



- (51) International Patent Classification:
H04B 7/00 (2006.01) *H04B 7/26* (2006.01)
- (21) International Application Number:
PCT/US2015/026043
- (22) International Filing Date:
15 April 2015 (15.04.2015)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:
14/258,007 21 April 2014 (21.04.2014) US
- (71) Applicant: ARM LIMITED [GB/GB]; 110 Fulbourn Road, Cambridge, CB1 9NJ (GB).
- (72) Inventor: HILLYARD, Jason, Edward Robert; 4310 Hortensia Street, San Diego, CA 92103 (US).
- (74) Agent: LEVEQUE, Renee' Michelle; Leveque Intellectual Property Law, P.C., 241 East 4th Street, #102, Frederick, Maryland 21701 (US).
- (81) Designated States (*unless otherwise indicated, for every kind of national protection available*): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.
- (84) Designated States (*unless otherwise indicated, for every kind of regional protection available*): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU,

[Continued on next page]

(54) Title: SYSTEMS AND METHODS FOR SHORT RANGE WIRELESS DATA TRANSFER

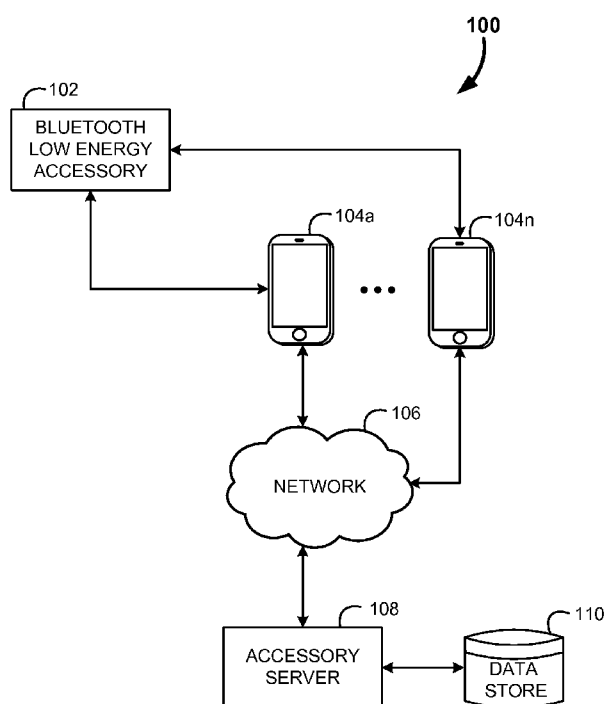


Fig. 1

(57) Abstract: Systems and methods for application level authentication are provided for use with the low energy Bluetooth device and accessory. This includes receiving accessory credentials from a server, establishing a Bluetooth low energy connection with the accessory, authenticating with the accessory, and lastly transferring data to the accessory. The transferring of the data may be either a bulk transfer, or a data stream. The authenticating may be an application layer authentication between a device and the accessory using a shared secret key and using a hash function. Additional embodiments include methods for over-the-air firmware updates, and device control of a low energy Bluetooth accessory.



LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK,
SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ,
GW, KM, ML, MR, NE, SN, TD, TG).

— *before the expiration of the time limit for amending the
claims and to be republished in the event of receipt of
amendments (Rule 48.2(h))*

Published:

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

**SYSTEMS AND METHODS FOR SHORT RANGE WIRELESS DATA
TRANSFER**

BACKGROUND

[0001] This invention relates generally to systems and methods for short range wireless data transfers. Such systems and methods enable new classes of low cost, low energy accessories that have the ability to get firmware updates, or other data transfers while still complying with Bluetooth low energy (BLE) standards.

[0002] Bluetooth low energy is an international open standard for low power short range wireless communication. BLE enables low power devices that have extended battery life, and are thus ideally suited for small accessories where power availability is at a premium, such as wireless watches, proximity key fobs, fitness sensors, etc.

[0003] However, current Bluetooth low energy protocols do not have the needed ability to perform extended data transfers, and particularly do not have functionality to perform firmware upgrades. Instead, they were designed for reading and writing small, discrete data values. For very basic accessory devices, this is not of concern since the firmware tends to remain static; however, as accessory products become more complex, the embedded firmware correspondingly becomes more complex. With this increase in firmware complexity, the chance that updates are needed multiplies. This is particularly true when the accessory communicates with a mobile device, such as a tablet or cell phone, where the operating system version changes on a near continual basis, and thereby potentially impacting device to accessory interoperability.

[0004] In addition to data transfer needs for bulk, continuous transfers, and firmware updating, BLE accessory devices often have other communication protocol needs that require special solutions to improve performance and interoperability. Many accessories need special “device control” features. Examples of device control features: configuring connection parameters, setting the connection security level, or disconnecting a connection.

[0005] Although these three device control examples given above could be performed with standard procedures defined by the Bluetooth specification, there is still a need for special solutions defined at the application level. This is because

mobile phone operating systems often limit the access apps have to these standard device control procedures. For example, iOS does not allow an app to set the security level of a connection.

[0006] Moreover, the Bluetooth specification defines the standard protocols and procedures for establishing a secure connection between two BLE devices. In a secure connection the data transferred between BLE radios is encrypted. Two devices are considered to be “bonded” when they have established and stored an encryption key used for secure communication.

[0007] Although this standard bonding security procedure is beneficial, it also has drawbacks. The process of bonding requires user interaction; the mobile phone OS will generally prompt the phone user with a popup message asking if it is ok to bond. If an accessory is used with multiple phones the accessory must bond separately with each phone, and bonding information must be stored in non-volatile memory for each bonded phone. An accessory also needs the ability to delete a bond; however since most accessory devices lack sophisticated user interfaces it may be impossible to select and delete the bond for a particular phone. Clearly there is a need for a more sophisticated application level authentication and encryption protocols.

[0008] It is therefore apparent that an urgent need exists for systems and methods short range wireless data transfers which comport to Bluetooth low energy standards to enable the bulk or streaming transfer of data to an accessory, firmware updates, authentication and encryption on the application level, and special control protocols. Such systems and methods enable firmware updates and other data transfers to classes of devices that currently do not have this level of functionality. This enables BLE accessories to continue their interoperability even when the device they are in communication with devices that have changed their operating system.

SUMMARY

[0009] To achieve the foregoing and in accordance with the present invention, systems and methods for short range wireless data transfers. Such systems and methods enable new classes of low cost, low energy accessories that have the ability to get firmware updates, or other data transfers while still complying with Bluetooth low energy (BLE) standards.

[0010] In some embodiments, a method for application level authentication is provided for use with the low energy Bluetooth device and accessory. This method includes receiving accessory credentials from a server, establishing a Bluetooth low energy connection with the accessory, authenticating with the accessory, and lastly transferring data to the accessory. The transferring of the data may be either a bulk transfer, or a data stream. The authenticating may be an application layer authentication between a device and the accessory using a shared secret key and using a hash function.

[0011] In some cases, an application on a device receives the accessory credentials and authenticates with the accessory without the device operating system's involvement. The method may also include defining a file transfer control message for a device to get and put data from and to the accessory, and defining separate channels for communicating the file transfer control messages and the transfer data. The length of the get or put operation may also be defined. The transferred data may be verified for completion and correctness.

[0012] Additional embodiments include methods for over-the-air firmware updates for low energy Bluetooth accessories. The over-the-air firmware updates include reading accessory information, authenticating with the accessory (as described above), initiating a diagnostic mode in the accessory, transferring firmware update data to the accessory, verifying the data transfer, and disconnecting from the accessory which triggers a reset of the accessory.

[0013] Additional embodiments include methods for device control of a low energy Bluetooth accessory. Device control includes the steps of sending a device control message from a device application to an accessory application, and receiving a response at the device application for the control message. The device control message may be a parameter update request.

[0014] The method may also include forming a communication channel between a device Bluetooth low energy stack and an accessory Bluetooth low energy stack. The communication channel is a standard Bluetooth low energy connection parameter update. In some cases, the parameter update request causes the accessory application to send a connection parameter update to the accessory Bluetooth low energy stack. The response is a device control message received from the accessory application including current connection parameters.

[0015] The device control message may also be a get ATT MTU operation. The ATT MTU operation causes the accessory application to send a get ATT MTU request to the accessory Bluetooth low energy stack. The response is a device control message received from the accessory application including current ATT MTU value.

[0016] The device control message may also be a security request. In this case a communication channel between a device Bluetooth low energy stack and an accessory Bluetooth low energy stack is formed which is a standard Bluetooth low energy pairing procedure. The device Bluetooth low energy stack confirms pairing with the device application. The security request causes the accessory application to send a security request message to the accessory Bluetooth low energy stack. The response is a device control message received from the accessory application including connection security level.

[0017] The device control message may also be a service change inquiry. A communication channel between a device Bluetooth low energy stack and an accessory Bluetooth low energy stack is formed, which is a standard Bluetooth low energy discovery procedures. The service change inquiry causes the accessory application to send a service change message to the accessory Bluetooth low energy stack, and subsequently a service change indication from the accessory Bluetooth low energy stack to the device Bluetooth low energy stack. The response is discovery results from the device Bluetooth low energy stack.

[0018] Note that the various features of the present invention described above may be practiced alone or in combination. These and other features of the present invention will be described in more detail below in the detailed description of the invention and in conjunction with the following figures.

BRIEF DESCRIPTION OF THE DRAWINGS

[0019] In order that the present invention may be more clearly ascertained, some embodiments will now be described, by way of example, with reference to the accompanying drawings, in which:

[0020] Figure 1 is an example schematic block diagram for a system for short range wireless data transfers, in accordance with some embodiments;

[0021] Figure 2 is an example schematic block diagram for a more detailed view of components within the Bluetooth low energy accessory, in accordance with some embodiments;

[0022] Figure 3 is an example schematic block diagram for more detailed view of the host protocol stack within the Bluetooth low energy accessory, in accordance with some embodiments;

[0023] Figure 4 is an example process flow diagram for application level authentication for short range wireless data transfers, in accordance with some embodiments;

[0024] Figure 5 is an example process flow diagram for a wireless firmware upgrade, in accordance with some embodiments;

[0025] Figure 6 is an example process flow diagram for a wireless parameter upgrade, in accordance with some embodiments;

[0026] Figure 7 is an example process flow diagram for determining the packet size that may be transmitted, in accordance with some embodiments;

[0027] Figure 8 is an example process flow diagram for changing a security level, in accordance with some embodiments;

[0028] Figure 9 is an example process flow diagram for notifying the GATT client that the services have changed on a GATT server, in accordance with some embodiments; and

[0029] Figures 10-15 are example operation diagrams for operation and data transfers between device and a BLE accessory, in accordance with some embodiments.

