(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
26 July 2018 (26.07.2018)

WIPO | PCT

(10) International Publication Number
WO 2018/136260 A1

(51) International Patent Classification:
G07C 9/00 (2006.01) *H04W 12/04* (2009.01)
H04H 60/91 (2008.01) *H04W 12/06* (2009.01)
H04L 29/06 (2006.01) *H04W 92/04* (2009.01)
H04L 29/08 (2006.01) *H04W 92/10* (2009.01)

(21) International Application Number:
PCT/US2018/012947

(22) International Filing Date:
09 January 2018 (09.01.2018)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
15/412,321 23 January 2017 (23.01.2017) US

(63) Related by continuation (CON) or continuation-in-part (CIP) to earlier application:
US 15/412,321 (CIP)
Filed on 23 January 2017 (23.01.2017)

(71) Applicant: **USCONTRACTING, INC.** [US/US]; 1410 Annapolis Rd., Odenton, Maryland 21113 (US).

(72) Inventors: **HAWORTH, William Frederick**; 246 Nottingham Hill, Sherwood Forest, Maryland 21405 (US). **MAYNARD, Kevin Austin**; 905 Saint Claire Ct, Annapolis, Maryland 21409 (US). **KIDWELL, Jeffrey Brader**; 2141 Lovepoint Rd, Stevensville, Maryland 21666 (US).

(74) Agent: **GEORGE, JiNan Glasgow**; PO Box 52546, Durham, North Carolina 27717 (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,

(54) Title: SYSTEMS AND METHODS FOR LOCATION-BASED AUTOMATED AUTHENTICATION

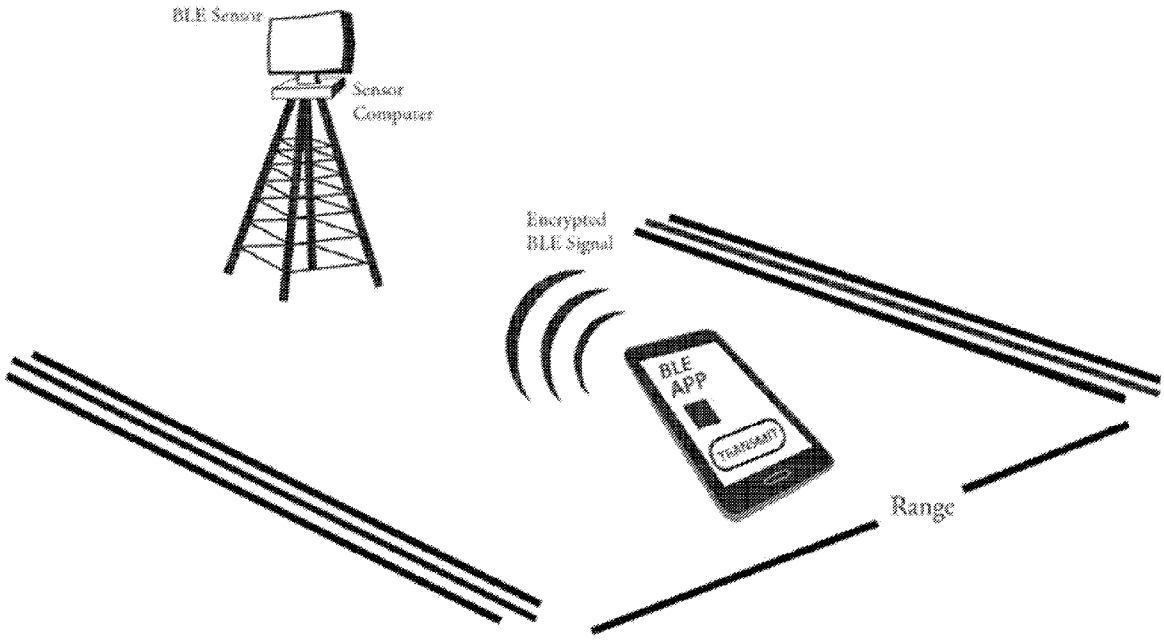

FIG. 1

(57) Abstract: Systems and methods for location-based automated authentication are disclosed. A system comprises a mobile device, a sensor and a backend platform. The sensor and the backend platform is in network communication. The mobile device is operable to continuously transmit Bluetooth Low Energy (BLE) signals comprising encrypted transitory identifiers. The sensor is operable to receive a BLE signal from the mobile device when the mobile device is within a predetermined range, and communicate over a network connection the encrypted transitory identifier comprised in the BLE signal to the backend platform. The backend platform is operable to extract a unique identifier and a changing encrypted identifier from the received encrypted transitory identifier, generate a changing encrypted identifier, and validate a user identification by comparing the generated changing encrypted identifier and the extracted encrypted transitory identifier.

WO 2018/136260 A1

[Continued on next page]

CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, 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, 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).

Declarations under Rule 4.17:

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*

— *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii))*

Published:

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

— *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))*

SYSTEMS AND METHODS FOR LOCATION-BASED AUTOMATED AUTHENTICATION

CROSS REFERENCES TO RELATED APPLICATIONS

[0001] This application relates to and claims priority from the following applications. This application claims priority from U.S. Application No. 15/412,321 filed January 23, 2017, which is incorporated herein by reference in its entirety.

BACKGROUND OF THE INVENTION

1. Field of the Invention

[0002] The invention relates to location-based automated authentication.

2. Description of the Prior Art

[0003] Personal mobile devices, especially smart phones, become so popular that almost everyone has one with them wherever they are. Modern communication technologies and various mobile applications have equipped smart phones with a variety of functions besides basic calling and texting. As one example, mobile devices are used for access authentication and validation.

[0004] By way of example the following are relevant prior art documents relating to access authentication and validation:

[0005] U.S. Patent Publication No. 20100201536 for "System and method for accessing a structure using a mobile device" by inventor William Benjamin Robertson *et al.*, filed February 10, 2009, describes a wireless device access system employs short-range wireless communication to detect the proximity of a user device to a structure and a wide-area data network to communicate an unlock request. The access system then authenticates the unlock request and the proximity of the user device prior to transmitting an unlock command to the structure. Additionally, the wireless device may require the proximity of a user token prior to operation and/or the access system may include an override within the structure blocking any

unlock command. Besides providing access to the structure, the system may perform other functions, such as monitoring room occupancy, switching power on and off, and the like.

[0006] U.S. Patent Publication No. 20130257589 for "Access control using an electronic lock employing short range communication with mobile device" by inventor Mohammad Mohiuddin *et al.*, filed March 01, 2013, describes systems and methods for obtaining access to an area or an object secured by an electronic locking device. The methods involve: obtaining, by a Mobile Communication Device ("MCD"), a unique identifier associated with the Electronic Locking Device ("ELD")via a first Short Range Communication ("SRC"); communicating the unique identifier from MCD to a Remote Communication Device ("RCD") via a network connection; receiving at least one symbol associated with the unique identifier that facilitates unlocking of ELD from RCD via the network connection; and causing ELD to be unlocked by communicating a key from MCD to ELD via a second SRC.

[0007] U.S. Patent Publication No. 20140220883 for "Presence Detection Using Bluetooth and Hybrid-Mode Transmitters" by inventor Aaron T. Emigh *et al.*, filed February 4, 2014, describes presence detection using Bluetooth and hybrid-mode transmitters. In some embodiments, one or more transmitters are configured to transmit an iBeacon broadcast and a proprietary Bluetooth Low Energy (BTLE) broadcast, wherein at least one of the transmitted broadcasts includes an identifier that specifies a venue. The broadcasts are captured by a handset and decoded to infer presence of the handset at the venue.

