



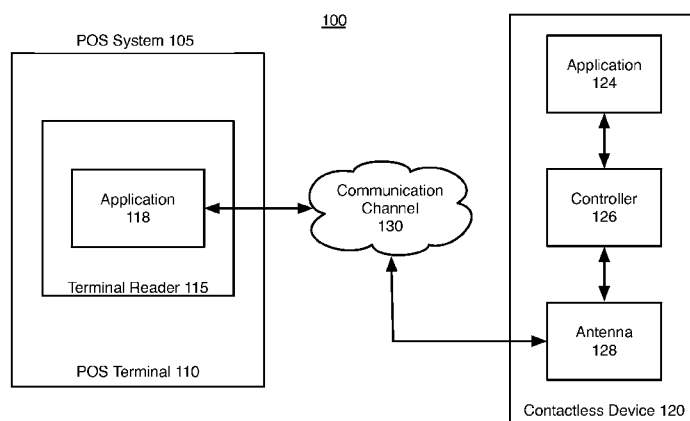
- (51) **International Patent Classification:**
H04B 7/24 (2006.01) *H04B 5/02* (2006.01)
- (21) **International Application Number:**
PCT/US2013/035861
- (22) **International Filing Date:**
9 April 2013 (09.04.2013)
- (25) **Filing Language:** English
- (26) **Publication Language:** English
- (30) **Priority Data:**
13/443,683 10 April 2012 (10.04.2012) US
- (71) **Applicant:** GOOGLE INC. [US/US]; 1600 Amphitheatre Parkway, Mountain View, CA 94043 (US).
- (72) **Inventors:** HERTEL, Philipp; 1600 Amphitheatre Parkway, Mountain View, CA 94043 (US). WALFISH, Sheldon, I.; 1600 Amphitheatre Parkway, Mountain View, CA 94043 (US). HERTEL, Alexander, W.; 1600 Amphitheatre Parkway, Mountain View, CA 94043 (US).
- (74) **Agent:** ISAACS, II, William, O.; Johnson, Marcou & Isaacs, LLC, 317A E. Liberty Street, Savannah, GA 31401 (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, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, 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, 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, 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, ML, MR, NE, SN, TD, TG).

Published:

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

(54) **Title:** DETECTING A COMMUNICATION TAP VIA SIGNAL MONITORING**Figure 1**

(57) **Abstract:** Using a Bluetooth communication channel for point of sale processing simulates a near field communication connection. A contactless device and the point of sale reader establish an unsecure communication channel. The user taps the contactless device with a point of sale terminal reader. The contactless device creates receive signal strength indicator ("RSSI") value spikes. The terminal reader measures the RSSI values and transmits them to the contactless device, which determines if the RSSI value reaches or exceeds a threshold configured for the contactless device. If the threshold is reached, the terminal reader and the contactless device establish a secure communication connection. The devices communicate via the secure communication connection, and the connection is terminated when a request to terminate is received.

DETECTING A COMMUNICATION TAP VIA SIGNAL MONITORING**RELATED APPLICATIONS**

[0001] This application claims priority to U.S. Application No. 13/443,683, filed April 10, 2012, and entitled “Detecting A Communication Tap Via Signal Monitoring.” The entire contents of the above-identified priority application are hereby fully incorporated herein by reference.

TECHNICAL FIELD

[0002] The present disclosure relates generally to contactless devices and more particularly to methods and systems that allow for point of sale processing and communication initiated by a Bluetooth communication channel.

BACKGROUND

[0003] Near field communication (“NFC”) is a proximity communication technology that can enable contactless device payment transactions with a point of sale system. NFC communication generally is conducted in a range from about 3 to about 4 inches. Such short communication distances enable secure communication between close field proximity enabled devices. In operation of an NFC transaction, a user “taps” a contactless device, such as an NFC-enabled mobile phone, to a reader of a point of sale system. The reader recognizes the NFC-enabled device when the device is moved within range of the reader, establishes a secure communication channel with the device, and initiates a payment transaction between the reader and the device. The duration of the NFC transaction is very short and does not easily permit communication of other information or the conduct of other services during the transaction. Additionally, the contactless device must be held close to the reader during the entire NFC transaction.

[0004] NFC contactless payment devices can function as a credit card to enable purchases at the point-of-sale by communicating credit card account information to the point of sale reader. However, the short duration of conventional NFC methods and systems for contactless payment devices does not enable the utilization of value-added services and user choices to a transaction. During the conventional transaction, the device and the reader communicate to complete the predefined transaction. Further user input or further transactions, such as user selection of coupons or loyalty rewards or automatic application of those items, is not possible in the predefined NFC transaction, without establishing another

connection or holding the device close to the reader for the entire transaction. Alternative conventional methods require multiple taps or a tap and hold of the contactless device to enable the utilization of each service, resulting in user inconvenience. Additionally, few mobile devices, such as mobile phones, are equipped with NFC functionality. Without NFC functionality, such mobile devices cannot be used for NFC transactions. Many mobile devices are equipped with Bluetooth technology. Accordingly, it would be desirable to use Bluetooth technology on the context of NFC transactions

SUMMARY

[0005] In certain exemplary aspects, systems and methods of allowing point of sale processing and communication initiated by a Bluetooth communication channel comprises a point of sale (“POS”) terminal reader that facilitates a Bluetooth communication connection with a contactless device. A contactless device and terminal reader establish an unsecure communication channel that can measure signal strength. The user taps the contactless device in the terminal reader’s radio frequency field. The contactless device creates receive signal strength indicator (“RSSI”) value spikes, which indicate the proximity of the contactless device to the reader based on the strength of the Bluetooth signal received from the reader. The terminal reader measure the RSSI values, calculates an average RSSI value and transmits them to the contactless device. The contactless device determines if the average value reaches or exceeds threshold value for the contactless device. In an alternative exemplary embodiment, the terminal reader compares the RSSI values to the threshold value for the contactless device, without transmitting the values to the device. If the threshold is reached, the terminal reader and the contactless device establish a secure communication connection. The device and the reader communicate via the secure communication connection and the connection is terminated when a request to terminate is received.

[0006] These and other aspects, objects, features, and advantages of the exemplary embodiments will become apparent to those having ordinary skill in the art upon consideration of the following detailed description of illustrated exemplary embodiments.

BRIEF DESCRIPTION OF THE DRAWINGS

[0007] Figure 1 is a block diagram depicting a system for detecting a communication tap of a contactless device with a point of sale (“POS”) reader device using signal monitoring according to an exemplary embodiment.

[0008] Figure 2 is a block flow diagram depicting a method for detecting a communication tap of a contactless device with a POS reader device by the contactless device using signal monitoring according to an exemplary embodiment.

[0009] Figure 3 is a block flow diagram depicting a method for determining the average receive signal strength indicator (“RSSI”) value according to an exemplary embodiment.