DETAILED DESCRIPTION

[0030] The present invention will now be described in detail with reference to several embodiments thereof as illustrated in the accompanying drawings. In the following description, numerous specific details are set forth in order to provide a thorough understanding of embodiments of the present invention. It will be apparent, however, to one skilled in the art, that embodiments may be practiced without some or all of these specific details. In other instances, well-known process steps and/or

structures have not been described in detail in order to not unnecessarily obscure the present invention. The features and advantages of embodiments may be better understood with reference to the drawings and discussions that follow.

[0031] Aspects, features and advantages of exemplary embodiments of the present invention will become better understood with regard to the following description in connection with the accompanying drawing(s). It should be apparent to those skilled in the art that the described embodiments of the present invention provided herein are illustrative only and not limiting, having been presented by way of example only. All features disclosed in this description may be replaced by alternative features serving the same or similar purpose, unless expressly stated otherwise. Therefore, numerous other embodiments of the modifications thereof are contemplated as falling within the scope of the present invention as defined herein and equivalents thereto. Hence, use of absolute and/or sequential terms, such as, for example, “will,” “will not,” “shall,” “shall not,” “must,” “must not,” “first,” “initially,” “next,” “subsequently,” “before,” “after,” “lastly,” and “finally,” are not meant to limit the scope of the present invention as the embodiments disclosed herein are merely exemplary.

[0032] The following discussion relates to methods and systems for short range wireless data transfers. Such systems and methods enable new classes of low cost, low energy accessories that have the ability to get firmware updates, or other data transfers while still complying with Bluetooth low energy (BLE) standards.

[0033] Bluetooth low energy is an international open standard for low power short range wireless communication. BLE enables low power devices that have extended battery life, and are thus ideally suited for small accessories where power availability is at a premium, such as wireless watches, proximity key fobs, fitness sensors, etc.

[0034] The ability to perform data transfers in the means described below enables firmware updates for BLE accessories. This ability enables the accessory manufacturer to fix bugs, solve interoperability problems, and improve product performance after the product has shipped. By enabling wireless data transfers, no physical connections are required, which minimizes costs associated with the accessory, and it is also easier for the user; in fact it can be done without the user's knowledge or interaction.

[0035] BLE accessory products often have other data transfer needs in addition to support for over-the-air firmware upgrades. For example, a fitness accessory may need to transfer a several kilobytes of data containing physical activity measurements to a phone. This is an example of a bulk data transfer of a finite length. Another example is an accelerometer sensor that constantly transfers a stream of accelerometer measurements to a phone. This is an example of a streaming data transfer that continues until the transfer is stopped. Currently disclosed systems and methods also enable these kinds of bulk and continuous data transfers, enabling greater functionality of BLE accessories.

[0036] As previously noted, the standard BLE communication protocols defined in the Bluetooth specification (which is herein incorporated by reference) are not necessarily designed for this sort of data transfer. Instead, they were designed for reading and writing small, discrete data values. As such, the currently disclosed systems and methods enable enhanced functionality over the standard protocols.

[0037] In addition to data transfers for firmware updates and bulk or continuous data transfers, other BLE accessory devices often have other communication protocol needs that require special solutions to improve performance and interoperability. Many accessories need special “device control” features. Examples of device control features include: configuring connection parameters, setting the connection security level, or disconnecting a connection. Likewise, as previously noted, there is a need for application layer authentication and encryption. The ability to supply these control features and authentication/encryption procedures is described in greater detail below.

[0038] The term “device” as used herein is intended to refer to any device to which a BLE accessory communicates with. Often these devices are also referred to as “mobile devices” as one focus of BLE accessory communication is with devices such as laptops, cell phones, and tablets. However, it should be understood that any device where communication to a BLE accessory is desired falls within the scope of the term “device”.

[0039] Also note that the term “accessory” is utilized to describe the BLE enabled device which communicates with the cell phone, tablet, computer, etc. The term accessory is utilized, primarily, to differentiate the BLE end client from the device to which it communicates. As such, while “accessory” typically denotes a reliance or

subsistence upon the main device, this is not entirely the case for the purposes of this disclosure. Rather an accessory, for purposes of this disclosure may refer to any device which employs BLE protocols and a radio to communicate with another device.

[0040] Note that the following disclosure includes a series of subsections. These subsections are not intended to limit the scope of the disclosure in any way, and are merely for the sake of clarity and ease of reading. As such, disclosure in one section may be equally applied to processes or descriptions of another section if and where applicable.

I. SHORT RANGE WIRELESS COMMUNICATION SYSTEMS

[0041] To facilitate this discussion, Figure 1 provides an example schematic block diagram for a system for short range wireless data transfers, shown generally at 100. In this example block diagram, a Bluetooth low energy (BLE) device is in communication with one or more devices 104a-n via a BLE wireless protocol. The Bluetooth low energy specification defines standard communications procedures for devices to send and receive data. The device 104a-n may include mobile devices such as cell phones and tablets, or other devices such as appliances, stationary computers, video game consoles, etc.

[0042] The device 104a-n connects to the BLE accessory 102. The device 104a-n is running an application which implements the application-level BLE communications protocol, defining the data sent between the device 104a-n and the accessory 102 for the particular application.

[0043] In a number of embodiments, the device 104a-n may also have connectivity to a larger network 106. This network may include a local area network or a broader wide area network. In some instances, the network 106 is a corporate network of the internet. In other cases the network 106 could include multiple networks in conjunction (for example, a cell phone network that connects to the internet).

[0044] The network 106 enables communication between the devices 104a-n and one or more accessory servers 108. The server 108 may include a database 110 that includes credential information, updates, etc. Often the server 108 may be hosted by, or on behalf, of the accessory manufacturer to enable firmware updates and enhanced post market control of the accessory 102. However, it is envisioned that the server

108 may alternatively be set up by an active community of users, or an interested third party.

[0045] Continuing to Figure 2, an example schematic block diagram for a more detailed view of components within the Bluetooth low energy accessory 102 is provided. Here the accessory 102 is illustrated as having a BLE radio 210 in communication with a microcontroller 220. The microcontroller 220 executes host protocol stack firmware 224 and the BLE application 222.

[0046] The Bluetooth specification defines a standard protocol stack used by BLE devices. An example protocol stack 224 is shown in Figure 3. The stack 224 consists of the following standard protocol layers:

[0047] L2CAP 310: The Logical Link Control Adaptation Protocol provides channelization and multiplexing to the ATT and SMP protocols;

[0048] ATT 304: The Attribute Protocol provides procedures for finding, reading and writing discrete data values known as attributes. This is a client-server protocol with one device acting as client and the other as server;

[0049] SMP 306: The Security Manager Protocol provides procedures for bonding and establishing an encrypted connection;

[0050] GAP 308: The Generic Access Profiles provides procedures for device management, connection management, and security management;

[0051] GATT 302: The Generic Attribute Profile defines how attributes are grouped into characteristics and services in order to perform a specific application function.

[0052] When a BLE link connects two or more devices, the devices must operate in certain roles defined by the Bluetooth specification. In the example shown in Figure 1, the device 104a-n operates as a Central device and the accessory 102 operates as a Peripheral device. The Central device initiates the connection and controls the connection timing. A Peripheral device broadcasts advertisements in order to accept a connection.

[0053] In addition to the Peripheral and Central connection roles, the devices also operate in certain protocol roles. One device must operate as an ATT and GATT server while the other device operates as an ATT and GATT client. In the example

shown in Figure 1, the devices 104a-n operates as an ATT and GATT client, accessing the ATT and GATT server on the accessory 102. Note that the connection roles and the client/server roles are independent; for example a device could be a Peripheral and client.

[0054] The two protocols most important to the systems and methods disclosed herein are ATT and GATT. ATT defines protocol messages for finding, reading, and writing attributes. The attributes are stored in a database in an ATT server. Each attribute has the following data elements associated with it:

[0055] A UUID that uniquely identifies the type of attribute;

[0056] Permissions that define whether the attribute can for example be read or written;

[0057] The attribute value.

[0058] The GATT layer provides another level of data abstraction. It groups attributes into data objects called characteristics. A characteristic is typically designed communicate a particular piece of data, for example a heart rate measurement. A characteristic consists of attributes containing the following information:

[0059] The characteristic properties;

[0060] The characteristic value;

[0061] Optionally, one or more characteristic descriptors.

[0062] Characteristics can be further grouped into a logical group called a service. A service is typically designed to perform a particular application function, for example a battery level service to communicate a device's battery level, or a heart rate service to configure and communicate a heart rate measurement.

II. DATA EXCHANGE PROFILE FOR DATA TRANSFERS

[0063] The following section provided details pertaining to the system architecture for the short range wireless data transfers central to this disclosure. Now, specifics of the mechanisms and protocols employed to achieve BLE data transfers will be explored. The data transfer utilized to effectuate firmware updates, bulk and continuous data transfers, application level authentication and encryption and device control features relies upon a novel protocol, referred herein as the Data Exchange

(DX) Profile. A Data Exchange Service (DXS) is used by the DX Profile to implement the following functionalities:

- [0064] Bulk file transfer;
 - [0065] Streaming data transfer;
 - [0066] Read, write, append, truncate, or erase a file;
 - [0067] Over-the-air (OTA) firmware upgrade;
 - [0068] Resume interrupted transfers;
 - [0069] Multiple simultaneous transfers;
 - [0070] Application layer authentication;
 - [0071] Session-based or file-based application layer encryption;
 - [0072] Device control features.
- [0073] The DXS defines four different characteristics. These characteristics essentially operate as communications channels to transfer messages for their respective purposes. The four characteristics are provided below:
- [0074] Device Control Characteristic. This characteristic is used to perform device control procedures, such as connection control.
 - [0075] File Transfer Control Characteristic. This characteristic is used for file transfer control messages.
 - [0076] File Transfer Data Characteristic. This characteristic is used for file transfer data.
 - [0077] Authentication Characteristic. This characteristic is used for authentication procedures, e.g. the Server can authenticate the Client.
 - [0078] Generally device control, authentication, and file transfer control employ GATT 302 protocols. File transfer data may rely upon either GATT 302 or L2CAP 310 protocols.
 - [0079] Implementing a file transfer over BLE poses a problem: Data transfer is traditionally performed over the ATT/GATT protocols, which were designed for transfer of small data values rather than bulk data transfer. Fast bulk data transfer can be implemented using a sequence of ATT Notification messages or ATT Write

Command messages, which do not require per-packet acknowledgement at the ATT layer. However data flow can be difficult to manage between the sender and receiver; for example, some mobile phone operating systems do not perform well and may even drop data of a very long sequence of ATT Write Command messages are sent.

[0080] Another alternative is to transfer bulk data using the new L2CAP “connection oriented channels” protocol defined in the Bluetooth 4.1 specification. This can provide a channel for fast and robust data transfer, however it is not backward compatible with existing Bluetooth 4.0 devices. In fact operating systems like iOS 7.0 and Android 4.4 do not yet support this feature.

