionality associated with providing secure access to wireless communication network 100 typically resides in wireless access point 103.

[0043] In step 305, hearable device 92 initiates a communication connection with wireless access point 103, such as when user 91 enters the wireless signal range of wireless communication network 100 while wearing hearable device 92. For example, when wireless communication network 100 is associated with a vehicle information system for a particular vehicle, step 305 may take place when user 91 approaches the particular vehicle; when wireless communication network 100 is associated with a home network, step 305 may take place when user 91 approaches the home associated with the home network.

[0044] In step 306, an authentication process for hearable device 92 is performed with respect to wireless communication network 100. When the authentication process is successfully completed, i.e., hearable device 92 and user 91 is authenticated, method 300 proceeds to step 307; when the authentication process is not successfully completed, i.e., hearable device 92 or user 91 is not authenticated, method 300 proceeds to step 308.

[0045] In some embodiments, as part of the authentication process of step 306, hearable device 92 determines whether the current wearer of hearable device 92 is properly matched to hearable device 92. For example, hearable device 92 may compare the inheritance factor generated in step 304 (i.e., the inheritance factor generated for and associated with the current wearer of hearable device 92) to the inheritance factor generated in step 302 (i.e., the inheritance factor generated and stored for and associated with the authorized wearer of hearable device 92). When the inheritance factor generated in step 304 is sufficiently similar to the inheritance factor generated in step 302, hearable device 92 is considered to properly match the current wearer of hearable device 92, and hearable device 92 performs a conventional authentication process with wireless access point 103. Specifically, hearable device 92 may transmit a unique ID associated with hearable device 92 to wireless access point 103, wireless access point 103 looks up the unique ID in communications network 100, and grants access thereto when the unique ID transmitted is correct.

[0046] It is noted that in some embodiments, hearable device 92 may determine whether the current wearer of hearable device 92 is properly matched to hearable device 92 prior to the current wearer of wearing hearable device 92 entering the wireless signal range of wireless communication network 100 (step 305). For example, hearable device 92 may determine whether the current wearer of hearable device 92 is properly matched to hearable device 92 whenever a particular user powers up hearable device 92, or whenever a particular user dons hearable device 92, as detected by one or more sensors in earpiece 201.

[0047] In other embodiments, the authentication process for hearable device 92 may be largely performed by wireless access point 103. As noted above in steps 303 and 304, in such embodiments, wireless access point 103 may query hearable device 92 for an inheritance factor associated with the current user of hearable device 92. In such embodiments, the inheritance factor for the authorized user of hearable device 92 may only be stored remotely from hearable device 92, such as in wireless access point 103 or computing device 101. Thus, the authentication process performed by wireless access point 103 includes comparing the inheritance factor for the authorized user of hearable device 92 to the inheritance factor associated with the current wearer of hearable device 92 that is generated by hearable device 92 in step 304.

[0048] In step 307, which is performed in response to hearable device 92 and user 91 being successfully authenticated, wireless entry point 103 allows access to communications network 100. In step 308, which is performed in response to hearable device 92 or user 91 being unsuccessfully authenticated, wireless entry point 103 suspends access to communications network 100.

[0049] Thus, by implementation of method 300, secure access to a communication network is provided by hearable device 92 based on multiple-factor authentication. The multiple-factor authentication may include, without limitation,

one or more inference factors associated with the authorized user of hearable device 92 and measurable by hearable device 92 (e.g., an EEG signature, an otoacoustic signature, etc.), a possession factor (e.g., possession of hearable device 92), and any suitable knowledge factor (e.g., a PIN or password). In embodiments in which only inference and possession factors are employed, multiple factor authentication can be performed transparently to the user. Consequently, a user can securely and conveniently access a communications network via hearable device 92 without the need for a PIN, a physical key or fob, and without the concern that mere possession of hearable device 92 may compromise the security of the communications network.

[0050] In sum, various embodiments set forth systems and techniques for securely accessing a computing device within a communication network via a hearable device. Advantageously, by authenticating a user of the hearable device based on one or more inference factors that are measured by the hearable device, secure access to the communication network may be granted without a PIN or physical key or fob. A further advantage is that possession of the hearable device by an unauthorized user is insufficient to compromise the security of the communication network.