[0010] Figure 4 is a block flow diagram depicting a method for detecting a communication tap of a contactless device with a POS reader device by the POS reader device according to an exemplary embodiment.

DETAILED DESCRIPTION OF EXEMPLARY EMBODIMENTS

Overview

[0011] The exemplary embodiments provide methods and systems that enable the detection of a communication tap via signal monitoring include a Bluetooth communication channel that allows communication with a POS reader from outside the reader’s NFC field of communication. The contactless device and the terminal reader establish an unsecure communication channel that can measure signal strength, for example an insecure RFCOMM channel. Upon successful connection, the contactless device and terminal reader engage in a security protocol that occurs over the RFCOMM channel. Manual pairing and entry of a personal identification number (“PIN”) is not required. The user simulates an NFC tapping motion by moving the contactless device toward the POS reader to place the device next to the reader. The tapping motion causes the contactless device to create RSSI value spikes. For example, the tapping motion of the contactless device creates measurable spikes of the power present in the radio signal received by the reader. The terminal reader measures the RSSI values, calculates an average RSSI value and transmits them to the contactless device. The transmitted values may comprise the average RSSI value. The average RSSI value is calculated by determining a total time period for measuring the RSSI value from the device, determining the number of intervals during this time period in which measurements will be taken from the device, and the period of time between each interval. The terminal reader then detects an initial RSSI value and subsequent RSSI values at the set intervals for the determined period of time and computes the average RSSI value.

[0012] RSSI is a measurement of the strength of the signal received from a device. The signal strength is lower if the contactless device is farther from the reader, and the signal strength increases as the contactless device is moved towards the reader.

Accordingly, the RSSI can be monitored over time to detect when a user “taps” the contactless device to the reader, in a manner similar to “tapping” the contactless device to the reader for an NFC communication.

[0013] Once the average RSSI value is measured and transmitted to the contactless device, the contactless device determines whether the average value reaches or exceeds a minimum threshold value for the contactless device. If the threshold is reached, the terminal reader and the contactless device establish a communication connection. If the threshold is not reached, the reader continues to monitor for a tap. In an alternative exemplary embodiment, the terminal reader compares the RSSI values to the threshold value for the contactless device, without transmitting the values to the device.

[0014] To establish a new secure communication connection, the terminal reader communicates a request to the contactless device. The contactless device accepts the secure communication request. The devices communicate via the secure communication connection, and the connection is terminated when a request to terminate is received.

[0015] The functionality of the exemplary embodiments will be explained in more detail in the following description, read in conjunction with the figures illustrating the program flow.

System Architecture

[0016] Figure 1 is a block diagram depicting a system 100 for detecting a communication tap of a contactless device 120 with a terminal reader 115 using signal monitoring according to an exemplary embodiment. As depicted in Figure 1, the exemplary operating environment 100 includes a merchant POS system 105 and a contactless device 120 that are configured to communicate with one another via one or more communication channels 130.

[0017] The communication channel 130 includes a telecommunication means by which network devices (including devices 110 and 120) can exchange data. In exemplary embodiments, the communication channel 130 comprises a proximity communication connection, such as Bluetooth, NFC, or Wi-Fi. Bluetooth can enable the exchange of data over short distances through the creation of personal area networks with high levels of security. NFC and Wi-Fi also can enable data communication over short distances. The terms “data” and “information” are used interchangeably herein to refer to text, images, audio, video, or any other form of information that can exist in a computer-based environment.

[0018] The POS system 105 includes a terminal reader 115 that is capable of communicating with the contactless device 120 and the POS terminal 110 via an application 118. In an exemplary embodiment, the terminal reader 115 communicates with the contactless device 120 using a Bluetooth communication protocol. In alternative exemplary embodiments, the terminal reader 115 communicates with the contactless device 120 using an NFC or a Wi-Fi communication protocol.

[0019] As depicted in Figure 1, the terminal reader 115 may be a component of the POS terminal 110. In an alternative exemplary embodiment, the terminal reader 115 may be a standalone device that communicates with the POS terminal 110 via one or more secure communication channels. As a standalone device, the terminal reader 115 may be communicatively coupled to the POS terminal 115.

[0020] In an exemplary embodiment, the contactless device 120 is a smart device that can communicate via an electronic, magnetic, or radio frequency field between the device and another device, such as the terminal reader 115. In an exemplary embodiment, the contactless device 120 has processing capabilities, such as storage capacity/memory (not depicted) and one or more application 124 that can perform a particular function. In an exemplary embodiment, the contactless device 120 comprises an operating system (not depicted) and user interface (not depicted). Exemplary contactless devices 120 include smart phones; mobile phones; personal digital assistants (“PDAs”); mobile computing devices, such as netbooks and iPads; other electronically enabled key fobs; electronically enabled credit card type cards; and other devices, in each case having processing and user interface functionality. Certain contactless devices 120 can be used for multiple purposes, including financial transactions, coupons, ticketing, secure authentication, and other related applications.

[0021] The controller 126 controls the overall operation of communication, including the processing and control of voice and data communications. In an exemplary embodiment, the controller 126 communicates with the application 124 in the contactless device 120. The controller 126 can interact with a secure key encrypted application 124 for decryption and installation of information in a secure element (not depicted). In an exemplary embodiment, the controller 126 is a Bluetooth link controller. The Bluetooth link controller can be capable of sending and receiving data, identifying the terminal reader 115, performing authentication and ciphering functions, and directing how the contactless device 120 will listen for transmissions from the device reader 115 or configure the contactless device 120 into various power-save modes according to the Bluetooth-specified procedures.

[0022] The application 124 is a program, function, routine, applet or similar entity that exists on and performs its operations on a contactless device 120. For example, the application 124 may be one or more of a digital wallet application, a coupon application, a loyalty card application, another value-added application, a user interface application, or other suitable application operating on the contactless device 120. Additionally, the secure element (not illustrated) also may comprise secure contactless software applications, such as payment applications, secure forms of the applications 124, authentication applications, payment provisioning applications, or other suitable application using the secure functionality of the secure element.

[0023] The contactless device 120 communicates with the terminal reader 115 via an antenna 128. In an exemplary embodiment, once the contactless device application 124 has been activated and prioritized, the controller 126 is notified of the state of readiness of the contactless device 120 for a transaction. The controller 126 outputs through the antenna 128 a radio signal, or listens for radio signals from the terminal reader 115. The method for detecting a communication tap via signal monitoring is described in more detail hereinafter with reference to the methods described in Figures 2-4.

System Process

[0024] Figure 2 is a block flow diagram depicting a method 200 for method for detecting a communication tap of a contactless device 120 with a terminal reader 115 by the contactless device 120 using signal monitoring according to an exemplary embodiment. The method 200 is described with reference to the components illustrated in Figure 1.