[0008] U.S. Patent Publication No. 20140375421 for "Systems and methods for enabling access control via mobile devices" by inventor John David Morrison *et al.*, filed June 18, 2014, describes systems and methods for enabling access control via mobile devices. Embodiments of the invention have been particularly developed for allowing a user to gain access to a controlled functionality (for example the unlocking of a door) using a smartphone

or the like. These leverage short-range wireless communications, such as Bluetooth Low Energy or Near Field Communications.

[0009] U.S. Patent Publication No. 20160055693 for "Validation in secure short-distance-based communication and enforcement system according to visual objects" by inventor Avishek Somani *et al.*, filed June 18, 2015, describes a secure short-distance-based communication and enforcement system validates users in a validation and enforcement area and can check if users in the validation and enforcement area have been validated. A visual object can be displayed on an enforcement computer and a mobile device of a user in the in the validation and enforcement area to determine if a user is validated. The visual object may be periodically changed.

SUMMARY OF THE INVENTION

[0010] Systems and methods for location-based automated authentication are disclosed. A system comprises a mobile device, a sensor and a backend platform. The sensor and the backend platform are in network communication. The mobile device is operable to continuously transmit Bluetooth Low Energy (BLE) signals comprising encrypted transitory identifiers. The sensor is operable to receive a BLE signal from the mobile device when the mobile device is within a predetermined range, and transmit an encrypted transitory identifier comprised in the BLE signal to the backend platform. The backend platform is operable to extract a unique identifier and a changing encrypted identifier from the received encrypted transitory identifier, generate a changing encrypted identifier, and validate a user identification by comparing the generated changing encrypted identifier and the extracted encrypted transitory identifier. An associated mobile application is installed on the mobile device. The associated mobile application is activated and send user identification parameters to the backend platform. The mobile application and the backend platform use the same algorithm to generate changing encrypted identifiers.

[0011] These and other aspects of the present invention will become apparent to those skilled in the art after a reading of the following description of the preferred embodiment when considered with the drawings, as they support the claimed invention.

BRIEF DESCRIPTION OF THE DRAWINGS

[0012] FIG. 1 is a diagram of BLE transmission and range in one embodiment of the present invention.

[0013] FIG. 2 is a flowchart of the automated authentication process in one embodiment of the present invention.

[0014] FIG. 3 is a diagram of architecture data flow for the authentication process in one embodiment of the present invention.

[0015] FIG. 4 is an illustration of a toll lane use case in one embodiment of the present invention.

DETAILED DESCRIPTION

[0016] The present invention provides systems and methods for identifying and authenticating mobile devices in designated locations. A mobile device downloads and activates a mobile application ("app"), and provides identification information to be stored in the BAS. The mobile device then transmits Bluetooth Low Energy (BLE) signals containing encrypted identification information. A sensor receives the BLE signals when the mobile device is within range and communicates to a Backend Account System (BAS). The BAS validates and authenticates the user identification, corresponding functions and actions are executed, and a response is sent to the sensor. The mobile device receives the response from the backend system at a later point regarding the execution of the functions and/or actions. Additionally, the mobile device user can query for the history of transactions at any time.

[0017] The present invention is a Location-Based Automated Authentication System (LBAAS). The LBAAS involves a secure platform for identifying specific users in

designated geographic locations. In the present invention, an Encrypted Transitory Identifier (ETID) is transmitted via a BLE signal from a mobile device through a BLE sensor and into the BAS system; and the ETID is resolved at the BAS system into a Unique Identifier (UID) and Changing Encrypted Identifier (CEID) that are used to recognize and authenticate a user.

[0018] The ETID is a dynamic and temporary transmission from a user's mobile device. The Back-end Account System (BAS) uses a function in the form of $f_x(ETID)=UID + CEID$ to decode and translate a valid ETID into a static UID associated with a user and a CEID.

[0019] The entire LBAAS consists of three major components: a mobile application that broadcasts using BLE, a sensor, and a BAS. These components and their functions are described below in Table 1.

[0020] Table 1 - System Component Descriptions & Functions

Component	Composition	Function
Mobile Application	A software program running on a mobile device	Transmits ETID via BLE when activated by user
A sensor	A computer with an attached antenna capable of receiving BLE signals, strategically placed and calibrated based on system functions and requirements	Receives the BLE signals, decodes EITD, and communicates with the BAS
Back-end Account System (BAS)	A remote computer and data store	Stores user information needed by the system to perform its function; generates and stores a UID; resolves and validates the CEID from mobile device

[0021] In one embodiment, the sensor consists of a Linux based computer with an attached 2.4 GHz high-gain directional antenna. The sensor is in a ready state to collect input from an application running on a mobile device within its immediate vicinity. The mobile application is designed for devices that have Bluetooth 4.0, capable of emitting BLE signals. The BAS runs on a remote set of Linux based computers with sufficient capacity to handle many

concurrent lookups from multiple sensors. In one embodiment, the BAS is configured for a specific application, such as a toll gate scenario, on a platform tailored to system requirements. This can be one or more computers or on a cloud-based platform, which is able to host many different BAS systems for different applications.

[0022] All mobile devices are first registered in the BAS in order to identify and authenticate users. A user downloads and activates a mobile application to a mobile device, and provides identification information to be stored in the BAS. This identification information is used to create a UID as an index for the user. A Changing Time Interval (CTI) for the system is also saved to a user's account along with other account parameters and data to act as a seed in the creation of CEIDs on both the mobile device and the BAS.

[0023] FIG. 1 is a diagram of BLE transmission and range in one embodiment of the present invention. During a normal operation, the mobile application generates and transmits an ETID via BLE, and a sensor recognizes and reads BLE signals along with their corresponding signal strengths. The mobile device is within the detection rage of the sensor when a signal strength threshold is met. The sensor receives the emitted BLE signal, decodes the ETID, and passes it to the BAS for confirmation of a valid user. The BAS extracts a UID and CEID from the ETID, validate the user's identity, returns a response depending on the application to the sensor, and then performs other specific system functions and operations, e.g., billing, e-mail, text notifications to the originating mobile device, or generating system logs. If it is a valid user, a corresponding system function (e.g., raising a gate or activating a light) is executed and the response provides positive user feedback. If it is not a valid user, the response provides negative user feedback. FIG. 2 illustrates the Automated Authentication Process in one embodiment of the present invention. Feedback for unauthorized users on their mobile devices is limited based on whether they have active accounts in the BAS.

[0024] FIG. 3 illustrates a data flow architecture for user authentication.

[0025] When a user first downloads and opens the mobile application, they provide information to populate the BAS. There are a few other key parameters automatically collected or generated including a Changing Time Interval (CTI), an Original Account Timestamp (OAT), a Unique ID (UID), and Unique Encryption Key. These parameters are stored in both the BAS and the non-volatile memory of the mobile device; and are required to identify and authorize the particular mobile device in real time.

[0026] Once all the necessary parameters are created and stored, the authentication process begins when a user turns on the application and BLE signals are emitted from the mobile device. Preferably, a user verification step, for example, a pin, a fingerprint, or a voice password, is needed for turning on the mobile application for security purposes. For example, an application may require the use of verification for a limited time to prevent unauthorized use of the mobile device. The content of the BLE signal is generated from a series of proprietary steps that effectively provide a unique secure algorithm that runs in the background of the application. The OAT, CTI, and the Current Timestamp (CT) is used to calculate a value for user authentication. This value is then encrypted with an Advanced Encryption Standard (AES) algorithm using the Unique Encryption Key. The result is reduced into a usable size and known as the CEID. The CEID is then combined with the UID to create the ETID that is packaged and transmitted in a unique BLE signal. The present invention provides secure user identification transmission over BLE signals, because the CEIDs in the BLE signals change over time based on the algorithm used to create the CEIDs. This way, the BLE signals cannot be emulated, copied or replayed.