[0051] The descriptions of the various embodiments have been presented for purposes of illustration, but are not intended to be exhaustive or limited to the embodiments disclosed. Many modifications and variations will be apparent to those of ordinary skill in the art without departing from the scope and spirit of the described embodiments.

[0052] Aspects of the present embodiments may be embodied as a system, method or computer program product. Accordingly, aspects of the present disclosure may take the form of an entirely hardware embodiment, an entirely software embodiment (including firmware, resident software, micro-code, etc.) or an embodiment combining software and hardware aspects that may all generally be referred to herein as a “circuit,” “module” or “system.” Furthermore, aspects of the present disclosure may take the form of a computer program product embodied in one or more computer readable medium(s) having computer readable program code embodied thereon.

[0053] Any combination of one or more computer readable medium(s) may be utilized. The computer readable medium may be a computer readable signal medium or a computer readable storage medium. A computer readable storage medium may be, for example, but not limited to, an electronic, magnetic, optical, electromagnetic, infrared, or semiconductor system, apparatus, or device, or any suitable combination of the foregoing. More specific examples (a non-exhaustive list) of the computer readable storage medium would include the following: an electrical connection having one or more wires, a portable computer diskette, a hard disk, a random access memory (RAM), a read-only memory (ROM), an erasable programmable read-only memory (EPROM or Flash memory), an optical fiber, a portable compact disc read-only memory (CD-ROM), an optical storage device, a magnetic storage device, or any suitable combination of the foregoing. In the context of this document, a computer readable storage medium may be any tangible medium that can contain, or store a program for use by or in connection with an instruction execution system, apparatus, or device.

[0054] Aspects of the present disclosure are described above with reference to flowchart illustrations and/or block

diagrams of methods, apparatus (systems) and computer program products according to embodiments of the disclosure. It will be understood that each block of the flowchart illustrations and/or block diagrams, and combinations of blocks in the flowchart illustrations and/or block diagrams, can be implemented by computer program instructions. These computer program instructions may be provided to a processor of a general purpose computer, special purpose computer, or other programmable data processing apparatus to produce a machine, such that the instructions, which execute via the processor of the computer or other programmable data processing apparatus, enable the implementation of the functions/acts specified in the flowchart and/or block diagram block or blocks. Such processors may be, without limitation, general purpose processors, special-purpose processors, application-specific processors, or field-programmable processors or gate arrays.

[0055] The flowchart and block diagrams in the figures illustrate the architecture, functionality, and operation of possible implementations of systems, methods and computer program products according to various embodiments of the present disclosure. In this regard, each block in the flowchart or block diagrams may represent a module, segment, or portion of code, which comprises one or more executable instructions for implementing the specified logical function(s). It should also be noted that, in some alternative implementations, the functions noted in the block may occur out of the order noted in the figures. For example, two blocks shown in succession may, in fact, be executed substantially concurrently, or the blocks may sometimes be executed in the reverse order, depending upon the functionality involved. It will also be noted that each block of the block diagrams and/or flowchart illustration, and combinations of blocks in the block diagrams and/or flowchart illustration, can be implemented by special purpose hardware-based systems that perform the specified functions or acts, or combinations of special purpose hardware and computer instructions.

[0056] While the preceding is directed to embodiments of the present disclosure, other and further embodiments of the disclosure may be devised without departing from the basic scope thereof, and the scope thereof is determined by the claims that follow.

The claimed invention is:

1. An apparatus comprising:

an earpiece;

a sensor configured to measure an inherent attribute associated with a user;

a wireless transceiver configured to communicate with a wireless access point of a wireless communication network; and

a controller configured to establish authenticated access to the wireless communication network based on the inherent attribute associated with the user.

2. The apparatus of claim 1, wherein the sensor is disposed in the earpiece and is configured to contact a surface of an ear canal of the user.

3. The apparatus of claim 1, wherein the sensor includes at least one of an electroencephalogram sensor, an otoacoustic microphone, an impedance sensor, a temperature sensor, and a heartbeat/respiration sensor.

4. The apparatus of claim 1, wherein the inherent attribute associated with the user includes at least one of an electroencephalogram signature, an otoacoustic signature, an elec-

trical impedance between the earpiece and an ear canal of the user, and a heartbeat signature.

5. The apparatus of claim 1, wherein the earpiece is configured to conform to at least a portion of an ear canal of a particular user.