[0025] In block 210, the contactless device 120 and the terminal reader 115 establish a communication channel 130. In an exemplary embodiment, the communication channel is an unsecure communication channel. In an exemplary embodiment, the devices establish an open connection as soon as the devices discover one another. For example, the devices may establish a Bluetooth communication channel wherein no personal identification number (PIN) is required and no manual pairing is required. In an exemplary embodiment, the unsecure communication channel is used to measure signal strength and to determine when a “tap” has occurred.

[0026] In an exemplary embodiment, the contactless device 120 enters a proximity (for example, 100 meters) to the terminal reader 115, wherein the contactless device 120 is close enough to discover and/or contact the terminal reader 115 over a Bluetooth channel. In an alternative exemplary embodiment, the terminal reader 115 may discover and/or contact the contactless device 120. In an exemplary embodiment, Bluetooth

discovery occurs. For example service discovery protocol (“SDP”) allows the devices 120 and 115 to discover which services each device supports and what parameters to use to connect to them. In an alternative exemplary embodiment, an external mechanism determines that the contactless device 120 is within communication range of the terminal reader 115. For example, the contactless device’s built-in global positioning system (“GPS”) may be used. The contactless device 120 will attempt to contact the terminal reader 115 by connecting to the reader’s Bluetooth address and port using an insecure RFCOMM. An insecure RFCOMM is an ordinary Bluetooth socket that does not require Bluetooth device pairing to occur. Therefore, it is “insecure” because there is no identification of the endpoints other than a Bluetooth address. If the contactless device 120 is detected in the proximity of the terminal reader 115 using different means than SDP (for example, using GPS), it will require the terminal reader’s 115 Bluetooth address. In an exemplary embodiment, the terminal reader’s 115 Bluetooth address is provided via a cloud network backend that provides the location of the terminal reader 115 as well as its Bluetooth address in order to open an insecure RFCOMM channel. Upon successful connection to the terminal reader 115 by the contactless device 120, the devices 115 and 120 engage in a security protocol that occurs over the RFCOMM channel. In an exemplary embodiment, the terminal reader 115 has a secure sockets layer (“SSL”) certificate and the contactless device 120 may open an SSL channel to the terminal reader 115 using the RFCOMM channel as a transportation layer. In an exemplary embodiment, the SSL channel is a secure communication channel.

[0027] In block 220, the movement of the contactless device 120 towards the terminal reader 115 creates receive signal strength indicator (“RSSI”) value spikes. RSSI is an indication of the power level of a signal being received by the antenna of a device. A higher RSSI number (which may be a less negative number in some cases) indicates a stronger signal. For Bluetooth technologies, RSSI also is analogous to an indication of the distance between devices. A higher RSSI number indicates the devices are closer than a lower RSSI number.

[0028] In an exemplary embodiment, the movement of the contactless device 120 during a “tap” with the terminal reader 115 creates the RSSI value spikes. The close proximity of the contactless device 120 to the terminal reader 115 results in larger RSSI value spikes requiring smaller movement of the contactless device 120. In another exemplary embodiment, the contactless device 120 is further from the terminal reader 115, requiring larger and more frequent movements to create RSSI value spikes.

[0029] In an exemplary embodiment, it may be difficult to detect when a tap has occurred. For example, detection may require an accelerometer. In an exemplary embodiment, detection of the tap indicates to the contactless device that it is communicating with a particular POS system 105. In an alternative exemplary embodiment, detection of the tap indicates that the contactless device 120 is ready to start a payment session.

[0030] In an exemplary embodiment for NFC operations, the terminal reader 115 generates a radio frequency or other field continuously polling for the presence of a contactless device 120, and the user “taps” the contactless device by placing the device 120 within the field of the reader 115. In another exemplary embodiment for NFC operations, the contactless device 120 generates a radio frequency or other field continuously polling for the presence of a terminal reader 115, and the user “taps” the contactless device by placing the device 120 in close proximity of the reader 115.

[0031] For Bluetooth communication, the contactless device 120 and the POS reader 115 do not have to be in such close proximity (for example, 3 inches to 4 inches apart as with NFC) for communication. However, to provide the security of requiring that the contactless device 120 and the POS reader 115 are within such close proximity, the method 200 uses Bluetooth signal monitoring to identify when the user simulates an NFC tap by moving the contactless device 120 towards the POS reader 115 to place the contactless device 120 within the close proximity to the POS reader 115.

[0032] In an exemplary embodiment, once a communication channel 130 is established, the terminal reader 115 begins to take measurements of the RSSI value for that connection. These RSSI values indicate the perceived strength of the signal from the contactless device 120, as observed by the terminal reader 115.

[0033] In exemplary embodiments, RSSI can be measured by either the contactless device 120, the POS reader 115, or both. The contactless device 120 measure the RSSI for the signals received from the POS reader 115. The POS reader 115 measures the RSSI for the signals received from the contactless device 120.

[0034] In an exemplary embodiment, the contactless device 120 opens a Bluetooth connection. The signal strength of the contactless device 120 is measured by the POS system 105 using periodic sampling. The POS system 105 indicates to the contactless device 120 that it is measuring the signal strength by sending measurements. For example, the POS system 105 may send a single measurement, multiple measurements, or an average of the measurements. The contactless device 120 determines when a tap has occurred based

on the signal strength measurements received from the POS system 105 by determining when the signal strength has spiked.

[0035] In an alternative exemplary embodiment, an accelerometer is utilized by the POS system 105. Because the POS system 105 can trick the contactless device 120 into thinking a spike has occurred based on the signal strength measurements sent, measurements may be made by either the contactless device 120 or the POS system 105. The accelerometer is built into the POS system 105 so the contactless device can read the signal strength of the POS system. The contactless device 120 may send signal strength measurements to the POS system 105 for determination whether a spike has occurred by the POS system 105 or the contactless device 120 may make the determination of when a signal spike has occurred.

[0036] In block 230, the terminal reader 115 and/or the contactless device 120 determines an average RSSI value. In an alternative exemplary embodiment, a single RSSI value measurement is sufficient, without determining an average RSSI value. The method 230 for determining the average RSSI value is described in more detail hereinafter with reference to the methods described with reference to Figure 3. While blocks 310-360 are generally described with reference to the terminal reader 115 monitoring RSSI based on signals received from the contactless device 120, the blocks can be performed by the contactless device 120 monitoring RSSI based on signals received from the terminal reader 115.

[0037] Figure 3 is a block flow diagram depicting a method 230 for determining the average RSSI value according to an exemplary embodiment. The method 230 is described with reference to the components illustrated in Figure 1.

[0038] In an exemplary embodiment, while the user taps the contactless device 120 in the proximity of the terminal reader 115, the reader 115 determines the average RSSI value. In another exemplary embodiment, the contactless device 120 determines the average RSSI value.