[0027] A calibrated BLE sensor reads BLE signals that are within range and translates the BLE signals from the mobile device into the ETID. The sensor then connects to the BAS to transfer the ETID.

[0028] The BAS extracts the UID from the ETID. The UID is used to look up the specific user parameters. The BAS performs the same algorithm as that of the mobile device, and generates a CEID using the CTI, the OAT, the CT, and the Unique Encryption Key. The BAS then compares the extracted CEID (from the ETID sent by the sensor) with the generated CEID to validate the user.

[0029] If the CEIDs match, the functions and/or actions of the system are carried out (e.g., flash an indicator or open a gate, and charging an account). If the values do not match, no further functions or actions are necessary. In either case, the BAS sends the successful or failed response back to the sensor so it may complete the transaction at the point of BLE reception.

[0030] The system in the present invention transforms an insecure open-source BLE format into a secure proprietary solution for automated transactions by the use of encryption, synchronous clocks, and highly sophisticated algorithms. With the unique security solution, the system is able to identify and authenticate users while preventing replay attacks. It is virtually impossible for someone to eavesdrop on someone else's BLE signal and retransmit the same signal.

[0031] Many mobile applications use BLE technology to scan for signals that trigger some other action. Typically, the mobile device is used as a scanner and not as a broadcaster. However, the present invention reverses the direction of the data flow. Instead of receiving signals, the mobile device in the present invention is broadcasting signals in the background of the phone with virtually no battery consumption. By reversing the data direction and using BLE, the architecture in the present invention has a relatively low impact on mobile device battery levels. BLE can be active for days without any substantial drain on battery resources. Mobile devices, for example mobile devices equipped with Bluetooth 4.0, Bluetooth 5.0 and later Bluetooth versions, are operable to transmit small amounts of data periodically with

very low power consumption using BLE functionality. In one embodiment of the present invention, BLE mobile devices broadcast ETIDs via BLE signals on the 2.4 GHZ bandwidth.

[0032] The BLE functionality works in two different modes, namely connected mode and advertising mode, which are utilized for different purposes. BLE mobile devices in the present invention preferably never operate in connected mode, and therefore never establish a communication connection with any other BLE devices. Never establishing a communication connection with any other BLE devices significantly reduces battery power consumption of the mobile device. In the present invention, BLE mobile devices transmit ETIDs in advertising mode. In one embodiment, a user is enabled to turn a BLE mobile device to a driving mode or standby mode so as to turn on or off the BLE advertising mode for ETID broadcasting. For example, a user gets into his/her car and turns his/her BLE mobile device to driving mode, and his/her mobile device starts emitting BLE signals including ETIDs. Once the user reaches his/her destination, he/she turns his/her BLE mobile device to standby mode, preferably by exiting driving mode, and the BLE mobile device stops transmitting BLE signals. In another embodiment, BLE mobile devices are operable to detect if the BLE mobile devices are in motion or stationary based on location services and related technologies. When a BLE mobile device detects itself in motion, the advertising mode is triggered and the mobile device starts transmitting BLE signals including ETIDs. When the BLE mobile device detects itself stationary for a predetermined time period, it stops transmitting BLE signals. In another alternative, the mobile device is operable to recognize that it is within a predetermined proximity of a vehicle or within the vehicle by receiving a BLE signal from the vehicle or any other method known in the art for a mobile device to recognize a presence of a vehicle and/or for a vehicle to recognize a presence of a mobile device, and the advertising mode is triggered so that the mobile device starts transmitting BLE signals including ETIDs.

[0033] The BLE functionality typically has four configurable frequency settings that affect ETID transmission rates. The actual frequency changes at the operating system level due to CPU activity of a device. If the CPU of a BLE mobile device is busy at the time the BLE mobile device is set in driving mode, the BLE mobile device transmits BLE signals slightly less frequently than when the CPU is idle. In one embodiment, the present invention utilizes the highest frequency setting for BLE transmissions to maintain reliability. The higher the frequency, the more BLE signals a BLE sensor collects while a BLE mobile device is within a certain distance of the BLE sensor. A high frequency setting is particularly important for BLE mobile devices in vehicles traveling at high speeds. For example, a vehicle traveling at 100 mph is only within the scanning range of a BLE sensor for a very brief time period. Higher BLE transmission frequency enables the BLE sensor to pick up more BLE signals as the vehicle travels at high speeds past the BLE sensor. In one embodiment, the BLE signal transmission frequency increases with the speed of a vehicle, with the speed being determined via a Global Positioning System (GPS) or any other technology for determining speed in real-time or near real-time. A lower BLE transmission frequency potentially causes a BLE sensor to miss BLE signals from a BLE mobile device as it passes at a high speed. Higher BLE transmission frequency provides lower latency and better reliability but with more battery consumption. In one embodiment, the BLE transmission frequency is set at 10 Hz, and the ETID transmission rate is about 10 Hz or 10 ETIDs per second. Frequency deviations are about 1-3 Hz due to CPU activities of a BLE mobile device when BLE signals transmitted from the BLE mobile device are received by a BLE sensor.

[0034] In the present invention, there is no initiation by the mobile device for communication with a computer system in order to exchange messages for authentication, and there is no connection needed between the mobile device and the BAS to complete a transaction. The mobile device merely emits BLE signals comprising ETIDs generated from CEIDs. Once the

sensor receives the BLE signals, the authentication process is done between the sensor and the BAS.

[0035] The unique broadcasting feature also enables the application to perform with very little network connection. A network is only needed during registration to connect the mobile device to the BAS. Once this information is recorded, the Automated Authentication Process is performed without network connection between the mobile device and the BAS. The receiving device is a stationary sensor which can be attached to a constant power source and handle all networking requirements. In other words, the mobile device merely emits BLE signals and the identification and authentication are performed on the sensor and the BAS.

[0036] The mobile device application and the BAS are highly customizable. The area within which a sensor will detect a BLE signal and the signal strength required to trigger the user authentication can be adjusted to meet requirements of different applications and/or tasks. Sensors can also be placed in a variety of different locations. Possible applications include: tolls, gates, entrances, garages, boat lifts, ski lifts, etc.

[0037] The present invention is applicable to places where Radio Frequency Identification (RFID) or Near Field Communication (NFC) technologies are used for identification authentication and validation. The encrypted BLE transmission by mobile devices in the present invention provides a comparably secure and more convenient mechanism for user identification. The use of both one-way identification and processing application on a single user device makes this a more convenient platform for user validation.

[0038] Use Case 1: Toll Collection

[0039] In one embodiment, the use of BLE enables a secure low energy solution for toll collection systems as shown in FIG. 4.

[0040] During a preliminary phase, BAS data requirements are defined and then the BAS is set up with a network connection; sensors are installed, calibrated, and connected to given toll

locations; and users download an app to their mobile devices and enter all required account information. Changing Time Interval, Original Timestamp, UID, Unique Encryption Key are automatically generated and saved to the user system account. Users provide credit card or bank information, billing addresses, valid vehicle plate numbers, and other personal information.