6. The apparatus of claim 1, wherein the controller is configured to establish authenticated access to the wireless communication network by:

generating an inherence security factor based on the inherent attribute of the user; and
authenticating the user based on the inherence security factor generated for the user.

7. The apparatus of claim 6, wherein the controller is configured to authenticate the user by comparing the inherence security factor generated for the user to an authorized inherence security factor.

8. The apparatus of claim 7, wherein the controller is further configured to: measure an inherent attribute associated with an authorized user of the apparatus; and

generate the authorized inherence security factor based on the inherent attribute associated with the authorized user of the apparatus.

9. The apparatus of claim 6, wherein the controller is configured to authenticate the user by transmitting the inherence security factor generated for the user to the wireless access point.

10. The apparatus of claim 1, wherein the controller is further configured to determine whether the user is wearing the apparatus prior to establishing authenticated access to the communication network.

11. The apparatus of claim 1, further comprising a triggering device configured to generate an audio stimulus, and wherein the sensor is configured to measure the inherent attribute in response to the audio stimulus.

12. A method for securely accessing a wireless communication network, the method comprising:

measuring an inherent attribute associated with a user with a sensor that is disposed in an earpiece and configured to contact a surface of an ear canal of the user; and

establishing authenticated access to the wireless communication network based on the inherent attribute associated with the user.

13. The method of claim 12, wherein establishing authenticated access to the wireless communication network com-

prises communicating with a wireless access point of the wireless communication network via a wireless transceiver.

14. The method of claim 12, wherein establishing authenticated access to the wireless communication network comprises:

generating an inherence security factor based on the inherent attribute of the user; and
authenticating the user based on the inherence security factor generated for the user.

15. The apparatus of claim 14, further comprising authenticating the user by comparing the inherence security factor generated for the user to an authorized inherence security factor.

16. The apparatus of claim 15, further comprising:
measuring an inherent attribute associated with an authorized user of the apparatus; and

generating the authorized inherence security factor based on the inherent attribute associated with the authorized user of the apparatus.

17. A non-transitory computer readable medium storing instructions that, when executed by a processor, configure the processor to perform the steps of:

measuring an inherent attribute associated with a user with a sensor that is disposed in an earpiece and configured to contact a surface of an ear canal of the user; and

establishing authenticated access to the wireless communication network based on the inherent attribute associated with the user.

18. The non-transitory computer readable medium of claim 17, wherein establishing authenticated access to the wireless communication network comprises communicating with a wireless access point of the wireless communication network via a wireless transceiver.

19. The non-transitory computer readable medium of claim 17, further comprising the step of determining whether the user is wearing the apparatus prior to establishing authenticated access to the communication network.

20. The non-transitory computer readable medium of claim 17, further comprising the step of generating an audio stimulus, and wherein the sensor is configured to measure the inherent attribute in response to the audio stimulus.

* * * * *

专利名称(译)	可验证身份验证技术		
公开(公告)号	US20170118204A1	公开(公告)日	2017-04-27
申请号	US14/919555	申请日	2015-10-21
[标]申请(专利权)人(译)	哈曼国际工业有限公司		
申请(专利权)人(译)	哈曼国际工业公司.		
当前申请(专利权)人(译)	哈曼国际工业公司.		
[标]发明人	LAINE HEIKKI BUTTS DONALD JOSEPH		
发明人	LAINE, HEIKKI BUTTS, DONALD JOSEPH		
IPC分类号	H04L29/06 A61B5/0484 A61B5/117 A61B5/01 A61B5/0205 A61B5/00 H04W12/06 A61B7/04		
CPC分类号	H04L63/0861 H04W12/06 H04L63/10 A61B5/04845 A61B7/04 A61B2503/12 A61B5/0205 A61B5/6817 A61B5/117 A61B5/053 A61B5/01 H04W12/08 H04W12/00504 H04W12/0605 H04W84/12		
其他公开文献	US10341339		
外部链接	Espacenet USPTO		

摘要(译)

各种实施例阐述了一种装置，包括耳机，被配置为测量与用户相关联的固有属性的传感器，被配置为与无线通信网络的无线接入点通信的无线收发器，以及控制器。控制器被配置为基于与用户相关联的固有属性来建立对无线通信网络的认证访问。所公开实施例的优点在于，可听设备可以基于由可穿戴设备测量的一个或多个固有因素，方便地验证用户对具有增强安全性的网络的访问。