[0081] The file transfer control messages for a client is defined to get and put (read and write) data from/to a server. Additionally, separate channels for communicating file transfer control messages and file transfer data are defined. The client can specify the length of a “Get” or “Put” operation, which typically will be less than the total length of the file. Therefore a file transfer typically involves a sequence of Get or Put operations. Lastly, the client and server can negotiate the file transfer data to be sent over either GATT or L2CAP.

[0082] This solution allows the client and server to balance throughput with interoperability by breaking up a file transfer into several shorter data transfers. It also can take advantage of devices supporting Bluetooth 4.1 L2CAP features while remaining backward compatible with Bluetooth 4.0 devices.

[0083] In addition, the file transfer protocol has unique features designed to support use cases for streaming data and over-the-air firmware upgrades. These features include a “file verify” operation, a “file type” parameter, and a “file resource” structure. The verify operation checks the CRC of the transferred file, in some embodiments. In alternate embodiments, other means for verification may be employed, such as checking cryptographic signature or the like. This is used to verify the complete and correct transfer of a file, such as a firmware file. The file type parameter distinguishes between streaming files and bulk files. Lastly, the file resource structure defines the handle, file type, length, permitted operations, name and version of each file.

[0084] Specific use cases of the data transfer functionalities described above will be discussed in greater detail in the following subsections.

A. Application Level Authentication

[0085] The authentication procedure performs application-layer authentication between an accessory 102 and device 104a-n, allowing the accessory 102 to authenticate the device 104a-n (or user via an application). The authentication algorithm, in some embodiments, is based on a shared secret key and may use AES-128 as a hash function. The authentication procedure requires a random number generator on the accessory 102 and an AES-128 (or other suitable hash function) implementation on the device 104a-n and accessory 102. In alternate embodiments, the authentication algorithm may also use public key cryptography to securely distribute a secret key between an accessory and device.

[0086] Application-layer authentication allows the accessory 102 to restrict access to certain features of the DX Profile only to authenticated devices 104a-n. The authentication procedure defines three levels of authentication: User, Maintenance, and Debug. Each level uses a different secret key. The Debug level uses a known fixed key.

[0087] One important benefit of application layer authentication is that it allows an accessory 102 to be authenticated to a user, via an application, rather than a device simply being authenticated to another device (e.g., a cell phone). This simplifies security for the user and aligns better with how users interact with their devices 104a-n: users typically have multiple cell phones or tablets and may run the same apps on them, which may connect to the same accessory devices 102.

[0088] Returning to Figure 1 for reference, application level authentication involves the accessory 102 interfacing with an application on the device 104a-n. This application queries the server 108 via the network 106 to retrieve the user's account information which includes the accessory's 102 credentials. These credentials are used to authenticate the user to the accessory 102.

[0089] Turning to Figure 4, an example process flow diagram for authentication thereby enabling further short range wireless data transfers is provided. In this example process, the user logs into his account on the credential server using a username and password (or other suitable technique) via an application on the device 104a-n (at 410).

[0090] The application then retrieves credentials for accessories that have previously been associated with the user's account (at 420). Accessories 102 may be linked with the users account automatically at purchase, or via a product registration. The credentials include a unique device identifier such as a serial number and the authentication secret key.

[0091] A Bluetooth low energy connection is then established between the device 104a-n and the accessory 102 (at 430). This connection includes providing the unique identifier from the accessory 102 to the application on the device 104a-n. The unique identifier and key associated with the identifier is used to authenticate the accessory 102 (at 440) using the earlier received credentials. The authentication then allows for access to additional features, such as data transfers (at 450), or additional features.

[0092] Moving to Figure 12, an example diagram is provided, at 1200, for the ATT transport used for the authentication process. The authentication characteristic uses the ATT Write Request PDU to transport messages sent by the device 104a-n. The accessory 102 returns the status of an operation in the ATT Write Response or ATT Error Response sent in response to the ATT Write Request. The ATT Handle Value Notification PDU is used to transport messages sent by the accessory 102.

B. Firmware Update

[0093] As previously indicated, the DX Profile also enables for wireless firmware updates. Although existing over the air firmware update mechanisms already exist, the presently disclosed system and methods differ in their ability to allow the client to select the block size for file transfers by breaking up a file transfer into multiple file Put operations, the length of which is determined by the client (i.e. the iOS app). If the app knows it can only transfer 20 packets reliably before pausing, it can simply set the Put length accordingly. In addition, there is a handshake sequence at the end of each Put operation where the server sends a message to the client that the Put is complete. This eliminates the need for a timer; the client now knows the current Put is complete and can proceed with the next one.

[0094] Additionally, the currently disclosed firmware updating procedures have the following features not commonly found in existing over the air firmware updating mechanisms:

1. Files can be transferred from client to server (Put) and server to client (Get). Multiple simultaneous file transfers are possible.
2. Data transport is supported over GATT or L2CAP.
3. Data is transferred in a block size determined by the client. The completion of each Put transfer is acknowledged by the server.
4. Verification of the firmware and server device reset is controlled by the client. The client can verify a firmware file transfer without first resetting the server.
5. The protocol has an “enter diagnostic mode” command that can be sent from the client. This allows a server to better manage its resources and activities (e.g. stop reading the accelerometer and storing measurements when in diagnostic mode, etc.).
6. The server can refuse a Put or Get request from the client or abort a Put or Get operation in progress.
7. The protocol has a mechanism for the server to authenticate the client before a file transfer is initiated. The server can refuse file transfers if authentication is not successful. The authentication protocol is not intrinsically coupled to the file transfer protocol.

[0095] Figure 5 is an example process flow diagram for a wireless firmware upgrade, shown generally at 500. The firmware update utilizes a bulk file transfer from a firmware file from the device 104a-n to the accessory 102. The firmware update procedure begins with the device 104a-n reading the accessory 102 information (at 510). The information read typically includes device model and firmware revision using DXS device control functionality.

[0096] Next, the device 104a-n seeks authentication and an authentication procedure is performed (as previously discussed) using the DXS authentication characteristic (at 520). After the authentication is successfully performed, the device 104a-n sends the accessory 102 a message that causes the accessory 102 to enter into diagnostic mode (at 530). The DXS device control message is utilized to cause this diagnostic mode.

[0097] Next, the device 104a-n pushes the new firmware file to the accessory 102 using DXS file transfer (at 540), as discussed above. The device 104a-n requests the accessory 102 to verify the downloaded file (at 550) using the DXS file verification operation. Once the file has been verified, the device 104a-n sends a message to the

accessory 102 to disconnect and reset (at 550). The disconnect and reset message is sent as a DXS device control message.

C. Device control

[0098] In addition to bulk file transfer and firmware updates, the disclosed systems and methods include a number of device control capabilities that utilize the DXS. These include the ability to control parameter updates, determining packet size allowances, changing a security level, GATT service change notifications, deletion of bonds, and entering the accessory into diagnostic mode.

[0099] The Bluetooth specification defines several standard protocol procedures for things like connection management and security. However, popular operating systems like iOS and Android don't allow apps access to these standard Bluetooth LE procedures. These same procedures however can often be performed when initiated by the peer device connected to the iOS or Android phone. The purpose of the application-level device control procedures implemented over GATT are to allow a client (an app) on a feature-limited operating system to perform standard BLE procedures by instructing the peer device (accessory) to request the procedure.

[00100] Figures 6 to 9 provide sample flow charts for differing device control procedures. Each functionality will be described in greater detail in association with the corresponding figure.

[00101] Figure 6 is an example communication diagram for a wireless parameter upgrade, shown generally at 600. This procedure updates the communication interval between devices in a connection; a short interval increases throughput, a long interval reduces power consumption. This process starts with the device application sending the accessory application a DXS device control message (at 610) requesting a parameter update. This causes the accessory application to connect with the accessory BLE stack for the parameter update (at 620).

[00102] The accessory BLE stack forms a standard BLE connection with the device BLE stack for parameter updating (at 630). The accessory BLE stack then indicates that the update is complete to the accessory application (at 640). The accessory application then sends the device application, using a DXS device control message, the current connection parameter information (at 650). In this manner, the parameters may be updated by the device application, essentially using the accessory as a proxy.

[00103] Figure 7 is an example process flow diagram for determining the packet size that may be transmitted, shown generally at 700. The ATT MTU value is used by the app to determine how large a packet it can send to an accessory device. This process starts with the device application sending the accessory application a DXS device control message (at 710) requesting the ATT MTU value. This causes the accessory application to connect with the accessory BLE stack (at 720).

[00104] The accessory BLE stack then provides the ATT MTU value to the accessory application (at 730). The accessory application then sends the device application, using a DXS device control message, the current ATT MTU information (at 740).

[00105] Figure 8 is an example process flow diagram for changing a security level, shown generally at 800. The security level of a connection indicates whether a connection is encrypted or unencrypted. The security level can be changed to request bonding and/or enable encryption. This process starts with the device application sending the accessory application a DXS device control message (at 810) with a security request. This causes the accessory application to connect with the accessory BLE stack for the security request (at 820).

[00106] The accessory BLE stack forms a standard BLE pairing procedure with the device BLE stack (at 830). The device BLE stack confirms the pairing with the device application (at 840), and then the accessory BLE stack then indicates that the pairing is complete to the accessory application (at 850). The accessory application then sends the device application, using a DXS device control message, the connection security level (at 860).

[00107] Figure 9 is an example process flow diagram for notifying the GATT client that the services have changed on a GATT server, shown generally at 900. This is a mechanism to notify a GATT client that the services have changed on a GATT server, and the client needs to discover services and characteristics again. This process starts with the device application sending the accessory application a DXS device control message (at 910) requesting service change. This causes the accessory application to connect with the accessory BLE stack for the service change (at 920).

[00108] The accessory BLE stack sends a standard change indication to the device BLE stack (at 930). The accessory BLE stack then forms standard discovery

procedures with the device BLE stack (at 940). The device BLE stack then sends discovery results to the device application (at 950).

[00109] In addition to the above identified device control features, additional procedures that are not standardized by the Bluetooth specification may be effectuated using the DX profile. These include bond deletion and entry to diagnostic mode. The deleting bond procedure allows an application to delete the bonds stored on an accessory. This is useful when the accessory has no user interface to perform this function. When deleting bonds the client sends a device control message instructing the server to delete all bonds. The server deletes all bonds. Note it is important for the server to authenticate the client (using the methods described earlier) before accepting this message. If an untrusted device is permitted to connect to a server and delete all its bonds it opens up a potential security hole whereby an attacker could force a server to re-bond then eavesdrop on the bonding protocol transaction and attempt to brute force crack the security key.

[00110] Likewise, the 'enter into diagnostic mode procedure' instructs the accessory to enter diagnostic mode. Typically this will shut down normal operation of the accessory (e.g. stop measuring heart rate, activity, etc.) and is performed before a firmware upgrade. When entering diagnostic mode the client sends a device control message instructing the server enter diagnostic mode. The server ceases performing certain normal operations, e.g. stops reading accelerometer data. Then the server send a diagnostic mode complete message to the client.