[0039] In block 310, the terminal reader 115 determines a total time period during which the terminal reader 115 will measure RSSI values and determining the average RSSI value. In an alternative exemplary embodiment, the contactless device 120 determines the total time period to be utilized in measuring RSSI values and determining the average RSSI value.

[0040] In an exemplary embodiment, the total time period can be 100 milliseconds, which can simulate a time period of a near field communication tap. The time period can be configured to measure a suitable interval such that an average RSSI value

during the time period indicates a “tapping” motion of the contactless device 120 with the terminal reader 115.

[0041] In block 320, the terminal reader 115 determines the number of intervals in which RSSI measurements will be taken to determine the average RSSI value. In an alternative exemplary embodiment, the contactless device 120 determines the number of intervals in which RSSI measurements will be taken to determine the average RSSI value.

[0042] In block 330, the terminal reader 115 determines the time period between intervals in which RSSI measurements will be taken to determine the average RSSI value. In an alternative exemplary embodiment, the contactless device 120 determines the time period between intervals in which RSSI measurements will be taken to determine the average RSSI value. In an exemplary embodiment, the intervals are continuous (for example, every millisecond).

[0043] The terminal reader 115 detects the initial RSSI value of the contactless device 120 in block 340. In an alternative exemplary embodiment, the contactless device 120 detects the initial RSSI value.

[0044] In block 350, the terminal reader 115 detects subsequent RSSI values at set intervals for a set period of time as determined in blocks 310, 320 and 330. In an alternative exemplary embodiment, the contactless device 120 detects subsequent RSSI values at set intervals for a set period of time as determined in blocks 310, 320 and 330.

[0045] The terminal reader 115 computes the average RSSI value over the set time period in block 360. In an alternative exemplary embodiment, the contactless device 120 computes the average RSSI value over the set time period.

[0046] From block 360, the method 230 proceeds to block 240 (Figure 2).

[0047] Returning to Figure 2, in block 240, the terminal reader 115 transmits an average RSSI value to the contactless device 120. In an exemplary embodiment, a moving average of the RSSI values is transmitted from the terminal reader 110 to the contactless device 120 several times per second. In an alternative exemplary embodiment, a single RSSI value is transmitted from by the terminal reader 115 to the contactless device 120 and the methods described in blocks 310-360 of Figure 3 are omitted.

[0048] In block 245, the contactless device 120 determines if the threshold RSSI value was reached. In an exemplary embodiment, an acceptable RSSI value range is pre-determined for the contactless device 120. In an alternative exemplary embodiment, the pre-determined acceptable value is communicated to the terminal reader 115 by the contactless

device 120 and the terminal reader 115 determines if the threshold average RSSI value was reached.

[0049] If the threshold average RSSI value was not reached in block 245, the method 200 returns to block 220 in which the user “taps” the contactless device 120 in the proximity of the terminal reader 115 to create RSSI value spikes.

[0050] If the average RSSI value meets or exceeds the configured threshold average RSSI value, the method 200 proceeds to block 250 in which the contactless device 120 sends a secure communication request to the terminal reader 115. In an exemplary embodiment, the communication request includes the average RSSI value. In an alternative exemplary embodiment, the terminal reader 115 sends a communication request to the contactless device 120. In an exemplary embodiment, the communication request is for a secure communication channel 130. In an exemplary embodiment, the secure communication channel 130 is an RF communications channel, such as Bluetooth.

[0051] In an exemplary embodiment, the communication request is an indication that the average RSSI value met or exceed the threshold value.

[0052] In block 260, the terminal reader 115 accepts the secure communication request.

[0053] In block 270, the terminal reader 115 and the contactless device 120 establish a new secure communication channel 130. The secure communication channel 130 can be established in exemplary embodiments via Bluetooth. Such secure communications can provide benefits over an NFC-type connection. For example, such secure communications can remain open for ranges farther than the limited 3-4 inch range of NFC communications. Additionally, such secure communications can remain open for longer time periods, for example, until terminated by the terminal reader 115, the contactless device 120, or by user input into the device 120.

[0054] In block 280, the terminal reader 115 and the contactless device 120 communicate via the secure communications channel 130. In exemplary embodiments, the secure communications can include conducting a secure payment transaction; applying coupons, loyalty rewards, or other offers to a transaction; incrementing loyalty rewards for the transaction; downloading applications or other information; or any other suitable communication.

[0055] Although described throughout this specification as the terminal reader 115 performing specific functions, such functions may be performed by the application 118

and/or the POS terminal 110 and communicated to the contactless device 120 via the terminal reader 115.

[0056] In block 280, the secure communications channel 130 can be terminated when the request to terminate a secure communication channel between the terminal reader 115 and the contactless device 120 is communicated, or any suitable time thereafter.

[0057] From block 280, the method 200 ends.

[0058] Figure 4 is a block flow diagram depicting a method 400 for detecting a communication tap of a contactless device 120 with a terminal reader 115 by the terminal reader 115 according to an exemplary embodiment. The method 200 is described with reference to the components illustrated in Figure 1.

[0059] In block 210, the contactless device 120 and the terminal reader 115 establish a communication channel 130. In an exemplary embodiment, block 210 of Figure 4 can be performed in a manner described previously with reference to block 210 of Figure 2.

[0060] In block 415, the contactless device 120 transmits characteristic and protocols to the terminal reader. In an exemplary embodiment, the characteristic and protocols comprise a RSSI threshold value that is pre-determined for the contactless device 120.

[0061] In an exemplary embodiment, blocks 220 through 230 of Figure 4 can be performed in a manner described previously with reference to blocks 220 through 430 of Figure 2.

[0062] In block 440, the terminal reader 115 compares the RSSI values to the RSSI threshold value transmitted by the contactless device 120 in block 405. In an exemplary embodiment, the terminal reader 115 compares the average RSSI value calculated in block 230 to the threshold RSSI value for the contactless device 120. In an alternative exemplary embodiment, the terminal reader 115 compares a single measured RSSI value to the RSSI threshold value for the contactless device 120. In this embodiment, the method described in block 230 of Figure 4 may be omitted.

[0063] In an exemplary embodiment, blocks 245 through 290 of Figure 4 can be performed in a manner described previously with reference to blocks 245 through 290 of Figure 2, except the terminal reader 115 sends a secure communication request to the contactless device 120 and the contactless device 120 accepts the request. In an exemplary embodiment, the request for a secure communication channel 130 comprises the measured or average RSSI value. In an alternative exemplary embodiment, the request for a secure

communication channel 130 also comprises the threshold RSSI value for the contactless device 120 received in block 415.

[0064] From block 290, the method 400 ends.