[0041] During an execution phase, a user gets in the car and turns on the application on his mobile device. The application generates a CEID using a secure algorithm and combines the CEID with the user's UID to create an ETID. The ETID is packaged and broadcast via a BLE signal. The BLE signal is continuous, but the ETID being broadcast changes based on the defined Changing Time Interval. As the car approaches the toll booth, the toll booth sensor starts to receive the BLE transmission. The mobile device is within range when a predetermined signal strength threshold is met. The toll booth sensor reads the BLE signal and translates it into the ETID. The toll booth sensor connects to the BAS and sends the ETID. The BAS receives the ETID and separates it into the UID and CEID. The BAS looks up the user system account using the UID separated from the received ETID. The parameters saved to the user system account within the BAS, including Changing Time Interval, Original Timestamp, UID, and Unique Encryption Key, are used to synthesize a CEID with the same algorithm used by the mobile device application. The BAS compares the synthesized CEID to the one received from the mobile device (via BLE and the toll booth sensor). If the CEIDs match, a license plate photo is taken for secondary verification; the user credit card or bank account is charged; a log or invoice is generated and sent to the user's mobile applications; and the light on the toll booth turns green. If the CEIDs do not match, a license plate photo could be taken for secondary verification or ticketing. For further integration, if the plate photo is verified and the account is charged, a log is generated and sent to the application to

notify the user that the account was successfully charged, and the light on the toll booth turns green. If the plate photo is not verified, the light on the toll booth turns red.

[0042] Use Case 2: Gated Entrance Admission

[0043] In one embodiment, the present invention is used for admitting to gated facilities, for example, a gated neighborhood, a garage, an entrance to a factory or other facilities, etc. A BAS is set up with specific data requirements for gated entrance admission. A gate sensor at the gated entrance is installed, calibrated and connected to the BAS in network communication. Authorized users download an app to their mobile devices and enter all required information. For example, authorized license plate numbers, authorized user names, work identifications, phone numbers, and other personal information for people who are authorized to enter a gated facility. Changing Time Interval, Original Timestamp, UID, Unique Encryption Key are automatically generated and saved to corresponding user system accounts.

[0044] A user turns on the app on his mobile device. The app generates a CEID using a secure algorithm and combines the CEID with the user's UID to generate an ETID. The ETID is packaged and broadcast via a BLE signal. The BLE signal is continuous, but the ETID changes based on the defined Changing Time Interval. As the user approaches the gated entrance, the gate sensor starts to receive the BLE transmission. The mobile device is within range when a predetermined signal strength threshold is met. The gate sensor reads the BLE signal and translates it into the ETID. The gate sensor then sends the ETID to the BAS. The BAS receives the ETID and separates it into the UID and CEID. The BAS looks up the user system account using the UID separated from the received ETID. The parameters saved to the user system account within the BAS, including Changing Time Interval, Original Timestamp, UID, and Unique Encryption Key, are used to synthesize a CEID with the same algorithm used by the mobile device application. The BAS compares the synthesized CEID to

the one received from the mobile device (via BLE and the gate sensor). If the CEIDs match, a gate light turns green and the gate is open for the user automatically; and the user may receive a notification on the mobile device regarding the admission at a later time. If the CEIDs do not match, the gate light turns red and the gate keeps closed, and the user receives a notification for denial.

[0045] Use Case 3: Employee Access

[0046] In one embodiment, the present invention is used for employee access authentication. For example, in a large company campus, there are different departments, usually employees are only authorized to enter the department they work at and public space, only certain employees such as high-level management personnel can access to multiple departments. For example, only laboratory staff and executives are allowed to enter a certain laboratory. A BAS is set up with specific data requirements for the laboratory entrance. A sensor at the entrance is installed, calibrated and connected to the BAS in network communication. Authorized employees download a mobile app to their mobile devices and enter all required information. For example, work identifications, employee names, phone numbers, and other employment related data for employees who are authorized to enter the laboratory. Changing Time Interval, Original Timestamp, UID, Unique Encryption Key are automatically generated and saved to the corresponding employee system accounts on both the mobile app and the BAS.

[0047] An employee turns on the app on his mobile device. At this point, the application may request a fingerprint scan to verify user identity. The fingerprint can be sent to the BAS to verify the user identity for a defined short interval. This activity will essentially authenticate the holder of the device as the individual authorized for entrance. The app generates a CEID using a secure algorithm and combines the CEID with the employee's UID to generate an ETID. The ETID is packaged and broadcast via a BLE signal. The BLE signal

is continuous, but the ETID changes based on the defined Changing Time Interval. As the employee approaches the entrance to the laboratory, the sensor at the entrance of the laboratory starts to receive the BLE transmission. The mobile device is with range when a predetermined signal strength threshold is met. The sensor reads the BLE signal and translates it into the ETID. The sensor then sends the ETID to the BAS. The BAS receives the ETID and separates it into the UID and CEID. The BAS looks up the employee system account using the UID separated from the received ETID. The parameters saved to the employee system account within the BAS, including Changing Time Internal, Original Timestamp, UID, and Unique Encryption Key, are used to synthesize a CEID with the same algorithm used by the mobile app. The BAS compares the synthesized CEID to the one received from the mobile device (via BLE and the sensor). If the CEIDs match, the entrance is unlocked and open for the employee automatically; and the employee receives a notification for successful admission. If the CEIDs do not match, the entrance keeps locked and closed, and the employee receives a notification for denial.

[0048] Such an employee access authorization system provides security and convenience for employee access, especially when an employee approaches to an entrance to his department with his hands full. The employee does not have to try to free up his hands for keying in a password or swiping a card or tapping a card in order to unlock and open the door, as along as the mobile application described in the present invention is turned on, the entrance is unlocked and open automatically once the employee gets to the proximity of the entrance and his identification is verified by the system as described above.

[0049] User Case 4: Loyalty Identification Recognition

[0050] In one embodiment, the present invention is used for presenting loyalty identification and making payment at a retail store. For example, a grocery store has its mobile application and the location-based automated authorization function is incorporated into the grocery store

mobile app. A BAS is set up with specific data requirements for recognizing loyalty identification and making payment. At least one point of sale (POS) station is calibrated to receive BLE signals and connected to the BAS in network communication. Customers in the store loyalty program download the store app to their mobile devices and enter all required information. For example, customer names, phone numbers, member identification numbers, bank account information, billing addresses, and other associated information. Changing Time Interval, Original Timestamp, UID, Unique Encryption Key are automatically generated and saved to corresponding loyalty system accounts.

[0051] A loyalty member turns on the store app on his mobile device. The store app generates a CEID using a secure algorithm and combines the CEID with the user's UID to generate an ETID. The ETID is packaged and broadcast via a BLE signal. The BLE signal is continuous, but the ETID changes based on the defined Changing Time Interval. As the loyalty member scans items in the cart at a POS station, the POS station starts to receive the BLE transmission. The mobile device is within range when a predetermined signal strength threshold is met. The POS station reads the BLE signal and translates it into the ETID. The POS station then sends the ETID to the BAS. The BAS receives the ETID and separates into the UID and CEID. The BAS looks up the loyalty system account using the UID separated from the received ETID. Parameters saved to the loyalty system account within the BAS, including Changing Time Interval, Original Timestamp, UID, and Unique Encryption Key, are used to synthesize a CEID with the same algorithm used by the store app. The BAS compares the synthesized CEID to the one received from the mobile device (via BLE and the point of sale station). If the CEIDs match, loyalty points and/or discounts are applied, the loyalty member's credit card or bank account is charged and a receipt is generated and sent to the loyalty member's store app automatically when the customer is ready to check out. If the CEIDs do not match, the customer is asked to provide other types of payment to check out.