III. EXAMPLES

[00111] Now that the systems and methods for firmware updates, file transfers and device controls has been described in considerable detail, a series of example communications are provided in reference to Figures 10-15 which are employed to effectuate the above methods. For example, Figure 10 provides examples of a set operation, a get operation and an update operation, shown generally at 1000.

[00112] The device control characteristic uses the ATT write request PDU to transport Get and Set messages sent by the client. The server returns the status of a Get or Set message in the ATT write response or ATT error response PDU. The ATT handle value notification PDU is used to transport update messages sent by the server.

[00113] A Set operation consists of an ATT write request followed by an ATT write response or ATT error response. A Get operation consists of ATT write request followed by an ATT write response, then followed by a handle value notification with an update message containing the result of the Get operation. Note that an update message serves two purposes: First, it is used to return the result of a Get message. Second, it is used to asynchronously send parameter data from the server to the client.

[00114] Figure 11 illustrates ATT transport operations, including control messaging, and data transfers between the accessory and device, shown generally at 1100. On the file control characteristic, the ATT write command PDU is used by the client to send file control messages. The ATT handle value notification PDU is used by the server to send file control messages. Likewise, on the file data characteristic, the ATT write command PDU is used by the client to send file data, and ATT handle value notification PDU is used by the Server to send file data.

[00115] Figure 12 illustrates the usage of ATT transport for authentication characteristics, shown generally at 1200. The authentication characteristic uses the ATT write request PDU to transport messages sent by the client. The server returns the status of an operation in the ATT write response or ATT error response sent in response to the ATT write request. The ATT handle value notification PDU is used to transport messages sent by the server.

[00116] An example of the authentication procedure is illustrated in Figure 13, shown generally at 1300. The client sends an authentication start with the desired authentication level. The server sends an ATT write response or an ATT error response. The server generates a random number and sends an authentication challenge. The client computes a hash and sends an authentication reply. The server also computes the hash, and compares it to that received from the client. Then the server sends an ATT write response or ATT error response. If the authentication was successful, the client computes a session key. The client sets the authentication level for the connection and also computes the session key. The authentication level is maintained until the connection is closed or until the authentication level is set again by another successful authentication procedure.

[00117] Continuing, Figure 14 provides an example of a bulk file transfer, shown generally at 1400. Bulk file transfer may also be performed with a resume if it has an interruption (not illustrated). If a bulk file transfer is interrupted, upon reconnecting,

the Client resumes the file transfer using the offset to get the next data that had not been received.

[00118] Likewise, Figure 15 provides for streaming file transfer, shown generally at 1500. In this example, the server contains a streaming file. The client gets the file and then later sends an abort to stop streaming of the file. Note that the client can receive some file data after sending an abort. The server sends an EOP when it has stopped sending data.

[00119] As can be imagined, numerous other examples and permutations of the disclosed firmware updates, file transfers, and device commands are possible, but have been omitted from the present disclosure in the interest of clarity and brevity. Although not all of the above disclosed functionalities have been exemplified using an example operation diagram, it should be understood that these operations are still within the intended scope of the invention.

[00120] In sum, the present disclosure provides systems and methods for short range wireless data transfers. Such systems and methods enable new classes of low cost, low energy accessories that have the ability to get firmware updates, or other data transfers while still complying with Bluetooth low energy (BLE) standards.

[00121] While this invention has been described in terms of several embodiments, there are alterations, modifications, permutations, and substitute equivalents, which fall within the scope of this invention. Although sub-section titles have been provided to aid in the description of the invention, these titles are merely illustrative and are not intended to limit the scope of the present invention.

[00122] It should also be noted that there are many alternative ways of implementing the methods and apparatuses of the present invention. It is therefore intended that the following appended claims be interpreted as including all such alterations, modifications, permutations, and substitute equivalents as fall within the true spirit and scope of the present invention.

CLAIMS

What is claimed is:

1. A method for application level authentication, useful in conjunction with a low energy Bluetooth device and accessory, the method comprising:
 - receiving accessory credentials from a server;
 - establishing a Bluetooth low energy connection with the accessory;
 - authenticating with the accessory; and
 - transferring data to the accessory.
2. The method of claim 1, wherein the transferring of the data is a bulk transfer.
3. The method of claim 1, wherein an application on a device receives the accessory credentials and authenticates with the accessory without the device operating system's involvement.
4. The method of claim 1, further comprising defining a file transfer control message for a device to get and put data from and to the accessory.
5. The method of claim 4, further comprising defining separate channels for communicating the file transfer control messages and the transfer data.
6. The method of claim 4, further comprising specifying the length of a get or put operation.
7. The method of claim 1, wherein the transferring of the data is a streaming transfer.
8. The method of claim 7, further comprising verifying the transferred data for completion and correctness.
9. The method of claim 1, wherein the authenticating is an application layer authentication between a device and the accessory using a shared secret key and using a hash function.
10. A method for over-the-air firmware updates, useful in conjunction with a low energy Bluetooth device and accessory, the method comprising:
 - reading accessory information;
 - authenticating with the accessory;

initiating a diagnostic mode in the accessory;

transferring firmware update data to the accessory;

verifying the data transfer;

disconnecting from the accessory, wherein the disconnection triggers a reset of the accessory.

11. The method of claim 10, wherein the verifying includes checking data completeness and correctness.
12. The method of claim 10, wherein the authenticating includes receiving accessory credentials from a server, and wherein the authenticating is an application layer authentication between a device and the accessory using a shared secret key and using a hash function.
13. A method for device control, useful in conjunction with a low energy Bluetooth device and accessory, the method comprising:
 - sending a device control message from a device application to an accessory application; and
 - receiving a response, at the device application, for the control message.
14. The method of claim 13, wherein the device control message is a parameter update request.
15. The method of claim 14, further comprising forming a communication channel between a device Bluetooth low energy stack and an accessory Bluetooth low energy stack, wherein the communication channel is a standard Bluetooth low energy connection parameter update.
16. The method of claim 14, wherein the parameter update request causes the accessory application to send a connection parameter update to the accessory Bluetooth low energy stack, , and wherein the response is a device control message received from the accessory application including current connection parameters.
17. The method of claim 13, wherein the device control message is a get ATT MTU operation.

18. The method of claim 17, wherein the ATT MTU operation causes the accessory application to send a get ATT MTU request to the accessory Bluetooth low energy stack, and wherein the response is a device control message received from the accessory application including current ATT MTU value.
19. The method of claim 13, wherein the device control message is a security request.
20. The method of claim 19, further comprising forming a communication channel between a device Bluetooth low energy stack and an accessory Bluetooth low energy stack, wherein the communication channel is a standard Bluetooth low energy pairing procedure, and the device Bluetooth low energy stack confirms pairing with the device application.
21. The method of claim 20, wherein the security request causes the accessory application to send a security request message to the accessory Bluetooth low energy stack, and wherein the response is a device control message received from the accessory application including connection security level.
22. The method of claim 13, wherein the device control message is a service change inquiry.
23. The method of claim 22, further comprising forming a communication channel between a device Bluetooth low energy stack and an accessory Bluetooth low energy stack, wherein the communication channel includes standard Bluetooth low energy discovery procedures.
24. The method of claim 23, wherein the service change inquiry causes the accessory application to send a service change message to the accessory Bluetooth low energy stack, and subsequently a service change indication from the accessory Bluetooth low energy stack to the device Bluetooth low energy stack, and wherein the response are discovery results from the device Bluetooth low energy stack.