General

[0065] Users may be allowed to limit or otherwise affect the operation of the features disclosed herein. For example, users may be given opportunities to opt-in or opt-out of the collection or use of certain data or the activation of certain features. In addition, users may be given the opportunity to change the manner in which the features are employed, including for situations in which users may have concerns regarding privacy. Instructions also may be provided to users to notify them regarding policies about the use of information, including personally identifiable information, and manners in which each user may affect such use of information. Thus, information can be used to benefit a user, if desired, through receipt of relevant advertisements, offers, or other information, without risking disclosure of personal information or the user's identity.

[0066] One or more aspects of the exemplary embodiments may include a computer program that embodies the functions described and illustrated herein, wherein the computer program is implemented in a computer system that comprises instructions stored in a machine-readable medium and a processor that executes the instructions. However, it should be apparent that there could be many different ways of implementing the exemplary embodiments in computer programming, and the exemplary embodiments should not be construed as limited to any one set of computer program instructions. Further, a skilled programmer would be able to write such a computer program to implement an embodiment based on the appended flow charts and associated description in the application text. Therefore, disclosure of a particular set of program code instructions is not considered necessary for an adequate understanding of how to make and use the exemplary embodiments. Moreover, any reference to an act being performed by a computer should not be construed as being performed by a single computer as the act may be performed by more than one computer.

[0067] The exemplary systems, methods, and blocks described in the embodiments presented previously are illustrative, and, in alternative embodiments, certain blocks can be performed in a different order, in parallel with one another, omitted entirely, and/or combined between different exemplary methods, and/or certain additional blocks can be performed, without departing from the scope and spirit of the invention. Accordingly, such alternative embodiments are included in the invention described herein.

[0068] The invention can be used with computer hardware and software that performs the methods and processing functions described above. As will be appreciated by those having ordinary skill in the art, the systems, methods, and procedures described herein can be embodied in a programmable computer, computer executable software, or digital circuitry. The software can be stored on computer readable media. For example, computer readable media can include a floppy disk, RAM, ROM, hard disk, removable media, flash memory, memory stick, optical media, magneto-optical media, CD-ROM, etc. Digital circuitry can include integrated circuits, gate arrays, building block logic, field programmable gate arrays ("FPGA"), etc.

[0069] Although specific embodiments of the invention have been described above in detail, the description is merely for purposes of illustration. Various modifications of, and equivalent blocks corresponding to, the disclosed aspects of the exemplary embodiments, in addition to those described above, can be made by those having ordinary skill in the art without departing from the spirit and scope of the invention defined in the following claims, the scope of which is to be accorded the broadest interpretation so as to encompass such modifications and equivalent structures.

CLAIMS

What is claimed is:

1. A computer-implemented method for detecting a tap of a mobile communication device with a point of sale system, comprising:

establishing a first communication channel by a point of sale (“POS”) device with a mobile communication device;

detecting, by the POS device, receive signal strength indicator (“RSSI”) value spikes based on the strength of a signal from the mobile communication device, as observed by the POS device when the mobile communication device is moved in proximity to the POS device;

transmitting, by the POS device, an RSSI value monitored during a predetermined period of time to the mobile communication device;

receiving, by the POS device, a request to establish a second communication channel with the mobile communication device in response to a determination that the RSSI value monitored during the predetermined period of time meets or exceeds a threshold value established for the mobile communication device;

communicating, by the POS device, an authorization to establish the second communication channel with the mobile communication device; and

communicating, by the POS device, information to and receiving, by the POS device, information from the mobile communication device via the communication channel.

2. The method of claim 1, wherein the first communication channel is a Bluetooth communication channel.

3. The method of claim 1, wherein the first communication channel is an unsecure communication channel.

4. The method of claim 1, wherein the first communication channel is a radio frequency (RF) communication channel.

5. The method of claim 1, wherein the second communication channel is a secure communication channel.

6. The method of claim 1, wherein the strength of the signal from the mobile communication device is measured by the POS device using periodic sampling.
7. The method of claim 1, wherein the POS device comprises a POS reader.
8. The method of claim 1, wherein the RSSI value transmitted to the mobile communication device is an average RSSI value.

9. A computer program product, comprising:
- a non-transitory computer-readable medium having computer-readable program code embodied thereon for detecting a tap of a mobile communication device with a point of sale system, the computer-readable medium comprising:
- computer-readable program code for establishing a first communication channel with a mobile communication device;
- computer-readable program code for detecting receive signal strength indicator ("RSSI") value spikes based on the strength of a signal from the mobile communication device when the mobile communication device is moved in proximity to a POS device;
- computer-readable program code for transmitting an RSSI value;
- computer-readable program code for communicating a request to establish a second communication channel with the mobile communication device; and
- computer-readable program code for receiving an authorization to establish the second communication channel with the mobile communication device.
10. The computer program product of claim 9, wherein the request to establish a second communication channel comprises an average RSSI value, and wherein the authorization indicates a confirmation that the average RSSI value meets or exceeds a threshold value established for the mobile communication device.
11. The computer program product of claim 9, wherein the first communication channel is a Bluetooth communication channel.
12. The computer program product of claim 9, wherein the first communication channel is an unsecure communication channel.
13. The computer program product of claim 9, wherein the second communication channel is a secure communication channel.

14. A system for detecting a tap of a mobile communication device with a point of sale system, comprising:

a computer configured to

establish a first communication channel with a mobile communication device;

detect receive signal strength indicator ("RSSI") value spikes based on the strength of a signal from the mobile communication device when the mobile communication device is moved in proximity to a POS device; and

transmit an RSSI value; and

an application module configured to execute on a mobile communication device to transmit a request to establish a second communication channel.

15. The system of claim 14, wherein the computer comprises point of sale system.

16. The system of claim 14, wherein the computer comprises point of sale system reader.

17. The system of claim 14, wherein the RSSI value comprises the average RSSI value,

wherein the application module is further configured to verify that the average RSSI value meets or exceeds the threshold value established for the mobile communication device, and

wherein the request comprises a confirmation that the average RSSI value meets or exceeds the threshold value established for the mobile communication device.

18. A computer-implemented method for detecting a tap of a mobile communication device with a point of sale system, comprising:

establishing a first communication channel by a point of sale (“POS”) device with a mobile communication device;

receiving, by the POS device, a threshold receive signal strength indicator (“RSSI”) value from the mobile communication device;

detecting, by the POS device, RSSI value spikes based on the strength of a signal from the mobile communication device, as observed by the POS device when the mobile communication device is moved in proximity to the POS device;

determining, by the POS device, that the RSSI value monitored during a predetermined period of time meets or exceeds the threshold RSSI value for the mobile communication device; and

transmitting, by the POS device, a request to establish a second communication channel with the mobile communication device in response to a determination that the RSSI value monitored during the predetermined period of time meets or exceeds a threshold value established for the mobile communication device.