[0052] Customers do not have to carry their credit cards and debit cards and membership cards and coupons and other physical payment mediums in a physical wallet when they shop in a store. A store app integrated with the location-based automatic authentication in the present invention enables a secure and convenient mobile payment for in-store shopping.

[0053] Certain modifications and improvements will occur to those skilled in the art upon a reading of the foregoing description. The above-mentioned examples are provided to serve the purpose of clarifying the aspects of the invention and it will be apparent to one skilled in the art that they do not serve to limit the scope of the invention. All modifications and improvements have been deleted herein for the sake of conciseness and readability but are properly within the scope of the present invention.

CLAIMS

The invention claimed is:

1. A system for location-based automated authentication, comprising:

a user device, a sensor and a backend platform;

wherein the sensor and the backend platform are in network communication;

wherein the user device is operable to construct a Bluetooth Low Energy (BLE) signal through:

constructing a unique value based on an original account timestamp, a changing time interval, and a current timestamp;

encrypting the unique value with a unique encryption key and compressing the encrypted unique value to derive a changing encrypted identifier, wherein the changing encrypted identifier changes based on the changing time interval;

combining the changing encrypted identifier with a unique identifier to form an encrypted transitory identifier;

packaging the encrypted transitory identifier into the BLE signal;

wherein the user device is operable to continuously transmit the BLE signal comprising the encrypted transitory identifier;

wherein the sensor is operable to receive the BLE signal from the user device when the user device is within a predetermined range, and transmit the encrypted transitory identifier comprised in the BLE signal to the backend platform;

wherein the backend platform is operable to:

extract the unique identifier and the changing encrypted identifier from the received encrypted transitory identifier;

retrieve user identification parameters based on the unique identifier, wherein the user identification parameters include the original account timestamp, the changing

time interval, the current timestamp, and the unique encryption key;

construct a second unique value based on the user identification parameters;

encrypt the second unique value with the unique encryption key and compress the encrypted second unique value to derive a second changing encrypted identifier;

validate a user identification by comparing the second changing encrypted identifier and the extracted changing encrypted identifier;

charge a user account according to a predefined amount upon validating the user identification; and

generate and store a log of charges and send a charge notification to the user device.

2. The system of claim 1, wherein the user device is further operable to download and activate an application program and send the user identification parameters to the backend platform through the application program.

3. The system of claim 2, wherein the backend platform is further operable to store the user identification parameters in the user account.

4. The system of claim 2, wherein the user identification parameters further comprise at least one from the group consisting of user names, phone numbers, work identification numbers, member identification numbers, financial account information, billing information and other personal information.

5. The system of claim 1, wherein the user device is operable to continuously transmit the BLE signal comprising the encrypted transitory identifier via a broadcast in BLE advertising mode.

6. The system of claim 1, wherein a BLE connection is never established between the user device and the sensor and a BLE connection is never established between the user device and the backend platform.

7. The system of claim 1, wherein the user device is operable to continuously transmit the

BLE signal comprising the encrypted transitory identifier approximately ten times per second.

8. The system of claim 1, wherein the predetermined range is defined based on a signal strength threshold.

9. The system of claim 1, wherein the user device and the backend platform have the same algorithm for generating the changing encrypted identifier and the second changing encrypted identifier.

10. The system of claim 1, wherein the user identification is validated when the second changing encrypted identifier and the extracted changing encrypted identifier match.

11. The system of claim 10, wherein the backend platform is further operable to execute an action when the user identification is validated.

12. The system of claim 1, wherein the backend platform is further operable to send a notification to the sensor regarding a validation result.

13. The system of claim 12, wherein the user device is further operable to receive the notification from the backend platform.

14. A method for location-based automated authentication, comprising:

a user device constructing a unique value based on an original account timestamp, a changing time interval, and a current timestamp;

the user device encrypting the unique value with a unique encryption key and compressing the encrypted unique value to derive a changing encrypted identifier, wherein the changing encrypted identifier changes based on the changing time interval;

the user device combining the changing encrypted identifier with a unique identifier to form an encrypted transitory identifier;

the user device packaging the encrypted transitory identifier into a Bluetooth Low Energy

(BLE) signal;

the user device continuously transmitting the BLE;

a sensor receiving the BLE signal when the user device is within a predetermined range;

the sensor communicating the encrypted transitory identifier comprised in the BLE signal to a backend platform via network communication;

the backend platform receiving the encrypted transitory identifier;

the backend platform extracting the unique identifier and the changing encrypted identifier from the received encrypted transitory identifier;

the backend platform retrieving user identification parameters based on the unique identifier, including the original account timestamp, the changing time interval, the current timestamp, and the unique encryption key and constructing a second unique value based on the user identification parameters;

the backend platform encrypting the second unique value with the unique encryption key and compressing the encrypted second unique value to derive a second changing encrypted identifier;

the backend platform validating a user identification by comparing the second changing encrypted identifier and the extracted changing encrypted identifier; and

the backend platform providing a visual indication of a successful validation or an unsuccessful validation.

15. The method of claim 14, further comprising the user device downloading and activating an application program and sending the user identification parameters to the backend platform through the application program.

16. The method of claim 15, further comprising the backend platform storing the user identification parameters in a user account.

17. The method of claim 14, further comprising the backend platform executing an action

when the second changing encrypted identifier and the extracted changing encrypted identifier match.

18. The method of claim 14, further comprising the backend platform sending a notification to the sensor regarding a result of the validation, and the user device receiving the notification from the backend platform.

19. A system for location-based automated authentication, comprising:

a user device, a sensor and a backend platform;

wherein the sensor and the backend platform are in network communication;

wherein the user device is operable to continuously transmit a Bluetooth Low Energy (BLE) signal comprising an encrypted transitory identifier via a broadcast in BLE advertising mode;

wherein the sensor is operable to receive the BLE signal from the user device when the user device is within a predetermined range, and transmit the encrypted transitory identifier comprised in the BLE signal to the backend platform;

wherein the backend platform is operable to extract a unique identifier and a changing encrypted identifier from the received encrypted transitory identifier, generate a changing encrypted identifier based on user identification parameters associated with the extracted unique identifier, and validate a user identification by comparing the generated changing encrypted identifier and the extracted encrypted transitory identifier; and

wherein a BLE connection is never established between the user device and the sensor and a BLE connection is never established between the user device and the backend platform.

20. The system of claim 19, wherein the user device transmits the BLE signal comprising the encrypted transitory identifier at about 10 Hz.