1/13

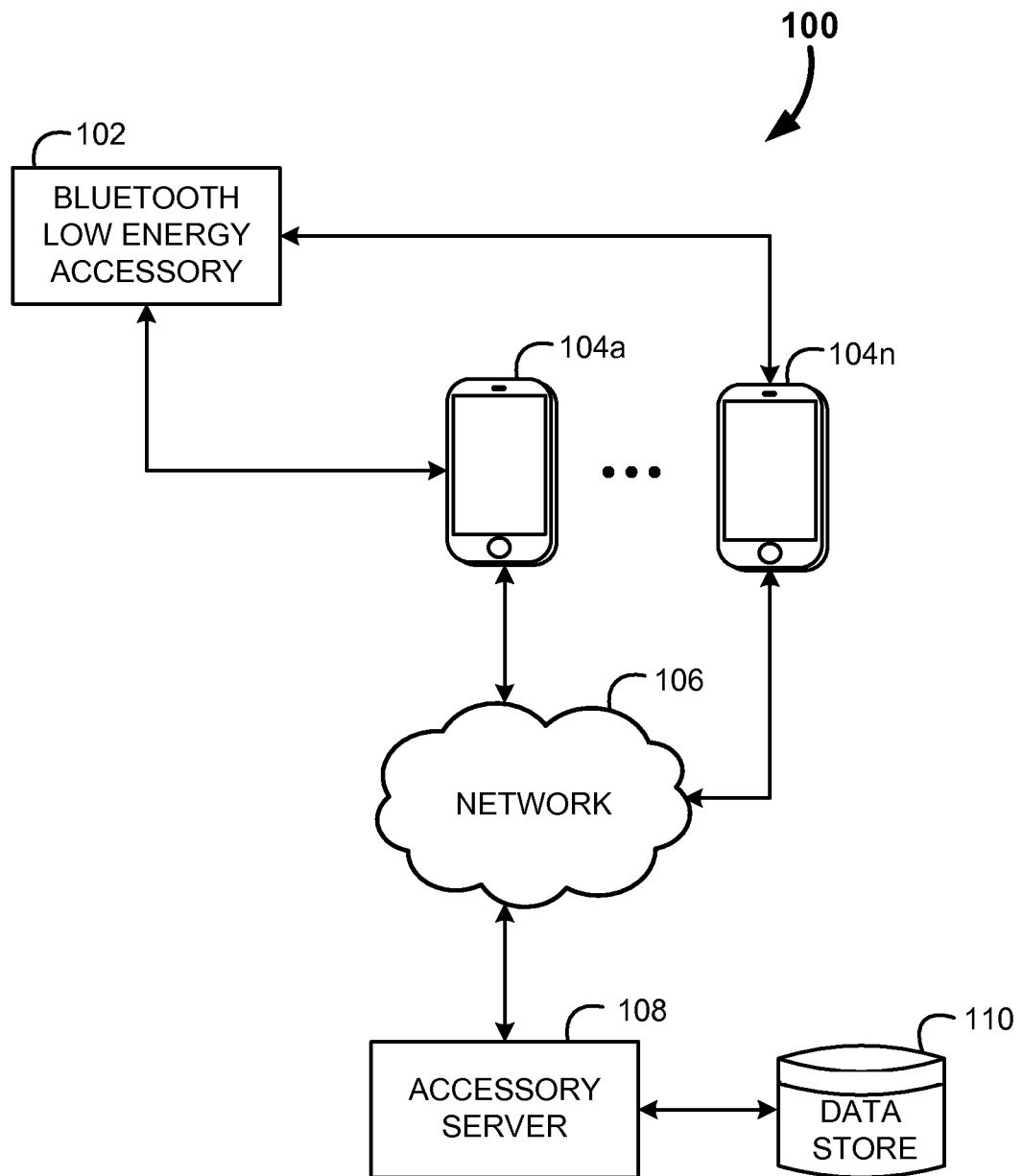


Fig. 1

2/13

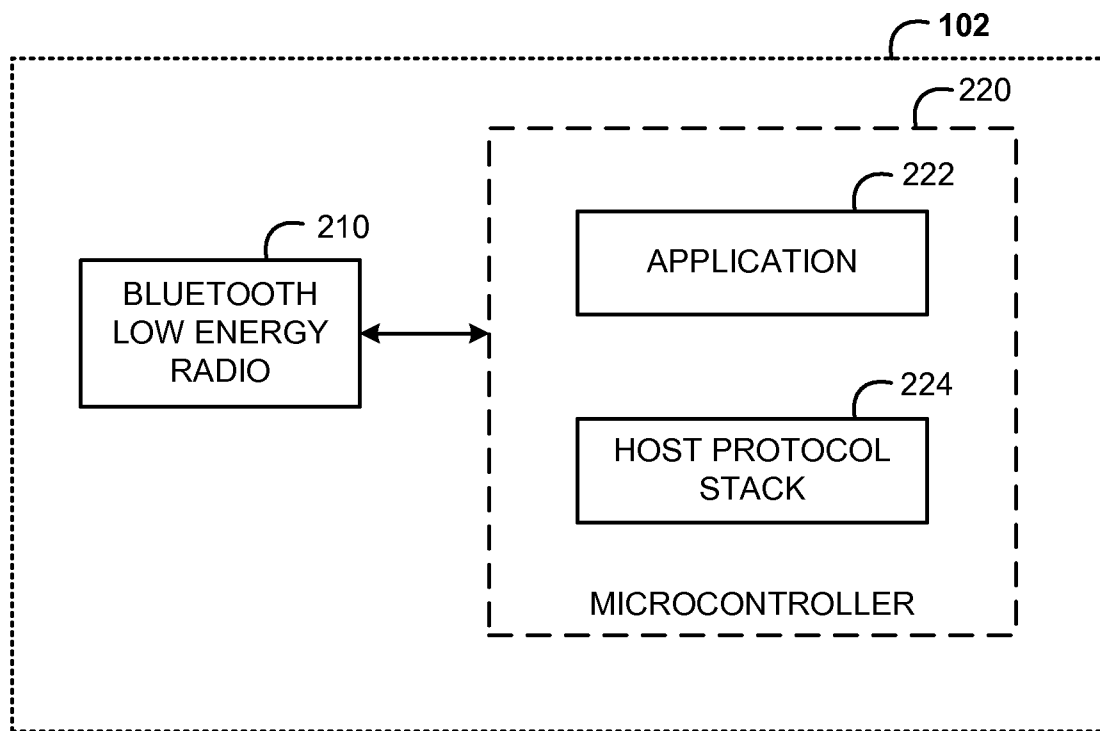


Fig. 2

3/13

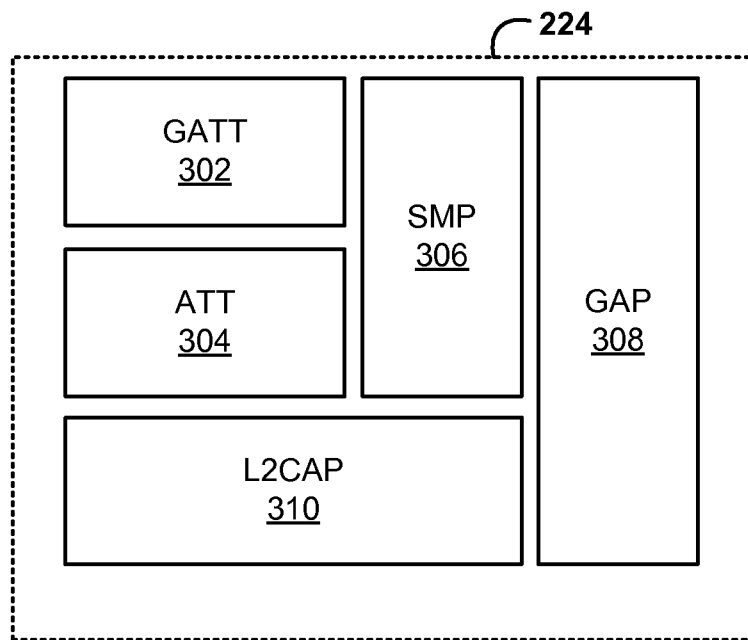


Fig. 3

4/13

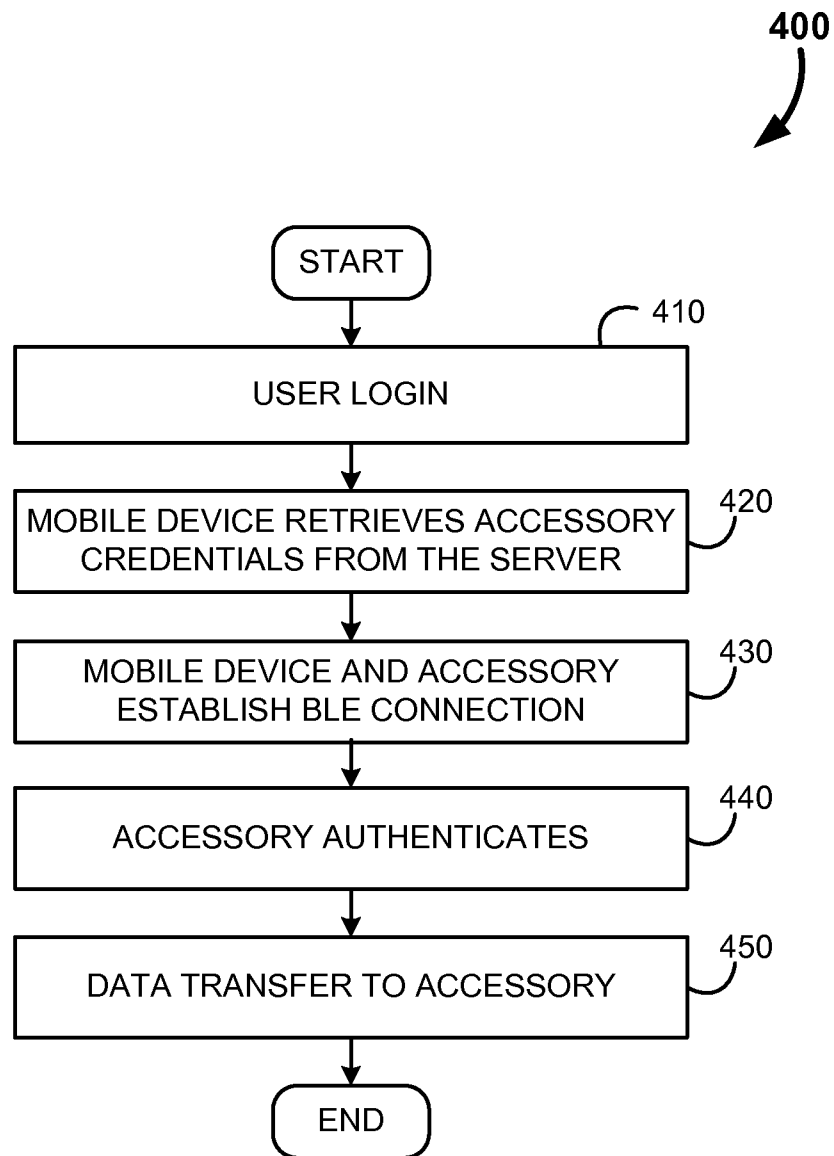