19. The method of claim 18, further comprising:

receiving, by the POS device, an authorization to establish the second communication channel with the mobile communication device; and

communicating, by the POS device, information to and receiving, by the POS device, information from the mobile communication device via the communication channel.

20. The method of claim 18, wherein the first communication channel is a Bluetooth communication channel.

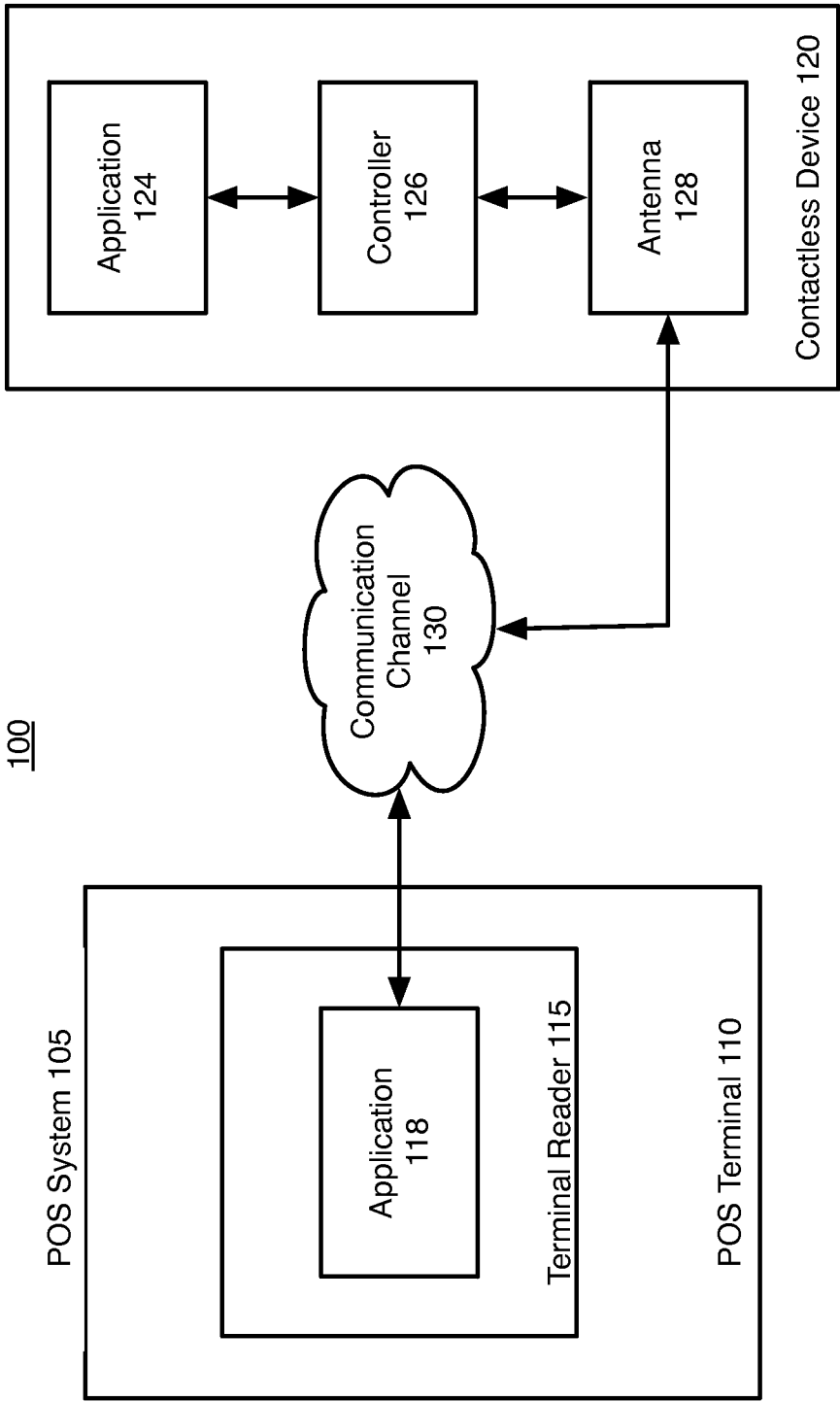
21. The method of claim 18, wherein the first communication channel is an unsecure communication channel.

22. The method of claim 18, wherein the first communication channel is a radio frequency (RF) communication channel.

23. The method of claim 18, wherein the second communication channel is an secure communication channel.

24. The method of claim 18, wherein the strength of the signal from the mobile communication device is measured by the POS device using periodic sampling.