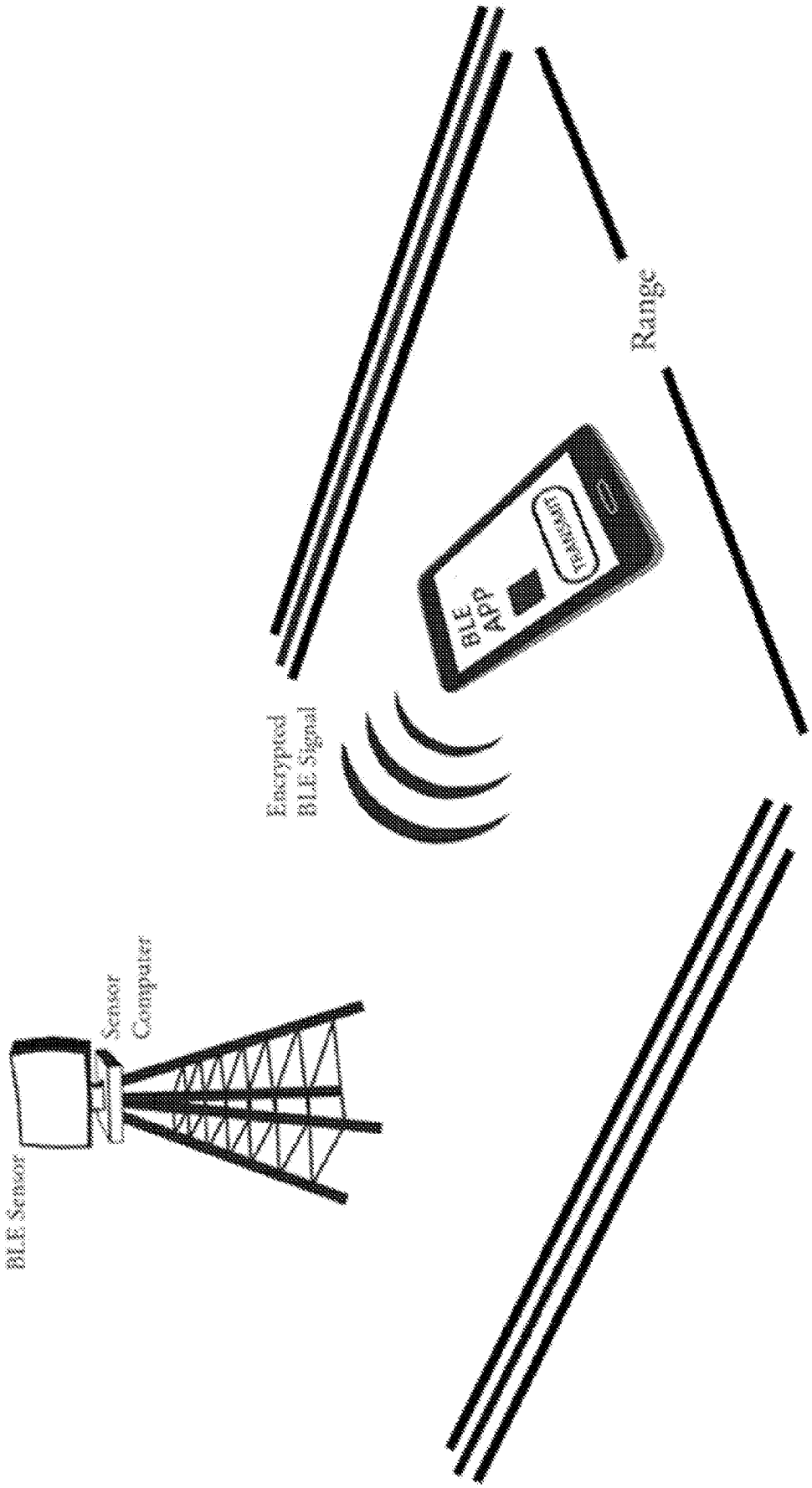
Range
BLE APP
Encrypted BLE Signal
Sensor Computer
BLE Sensor

FIG. 1

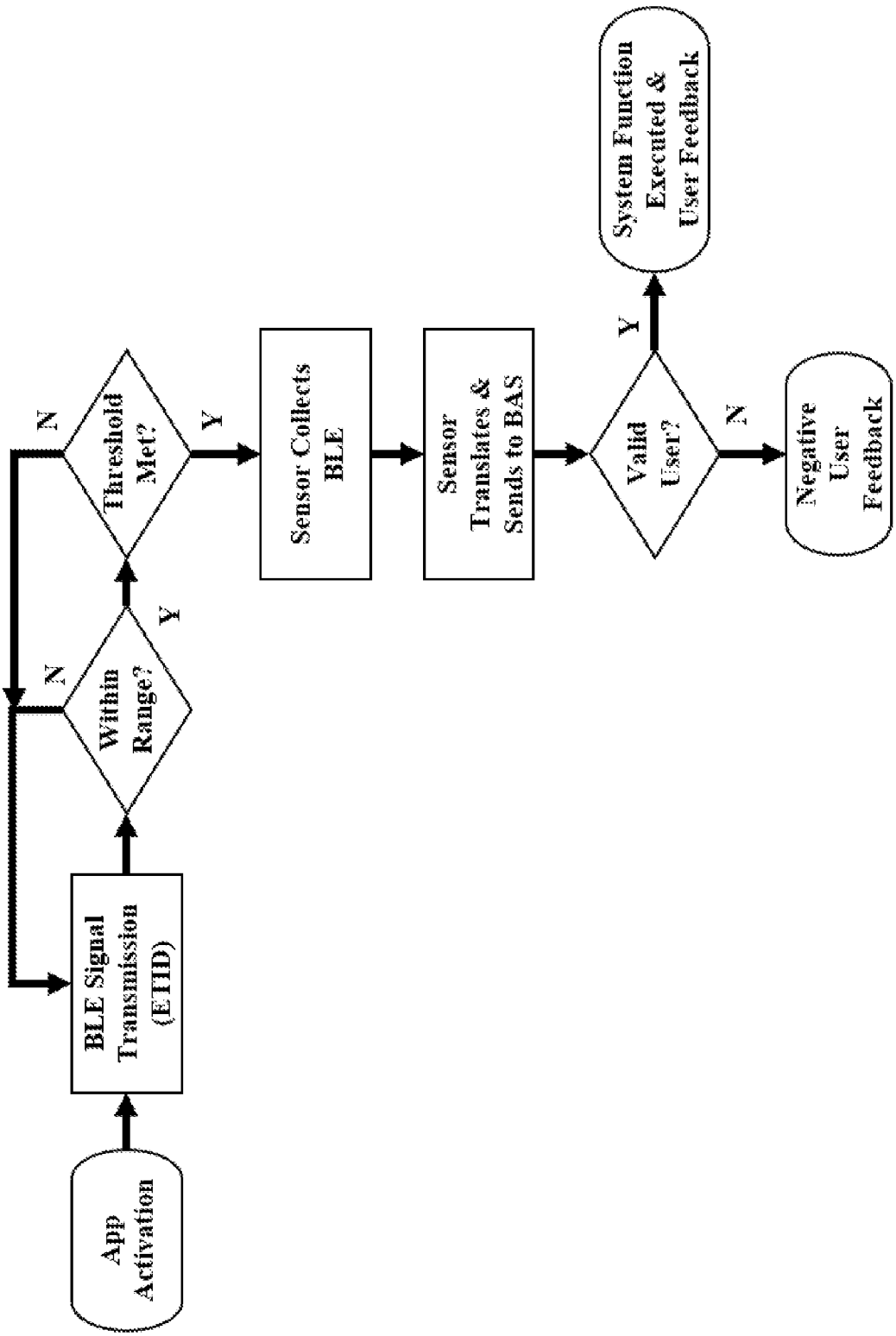
App Activation
BLE Signal Transmission (ETID)
Within Range?
N
Y
Threshold Met?
N
Y
Sensor Collects BLE
Sensor Translates & Sends to BAS
Valid User?
Y
N
System Function Executed & User Feedback
Negative User Feedback