Fig. 4

5/13

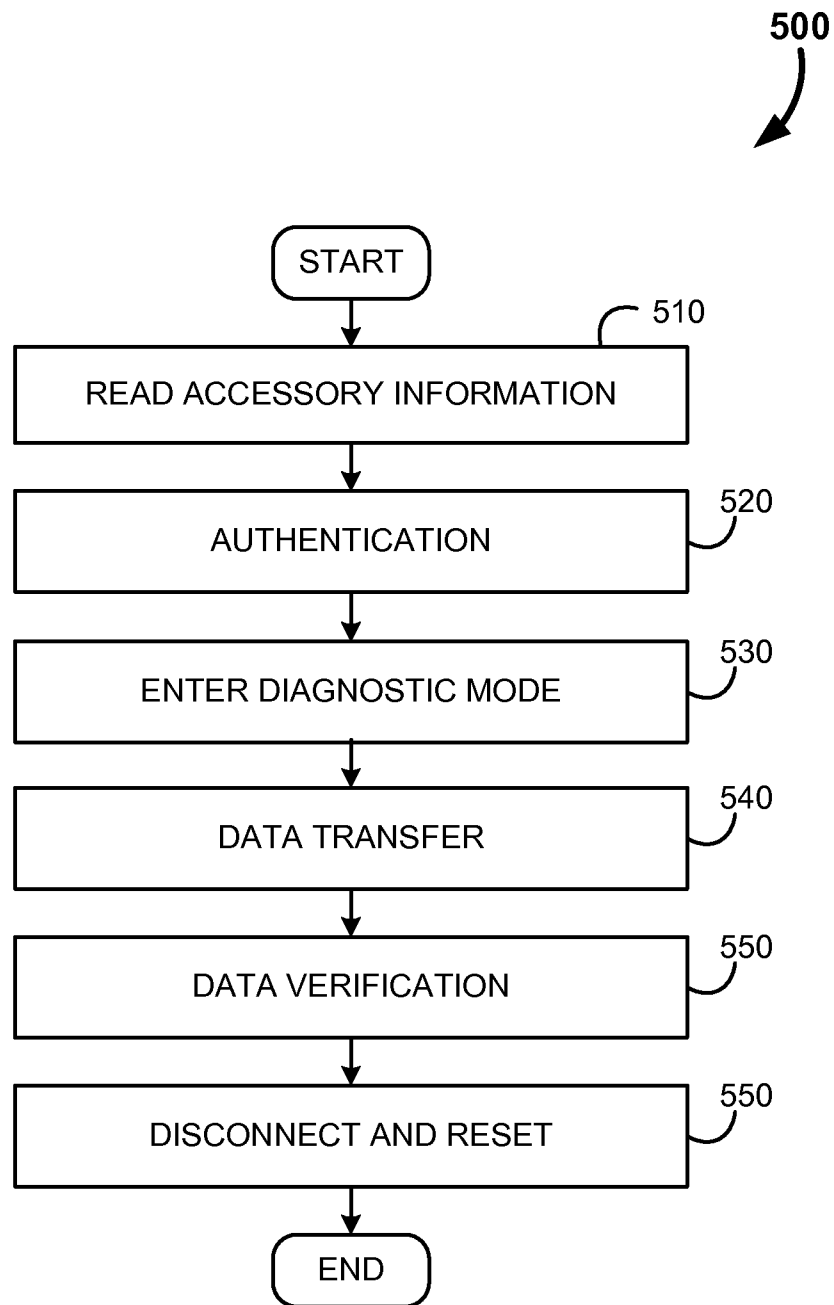


Fig. 5

6/13

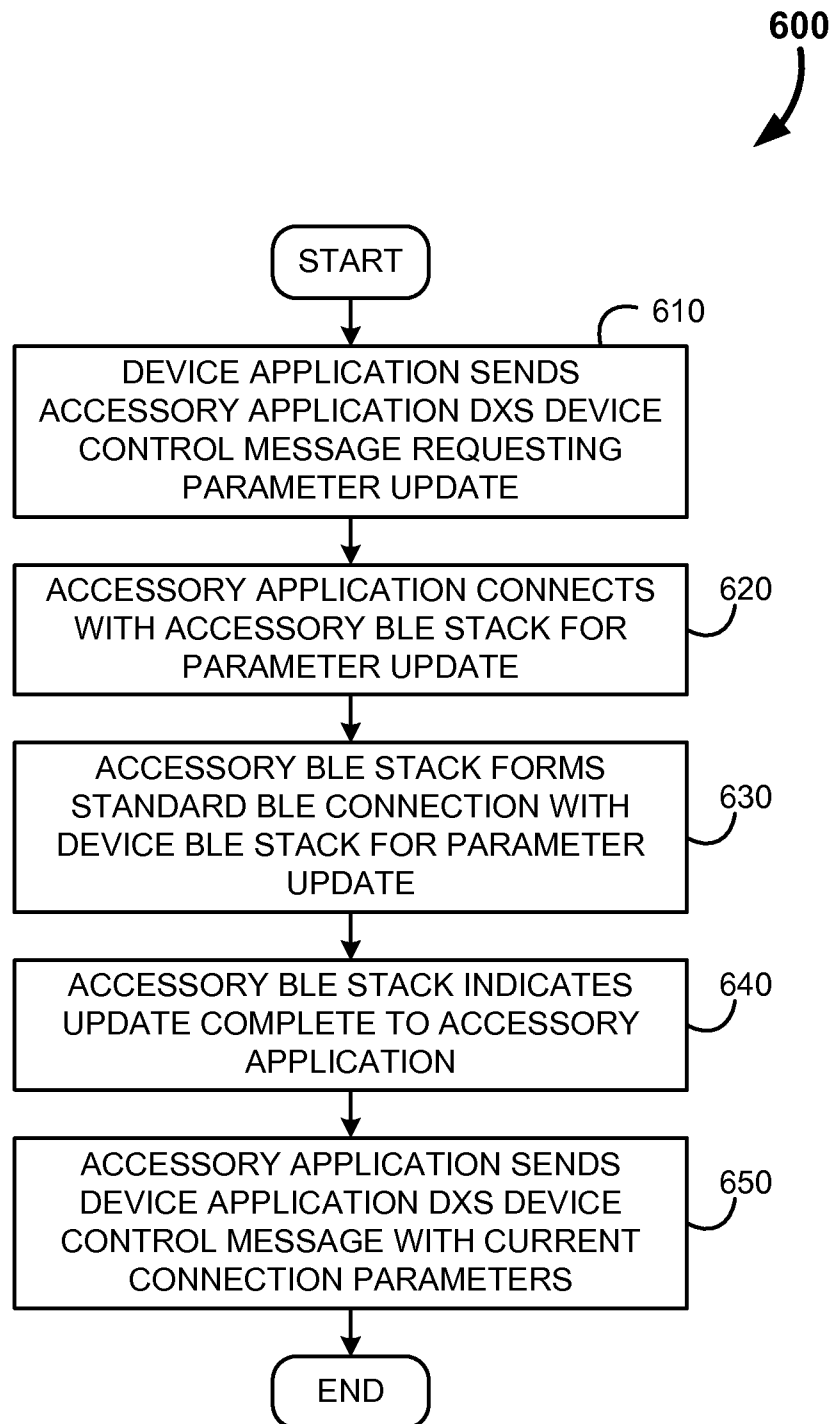


Fig. 6

7/13

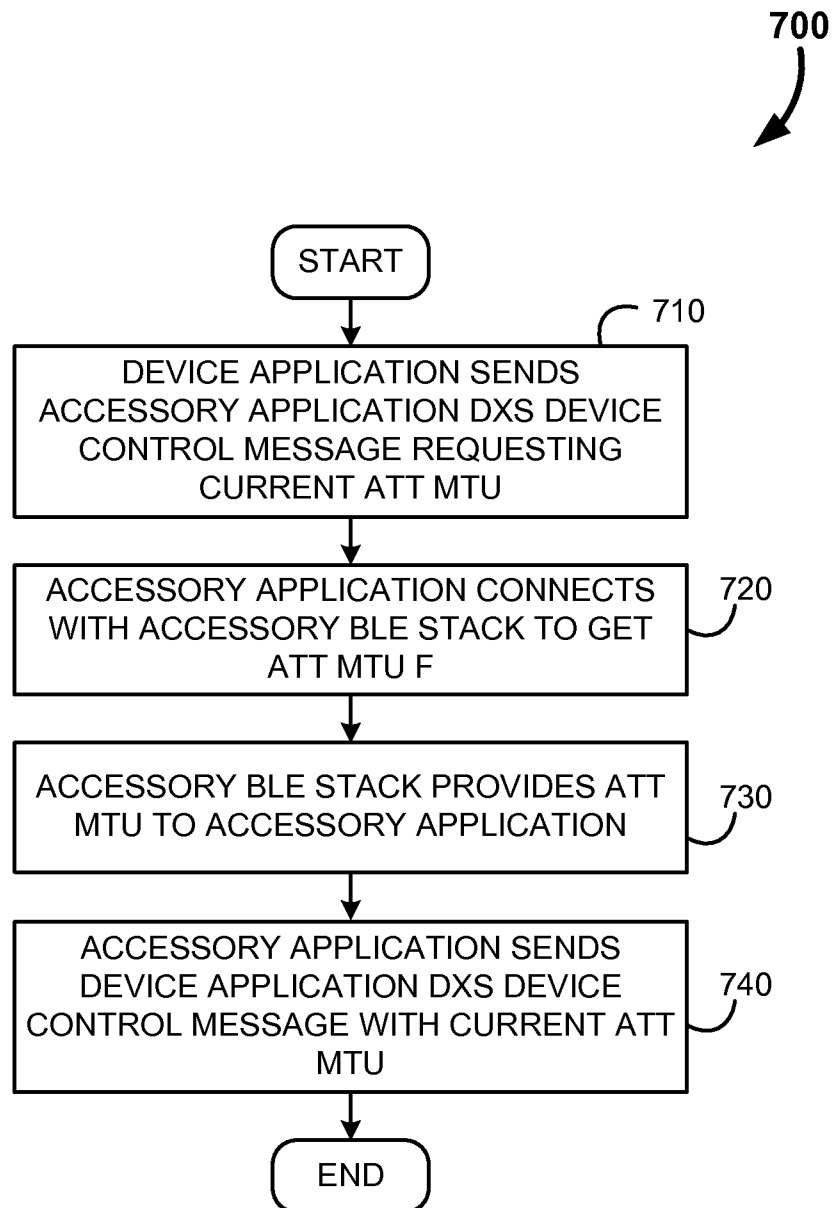
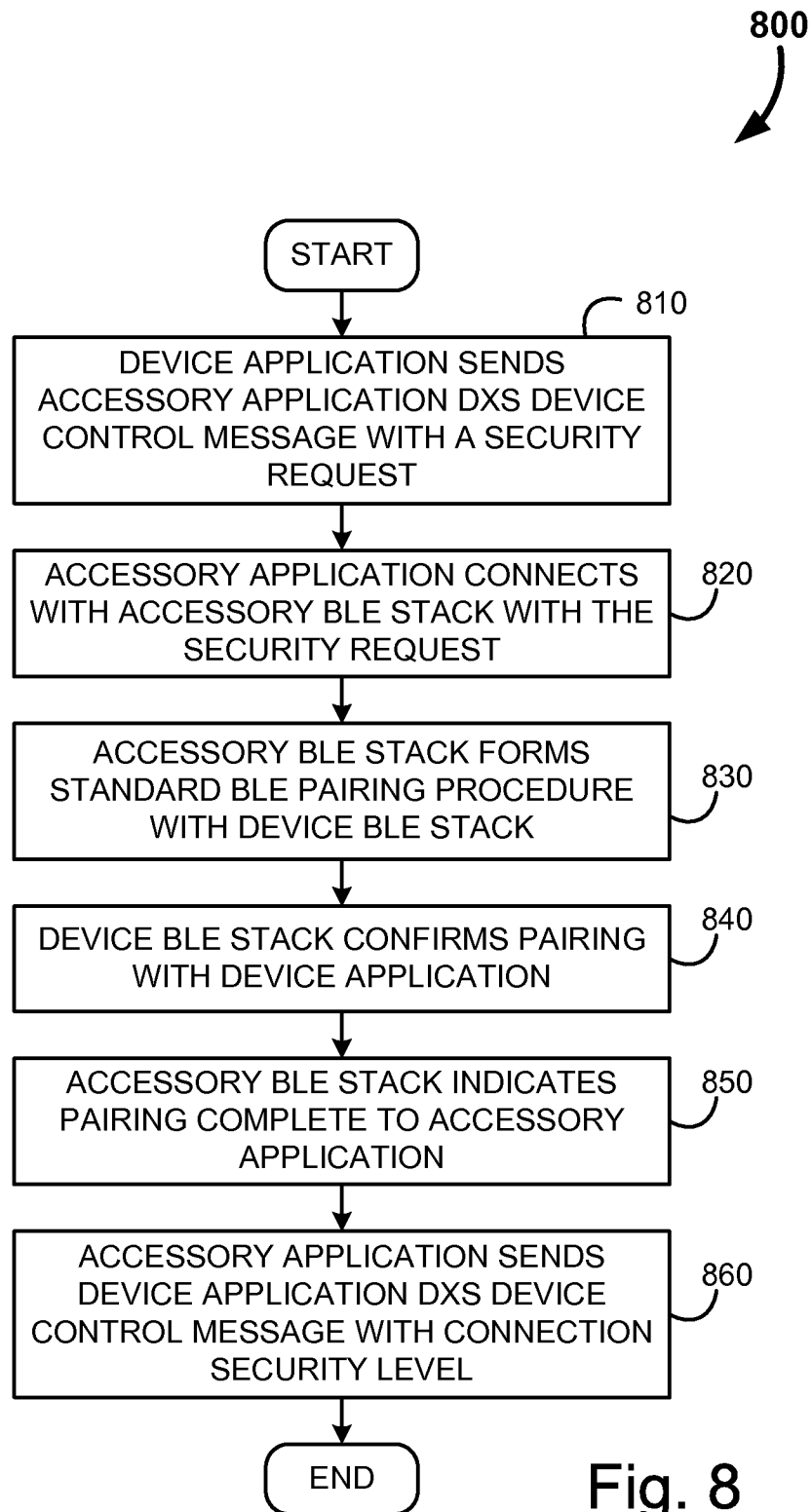