25. The method of claim 18, wherein the POS device comprises a POS reader.



2/4

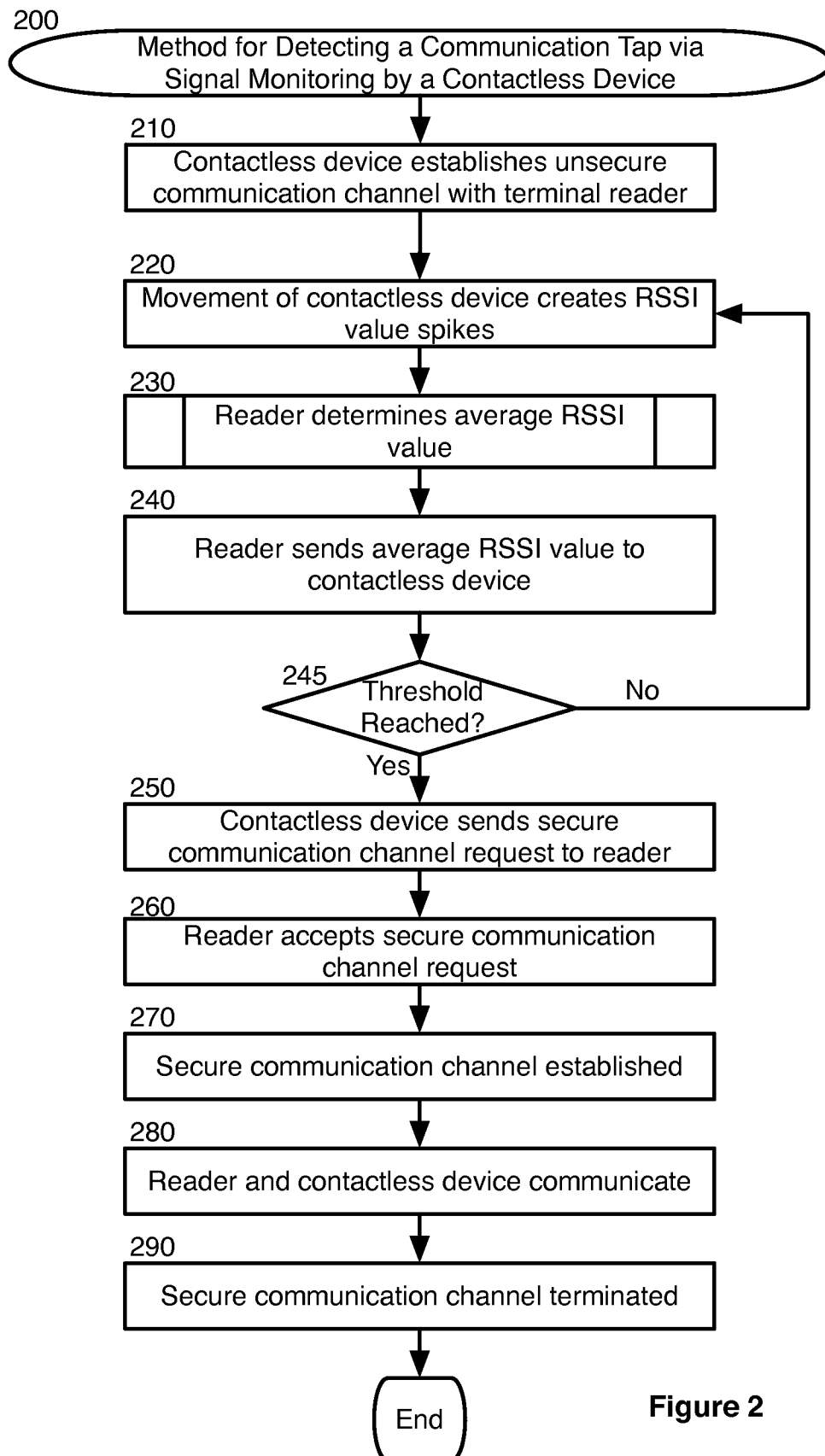
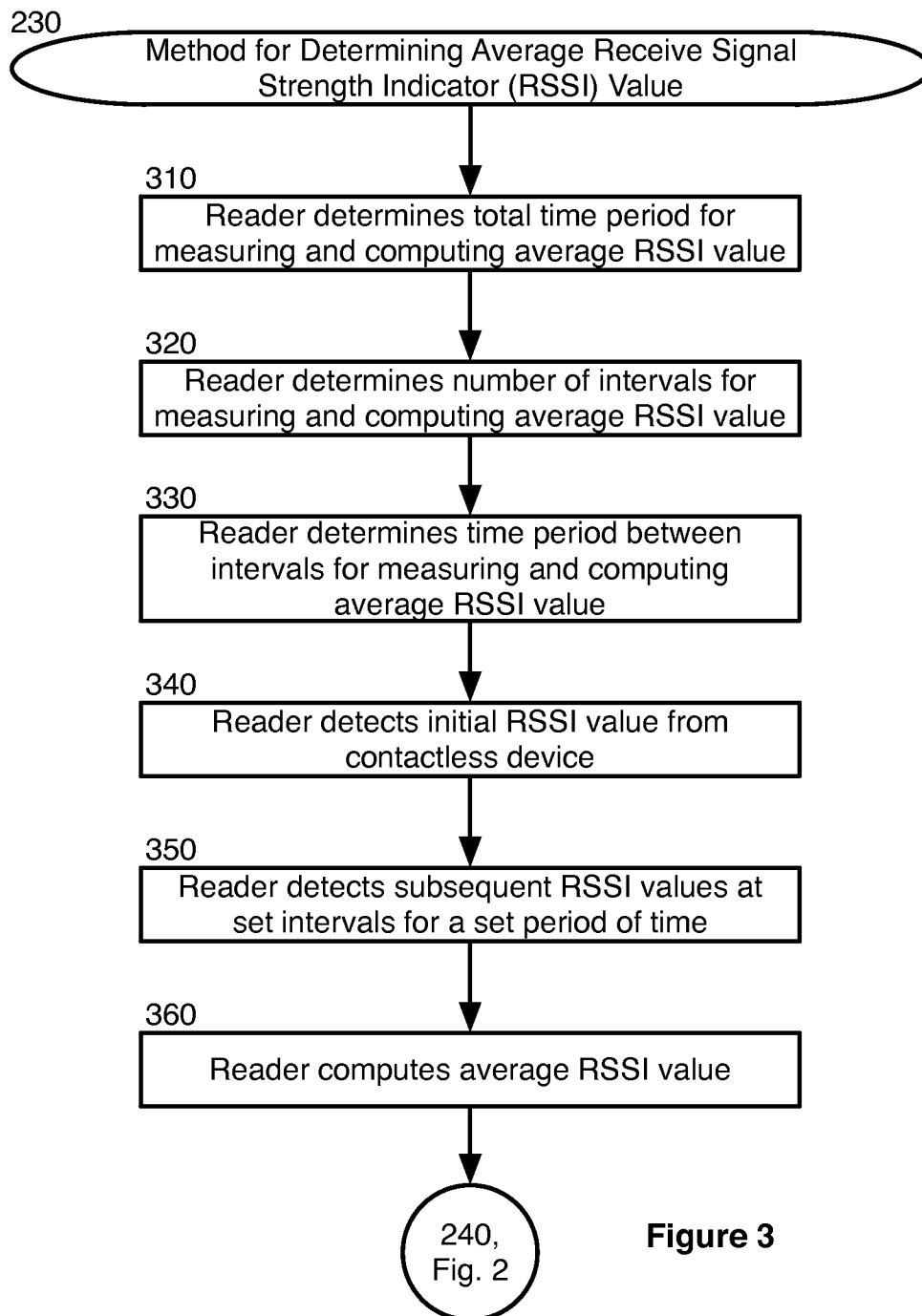