FIG. 2

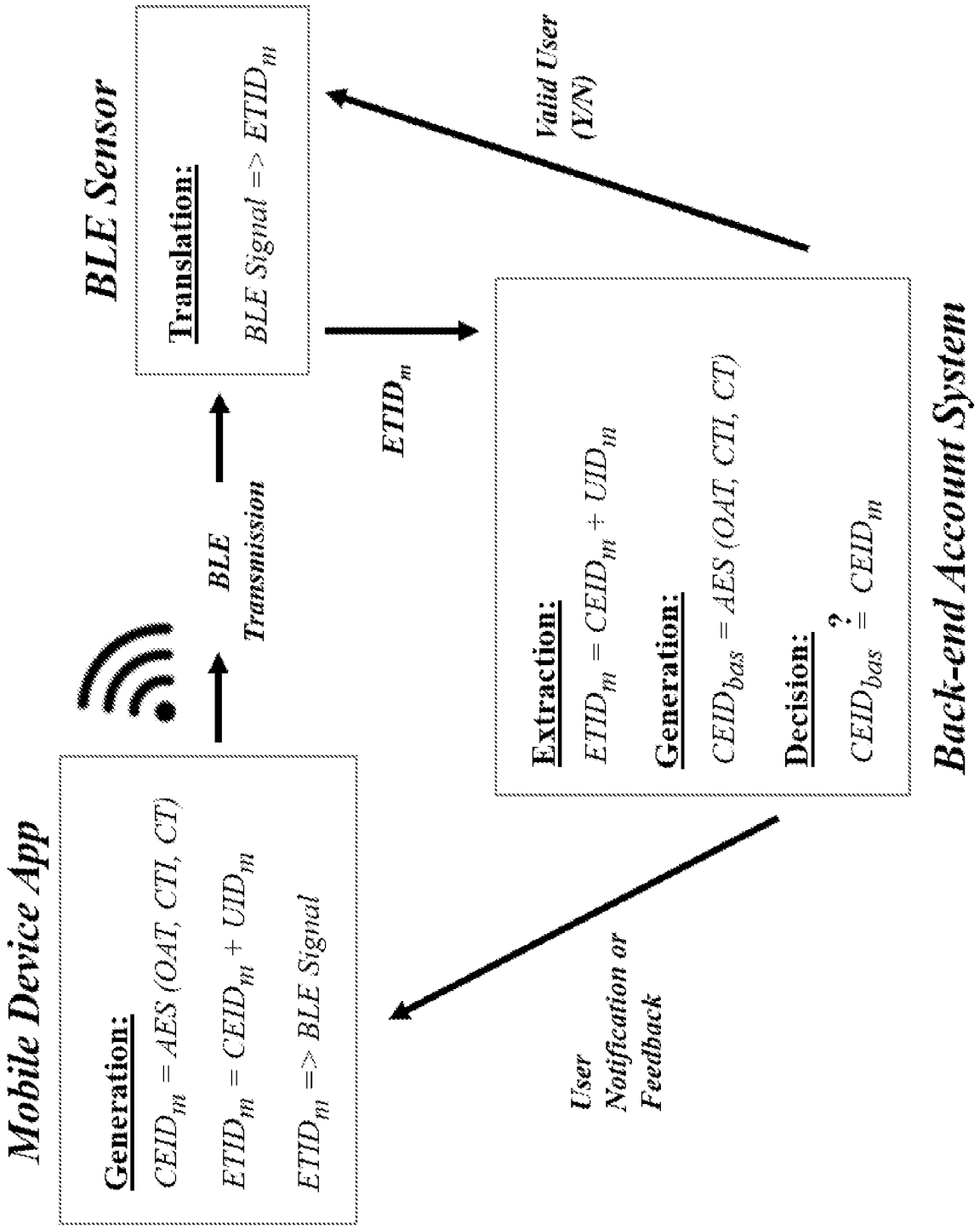
Mobile Device App
Generation:
$CEID_m = AES\ (OAT, CTI, CT)$
$ETID_m = CEID_m + UID_m$
$ETID_m$ => BLE Signal
BLE Transmission
BLE Sensor
Translation:
BLE Signal => $ETID_m$
$ETID_m$
Extraction:
$ETID_m = CEID_m + UID_m$
Generation:
$CEID_{bas} = AES\ (OAT, CTI, CT)$
Decision:
$CEID_{bas} \stackrel{?}{=} CEID_m$
Back-end Account System
Valid User (Y/N)
User Notification or Feedback

FIG. 3

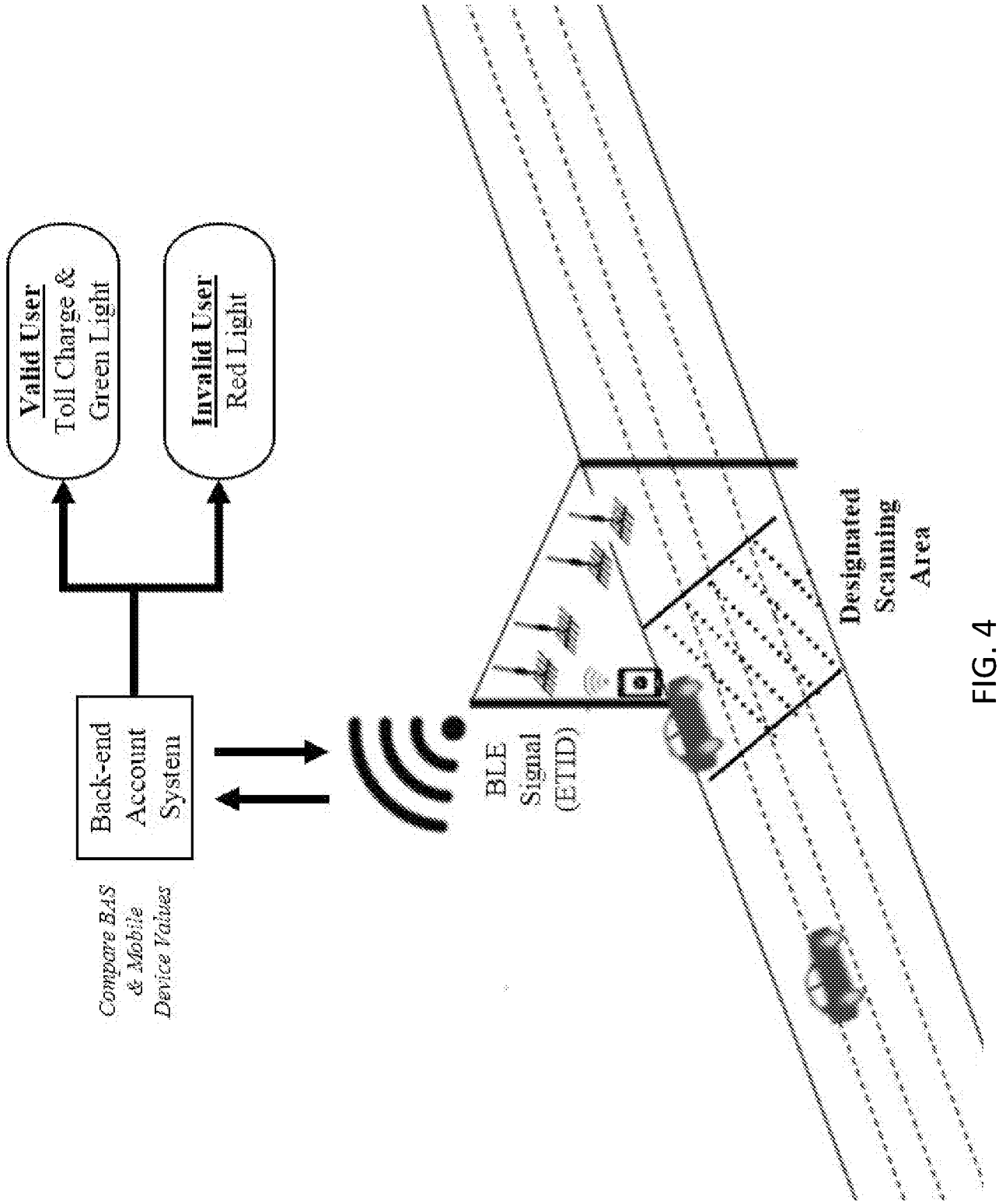
Valid User
Toll Charge &
Green Light
Invalid User
Red Light
Back-end
Account
System
Compare BAS
& Mobile
Device Values
BLE
Signal
(ETID)
Designated
Scanning
Area