Fig. 7



9/13

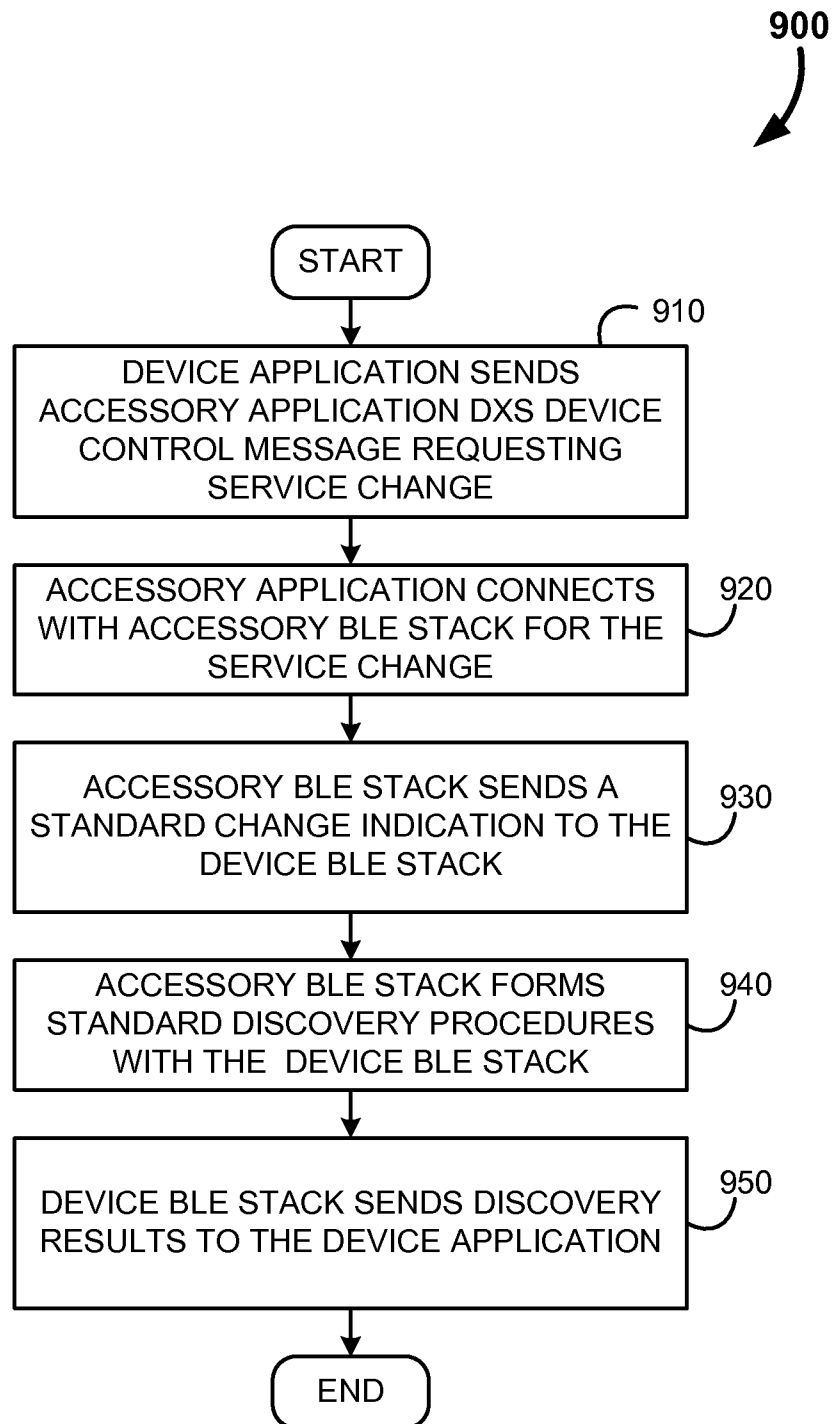


Fig. 9

10/13

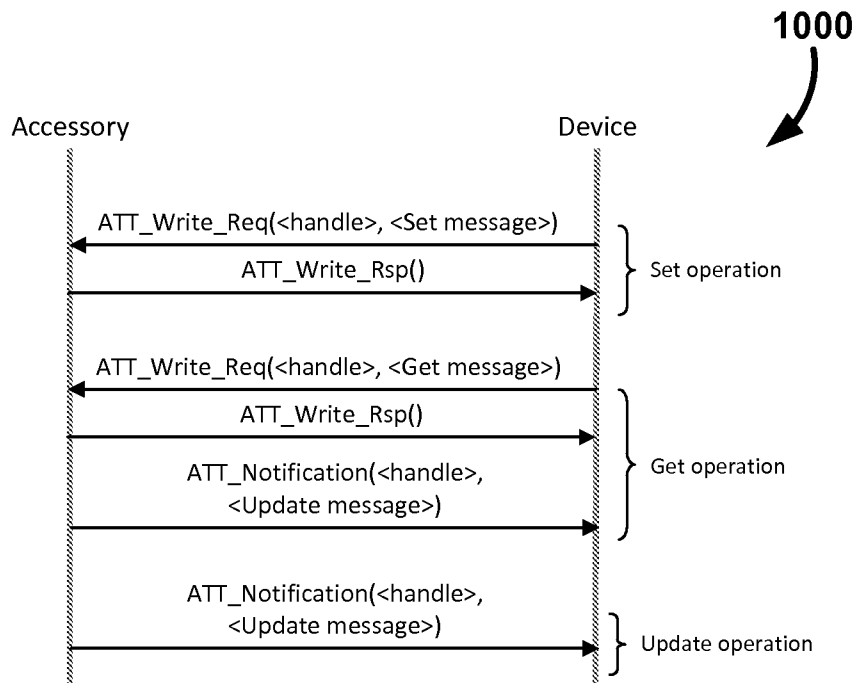


Fig. 10

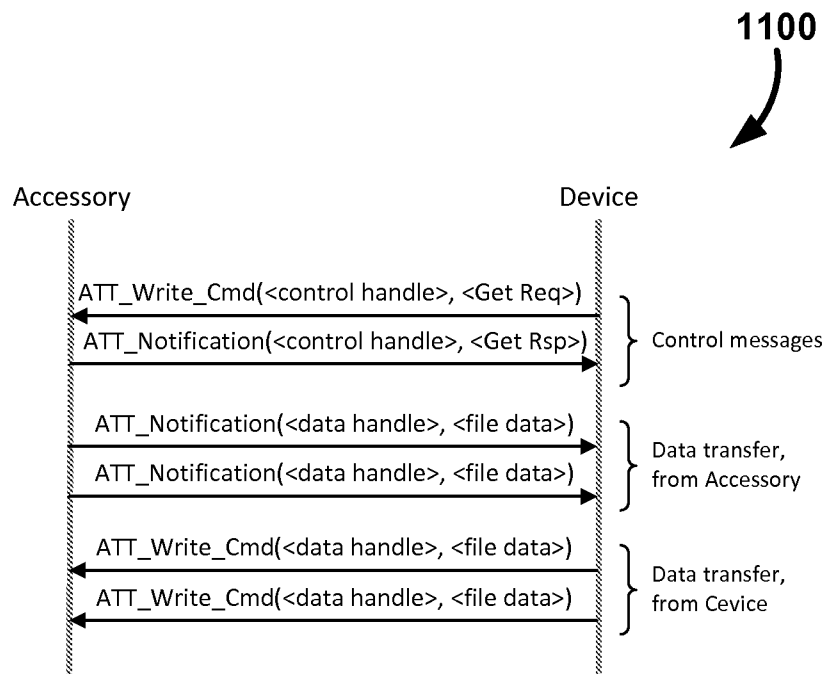


Fig. 11

11/13

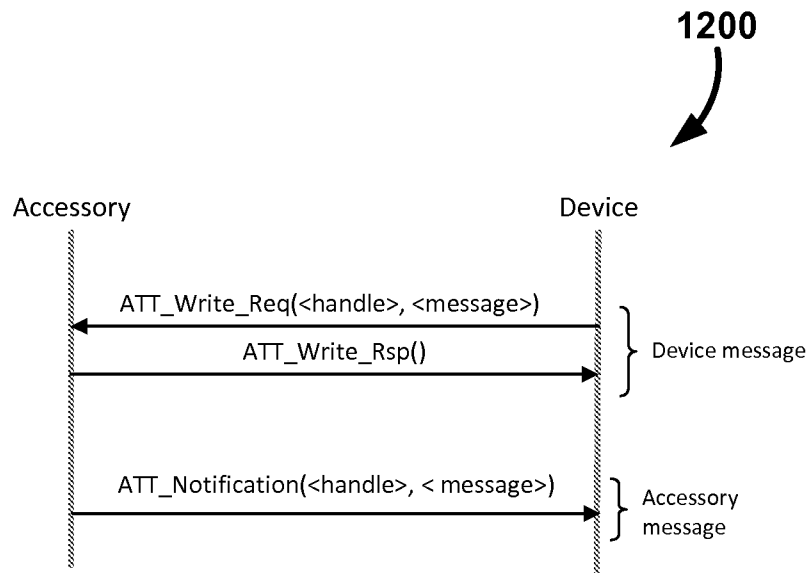


Fig. 12

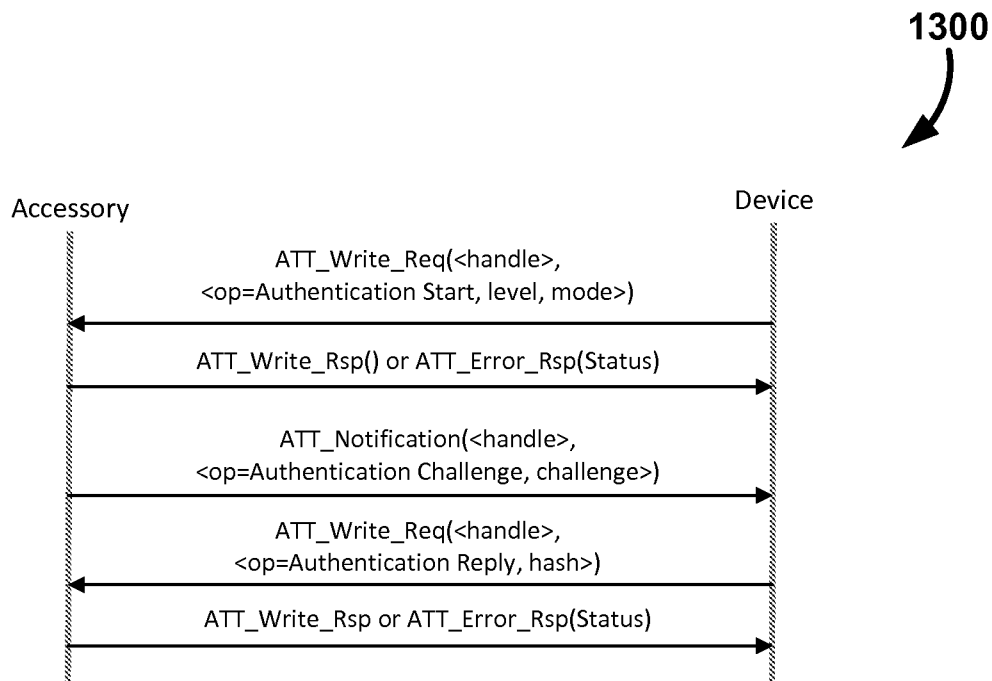


Fig. 13

12/13

1400

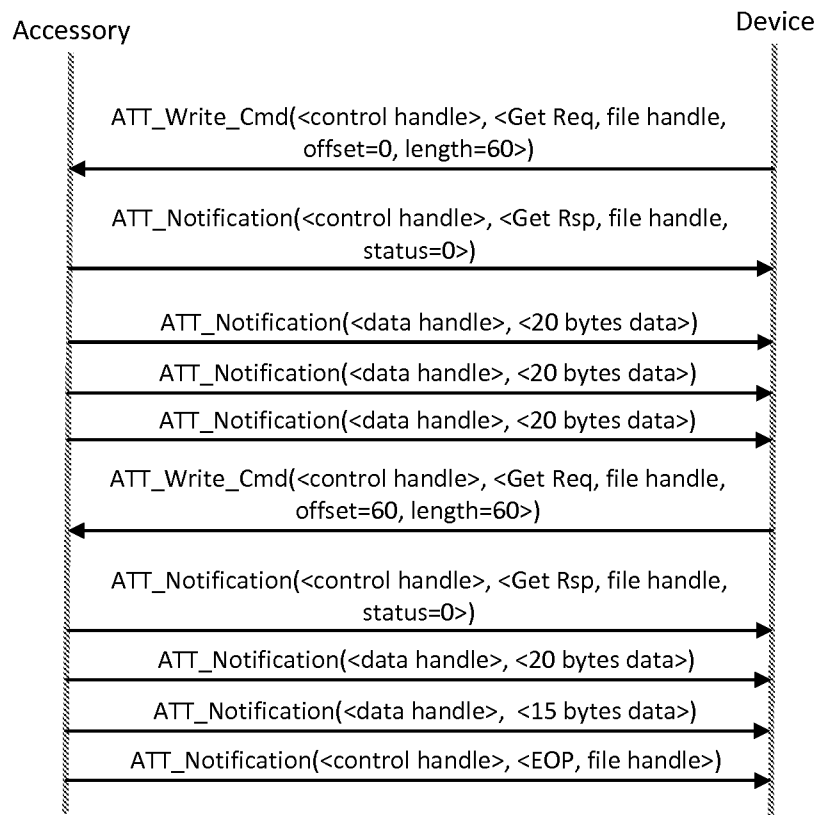


Fig. 14

13/13

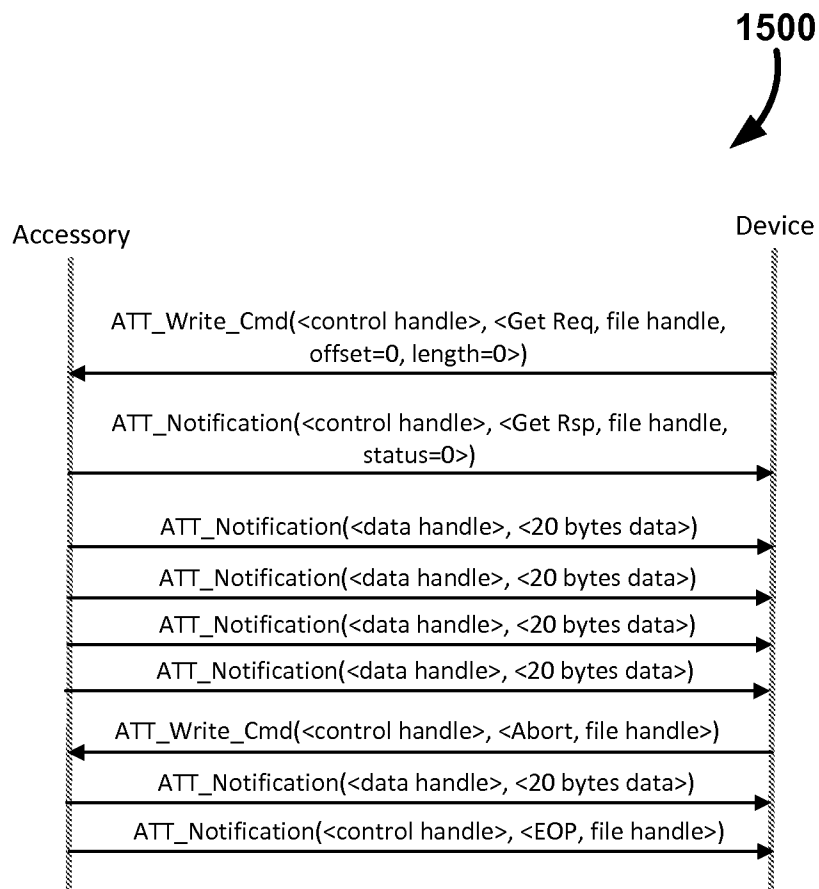


Fig. 15

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US 15/26043

A. CLASSIFICATION OF SUBJECT MATTER

IPC(8) - H04B 7/00, H04B 7/26 (2015.01)

CPC - H04W 84/18, H04M 1/7253, H04W88/06

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)

IPC(8)-H04B 7/00, H04B 7/26 (2015.01); CPC-H04W 84/18, H04M 1/7253, H04W88/06; USPC- 455/41.1, 41.2,41.3; 726/1, 2, 5;

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

CPC-H04M 2250/02, H04W76/02, H04L9/3236G06K19/0723, G06K7/0008, G06F21/6218; IPC(8)-H04B5/00, G06F7/04, G06F17/00, G06F17/30 (2015.01)

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

PatBase, Google Patents/Scholars: terms-BLE bluetooth low energy accessory application authentication file data transfer mobile device smartphone PDA telephone iphone application level control message update/security/service change request

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2010/0178871 A1 (House) 15 July 2010 (15.07.2010), para [0005]-[0034]; figs. 1-5.	13-24
Y	US 2013/0017816 A1 (Talty et al.) 17 January 2013 (17.01.2013), entire document, especially para [0007]-[0017]	1-9
Y	US 2014/0020073 A1 (Ronda et al.) 16 January 2014 (16.01.2014), entire document, especially para [0007]-[0132]	1-9
Y	US 2010/0088297 A1 (Killerich et al.), 8 April 2010 (08.04.2010), entire document, especially para [0022]-[0057]	2
Y	US 7,133,897 B1 (Tran) 7 November 2006 (07.11.2006), entire document, especially col 1, ln 59-col 5, ln 62	4-6, 8
A	WO 2013/006315 A1 (Sylvain et al.) 10 January 2013 (10.01.2013), entire document.	1-9
A	US 2013/0145057 A1 (Rathi et al.) 06 June 2013 (06.06.2013), entire document.	1-9
A	US 2011/0313922 A1 (Ben Ayed) 22 December 2011 (22.12.2011), entire document.	1-9

☐ Further documents are listed in the continuation of Box C.

* 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

26 August 2015 (26.08.2015)

Date of mailing of the international search report

21 SEP 2015

Name and mailing address of the ISA/US

Mail Stop PCT, Attn: ISA/US, Commissioner for Patents
P.O. Box 1450, Alexandria, Virginia 22313-1450

Facsimile No. 571-273-8300

Authorized officer:

Lee W. Young

PCT Helpdesk: 571-272-4300

PCT OSP: 571-272-7774

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US 15/26043

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

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

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

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

This International Searching Authority found multiple inventions in this international application, as follows:
This application contains the following inventions or groups of inventions that are not so linked as to form a single general inventive concept under PCT Rule 13.1. In order for all inventions to be searched, the appropriate additional search fees must be paid.