Figure 2

3/4



4/4

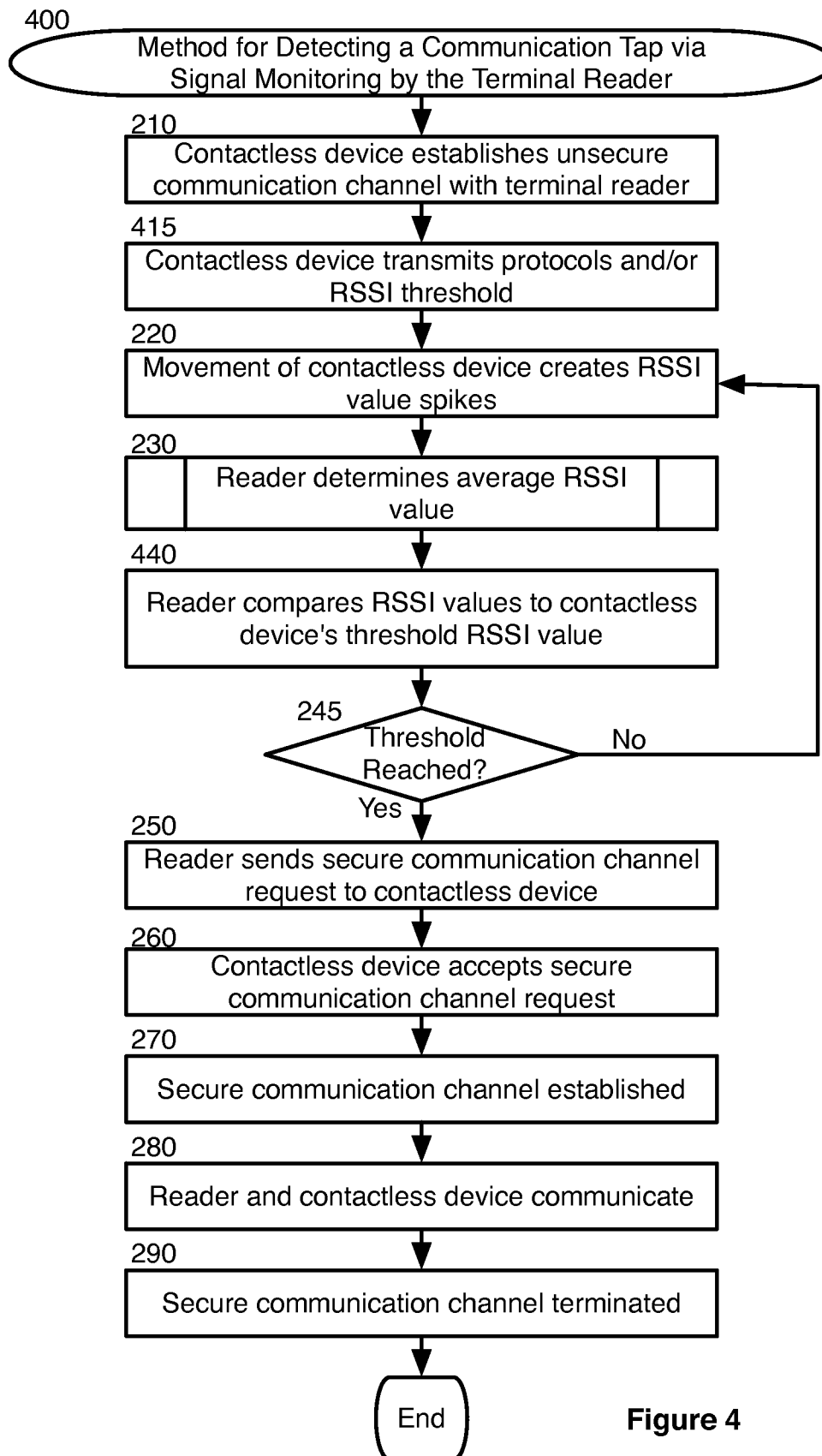


Figure 4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2013/035861**A. CLASSIFICATION OF SUBJECT MATTER****H04B 7/24(2006.01)i, H04B 5/02(2006.01)i**

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04B 7/24;H04B 5/02; H04Q 7/38; G06Q 30/00; H04M 11/00; H04W 4/02; H04M 1/66; G06Q 20/00

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

Korean utility models and applications for utility models

Japanese utility models and applications for utility models

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

eKOMPASS(KIPO internal) & Keywords: POS, RSSI, Bluetooth, unsecure/ secure communication channel

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X A A A A A	WO 2011-127627 A1 (METROLOGIC INSTRUMENTS, INC.) 20 October 2011 See paras. 2, 12, 17, 20-21, 31, 35-37, 43; claims 1, 6; and fig. 1. US 2008-0051059 A1 (MICHELLE FISHER) 28 February 2008 See paras. 25, 113, 116-120, 122; claim 1; and figs. 1, 5, 6A-6D. US 2010-0257033 A1 (JOHN R. ROBERTS et al.) 7 October 2010 See paras. 34-38, 46, 63; claim 1; and figs. 1, 3, 6, 7, 9. US 2011-0173073 A1 (TIEHONG WANG et al.) 14 July 2011 See paras. 23-27, 31-33, 36-38; claims 1, 5; and fig. 3. US 2008-0085698 A1 (JAMES GAMM) 10 April 2008 See paras. 6-10, 26-31; claims 1-2; and fig. 1.	1-2, 4-5, 7-11, 13-20 , 22-23, 25 3, 6, 12, 21, 24 1-25 1-25 1-25 1-25



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 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

21 June 2013 (21.06.2013)

Date of mailing of the international search report

24 June 2013 (24.06.2013)

Name and mailing address of the ISA/KR

Korean Intellectual Property Office
189 Cheongsu-ro, Seo-gu, Daejeon Metropolitan City,
302-701, Republic of Korea

Facsimile No. 82-42-472-7140

Authorized officer

KANG, Hee Gok

Telephone No. 82-42-481-8264



INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/US2013/035861

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2011-127627 A1	20.10.2011	CN102934466 A	13.02.2013
US 2008-0051059 A1	28.02.2008	US 2007-0156436 A1	05.07.2007
		US 2008-0051122 A1	28.02.2008
		US 2008-0052192 A1	28.02.2008
		US 2008-0052233 A1	28.02.2008
		US 2010-0161403 A1	24.06.2010
		US 2011-250866 A1	13.10.2011
		US 8019365 B2	13.09.2011
		US 8190087 B2	29.05.2012
		US 8275312 B2	25.09.2012
US 2010-0257033 A1	07.10.2010	CN102378988 A	14.03.2012
		EP 2414994 A1	08.02.2012
		JP 2012-523036 A	27.09.2012
		KR 2011-0138398 A	27.12.2011
		WO 2010-114564 A1	07.10.2010
US 2011-0173073 A1	14.07.2011	CN101164322 A0	16.04.2008
		CN101237257 A	06.08.2008
		CN101237257 C0	06.08.2008
		CN101247196 A	20.08.2008
		CN101247196 C0	20.08.2008
		CN101513086 A	19.08.2009
		CN101513086 B	11.01.2012
		CN102413173 A	11.04.2012
		US 2006-0077310 A1	13.04.2006
		US 2007-0047568 A1	01.03.2007
		US 2007-0123215 A1	31.05.2007
		US 2007-0287498 A1	13.12.2007
		US 2010-0057887 A1	04.03.2010
		US 2010-0191593 A1	29.07.2010
		US 2011-0149148 A1	23.06.2011
		US 7603131 B2	13.10.2009
		US 7647024 B2	12.01.2010
		US 7899492 B2	01.03.2011
		US 7957733 B2	07.06.2011
		US 7983616 B2	19.07.2011
		US 8050711 B2	01.11.2011
		US 8073468 B2	06.12.2011
		US 8285211 B2	09.10.2012
		WO 2006-020119 A2	23.02.2006
		WO 2007-021910 A2	22.02.2007
US 2008-0085698 A1	10.04.2008	None	