FIG. 4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2018/012947

A. CLASSIFICATION OF SUBJECT MATTER

G07C 9/00(2006.01)i, H04H 60/91(2008.01)i, H04L 29/06(2006.01)i, H04L 29/08(2006.01)i, H04W 12/04(2009.01)i, H04W 12/06(2009.01)i, H04W 92/04(2009.01)i, H04W 92/10(2009.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G07C 9/00; G08B 21/00; G06Q 30/00; H04W 8/14; H04W 4/02; G06Q 50/00; H04M 1/725; H04H 60/90; G08B 29/00; H04W 64/00; H04H 60/91; H04L 29/06; H04L 29/08; H04W 12/04; H04W 12/06; H04W 92/04; H04W 92/10

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Korean utility models and applications for utility models
Japanese utility models and applications for utility models

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
eKOMPASS(KIPO internal) & Keywords: located-base, authentication, mobile device, sensor, bluetooth

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2013-0217332 A1 (QUALCOMM INCORPORATED) 22 August 2013 See paragraphs [0080]-[0155], claims 1-10 and figures 1-3.	19-20
A		1-18
A	US 2010-0201536 A1 (WILLIAM BENJAMIN ROBERTSON et al.) 12 August 2010 See paragraphs [0011]-[0035], claims 1-5 and figures 1-3.	1-20
A	US 2016-0337508 A1 (HONEYWELL INTERNATIONAL INC.) 17 November 2016 See paragraphs [0016]-[0034], claim 1 and figures 1-2.	1-20
A	JP 2015-519798 A (GOOGLE INC.) 09 July 2015 See paragraphs [0014]-[0040], claim 1 and figures 1-2.	1-20
A	US 2010-0211431 A1 (HOWARD W. LUTNICK et al.) 19 August 2010 See paragraphs [0104]-[0116] and figures 1-2.	1-20

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

☒ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents,such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
22 June 2018 (22.06.2018)	**22 June 2018 (22.06.2018)**

Name and mailing address of the ISA/KR
International Application Division
Korean Intellectual Property Office
189 Cheongsa-ro, Seo-gu, Daejeon, 35208, Republic of Korea
Facsimile No. +82-42-481-8578

Authorized officer
LEE, Myung Jin
Telephone No. +82-42-481-8474

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/US2018/012947

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2013-0217332 A1	22/08/2013	CN 104246529 A	24/12/2014
		CN 104246529 B	26/01/2018
		CN 104247369 A	24/12/2014
		CN 104365122 A	18/02/2015
		CN 104428806 A	18/03/2015
		CN 104584589 A	29/04/2015
		CN 105557031 A	04/05/2016
		CN 106664523 A	10/05/2017
		EP 2817651 A2	31/12/2014
		EP 2817937 A2	31/12/2014
		EP 2817937 B1	05/04/2017
		EP 2842295 A1	04/03/2015
		EP 2845030 A2	11/03/2015
		EP 2942928 A1	11/11/2015
		EP 3047681 A1	27/07/2016
		EP 3047681 B1	18/10/2017
		EP 3189643 A1	12/07/2017
		JP 2015-510743 A	09/04/2015
		JP 2015-513838 A	14/05/2015
		JP 2015-515080 A	21/05/2015
		JP 2015-522960 A	06/08/2015
		JP 2016-534675 A	04/11/2016
		JP 6129880 B2	17/05/2017
		JP 6290104 B2	07/03/2018
		KR 10-1766951 B1	09/08/2017
		KR 10-2014-0144684 A	19/12/2014
		KR 10-2014-0146080 A	24/12/2014
		KR 10-2016-0057442 A	23/05/2016
		US 2013-0214909 A1	22/08/2013
		US 2013-0217333 A1	22/08/2013
		US 2013-0282438 A1	24/10/2013
		US 2013-0297422 A1	07/11/2013
		US 2014-0133656 A1	15/05/2014
		US 2014-0254466 A1	11/09/2014
		US 2014-0370879 A1	18/12/2014
		US 2015-0077229 A1	19/03/2015
		US 2017-0070847 A1	09/03/2017
		US 9544075 B2	10/01/2017
		US 9697453 B2	04/07/2017
		WO 2013-126747 A2	29/08/2013
		WO 2013-126747 A3	07/11/2013
		WO 2013-126759 A2	29/08/2013
		WO 2013-126759 A3	17/10/2013
		WO 2013-163326 A1	31/10/2013
		WO 2013-163333 A2	31/10/2013
		WO 2013-163333 A3	08/01/2015
		WO 2013-163334 A2	31/10/2013
		WO 2013-163334 A3	27/12/2013
		WO 2013-163338 A2	31/10/2013

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/US2018/012947

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
		WO 2015-042065 A1	26/03/2015
		WO 2015-042618 A1	26/03/2015
		WO 2016-036453 A1	10/03/2016
US 2010-0201536 A1	12/08/2010	AU 2010-214013 A1	19/08/2010
		AU 2010-214013 A1	25/08/2011
		AU 2010-214013 B2	15/10/2015
		CA 02751893 A1	19/08/2010
		CA 2751893 C	22/08/2017
		EP 2396984 A2	21/12/2011
		EP 2396984 A4	27/11/2013
		JP 2012-517541 A	02/08/2012
		JP 5591832 B2	17/09/2014
		US 2010-0201482 A1	12/08/2010
		US 2014-0292482 A1	02/10/2014
		US 2015-0213661 A1	30/07/2015
		US 2015-0279130 A1	01/10/2015
		US 2016-0035162 A1	04/02/2016
		US 2016-0210799 A1	21/07/2016
		US 2016-0300413 A1	13/10/2016
		US 8791790 B2	29/07/2014
		US 9129450 B2	08/09/2015
		US 9336635 B2	10/05/2016
		US 9361741 B2	07/06/2016
		US 9367975 B2	14/06/2016
		US 9558604 B2	31/01/2017
		WO 2010-093499 A2	19/08/2010
		WO 2010-093499 A3	28/10/2010
		WO 2010-093499 A8	19/08/2010
US 2016-0337508 A1	17/11/2016	CN 106161423 A	23/11/2016
		US 2016-0335819 A1	17/11/2016
		US 2017-0280322 A1	28/09/2017
		US 9589403 B2	07/03/2017
		US 9713002 B2	18/07/2017
JP 2015-519798 A	09/07/2015	DE 202013012436 U1	04/11/2016
		EP 2818011 A1	31/12/2014
		EP 2818011 B1	28/12/2016
		EP 3151619 A1	05/04/2017
		JP 5890584 B2	22/03/2016
		KR 10-1494588 B1	17/02/2015
		KR 10-2014-0139134 A	04/12/2014
		US 2013-0281110 A1	24/10/2013
		US 2014-0141804 A1	22/05/2014
		US 8639266 B2	28/01/2014
		US 9769601 B2	19/09/2017
		WO 2013-158401 A1	24/10/2013
US 2010-0211431 A1	19/08/2010	US 2015-0012359 A1	08/01/2015

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/US2018/012947

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
		US 8688517 B2	01/04/2014
		US 9940643 B2	10/04/2018