Group I: Claims 1-9 directed to a method for application level authentication, useful in conjunction with a low energy Bluetooth device and accessory.

Group II: Claims 10-12 directed to a method for over-the-air firmware updates, useful in conjunction with a low energy Bluetooth device and accessory.

Group III: Claims 13-24 directed to a method for device control, useful in conjunction with a low energy Bluetooth device and accessory.

---see extra sheet---

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.
2. ☐ As all searchable claims could be searched without effort justifying additional fees, this Authority did not invite payment of additional fees.
3. ☒ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:
1-9, 13-24
4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

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

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US 15/26043

Continuation of Box No. III:

The inventions listed as Groups I-III do not relate to a single general inventive concept under PCT Rule 13.1 because, under PCT Rule 13.2, they lack the same or corresponding special technical features for the following reasons:

Group I includes the special technical feature of receiving accessory credentials from a server; establishing a Bluetooth low energy connection with the accessory; authenticating with the accessory; and transferring data to the accessory, not required by groups II-III.

Group II includes the special technical feature of reading accessory information; initiating a diagnostic mode in the accessory; transferring firmware update data to the accessory; verifying the data transfer; and disconnecting from the accessory, wherein the disconnection triggers a reset of the accessory, not required by groups I and III.

Group III includes the special technical feature of sending a device control message from a device application to an accessory application; and receiving a response, at the device application, for the control message, not required by groups I-II.

The only feature shared by Groups I through III that would otherwise unify the groups, is the low energy Bluetooth device. However, this shared technical feature does not represent a contribution over prior art, because the shared technical feature is anticipated by US 2013/0017816 A1 to Talty et al. dated 17 January 2013 (hereinafter Talty) which teaches a low energy Bluetooth device (abstract and para [0006], Bluetooth low energy master communication device). As the technical feature was known in the art at the time of the invention, this cannot be considered a special technical feature that would otherwise unify the groups.

The only feature shared by Groups I through II that would otherwise unify the groups, is the authentication and transferring data. However, this shared technical feature does not represent a contribution over prior art, because the shared technical feature is anticipated by Talty which teaches authentication (Claim 2 authenticated for communication) and transferring data (para [0017] transferring data). As the technical feature was known in the art at the time of the invention, this cannot be considered a special technical feature that would otherwise unify the groups.

Therefore, Groups I-III lack unity under PCT Rule 13 because they do not share a same or corresponding special technical feature.