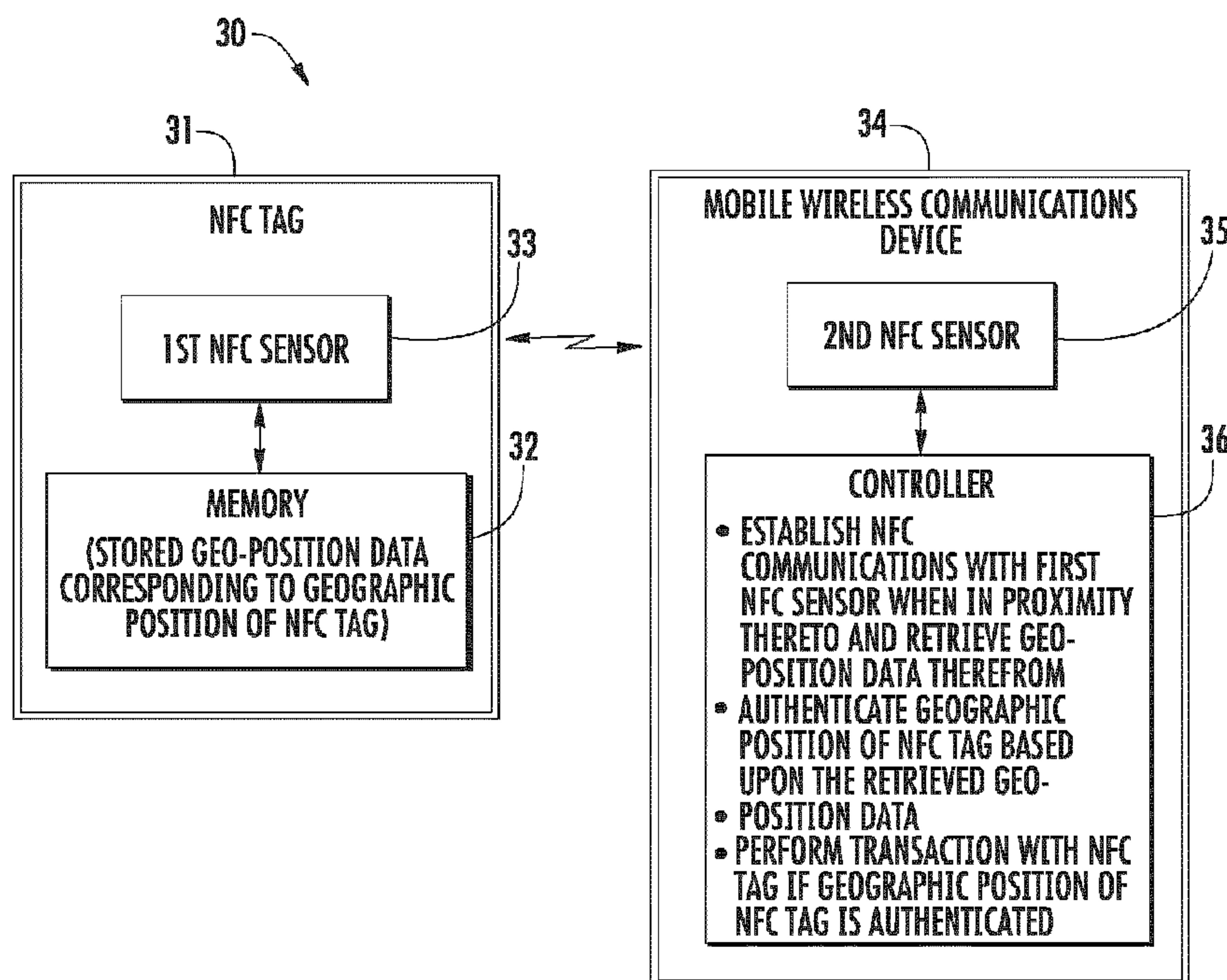




(86) Date de dépôt PCT/PCT Filing Date: 2011/10/13
 (87) Date publication PCT/PCT Publication Date: 2012/04/19
 (45) Date de délivrance/Issue Date: 2016/05/10
 (85) Entrée phase nationale/National Entry: 2013/04/11
 (86) N° demande PCT/PCT Application No.: CA 2011/050643
 (87) N° publication PCT/PCT Publication No.: 2012/048426
 (30) Priorité/Priority: 2010/10/14 (EP10187600.1)

(51) Cl.Int./Int.Cl. *H04W 84/18* (2009.01),
H04B 5/00 (2006.01), *H04W 12/10* (2009.01),
H04W 4/02 (2009.01)
 (72) Inventeur/Inventor:
 TYSOWSKI, PIOTR KONRAD, CA
 (73) Propriétaire/Owner:
 BLACKBERRY LIMITED, CA
 (74) Agent: RIDOUT & MAYBEE LLP

(54) Titre : SYSTEME DE COMMUNICATION EN CHAMP PROCHE (NFC) OFFRANT UNE AUTHENTIFICATION DE POSITION GEOGRAPHIQUE D'ETIQUETTE NFC, ET PROCESSES ASSOCIES
 (54) Title: NEAR-FIELD COMMUNICATION (NFC) SYSTEM PROVIDING NFC TAG GEOGRAPHIC POSITION AUTHENTICATION AND RELATED METHODS



(57) **Abrégé/Abstract:**

A near-field communication (NFC) system may include an NFC tag comprising a memory configured to store geo-position data corresponding to a geographic position of the NFC tag, and a first NFC sensor coupled to the memory and configured to initiate a transaction based upon NFC communications. The NFC system may further include a mobile wireless communications device comprising a second NFC sensor and a controller coupled thereto. The controller may be configured to establish NFC communications with the first NFC sensor when in proximity thereto and retrieve the geo-position data therefrom, authenticate a geographic position of the NFC tag based upon the retrieved geo-position data, and perform the transaction with the NFC tag if the geographic position of the NFC tag is authenticated.

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

(19) World Intellectual Property Organization
International Bureau(43) International Publication Date
19 April 2012 (19.04.2012)(10) International Publication Number
WO 2012/048426 A1

(51) International Patent Classification:

H04W 84/18 (2009.01) H04W 12/10 (2009.01)
H04B 5/00 (2006.01) H04W 4/02 (2009.01)

(21) International Application Number:

PCT/CA2011/050643

(22) International Filing Date:

13 October 2011 (13.10.2011)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

10187600.1 14 October 2010 (14.10.2010) EP

(71) Applicant (for all designated States except US): **RESEARCH IN MOTION LIMITED [CA/CA]**; 295 Phillip Street, Waterloo, Ontario N2L 3W8 (CA).

(72) Inventor; and

(75) Inventor/Applicant (for US only): **TYSOWSKI, Piotr Konrad [CA/CA]**; 459 Bluestream Rd., Waterloo, Ontario N2K 2R2 (CA).(74) Agent: **RIDOUT & MAYBEE LLP**; 225 King Street West, Toronto, Ontario M5V 3M2 (CA).

(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, 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, 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, MD, 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: NEAR-FIELD COMMUNICATION (NFC) SYSTEM PROVIDING NFC TAG GEOGRAPHIC POSITION AUTHENTICATION AND RELATED METHODS

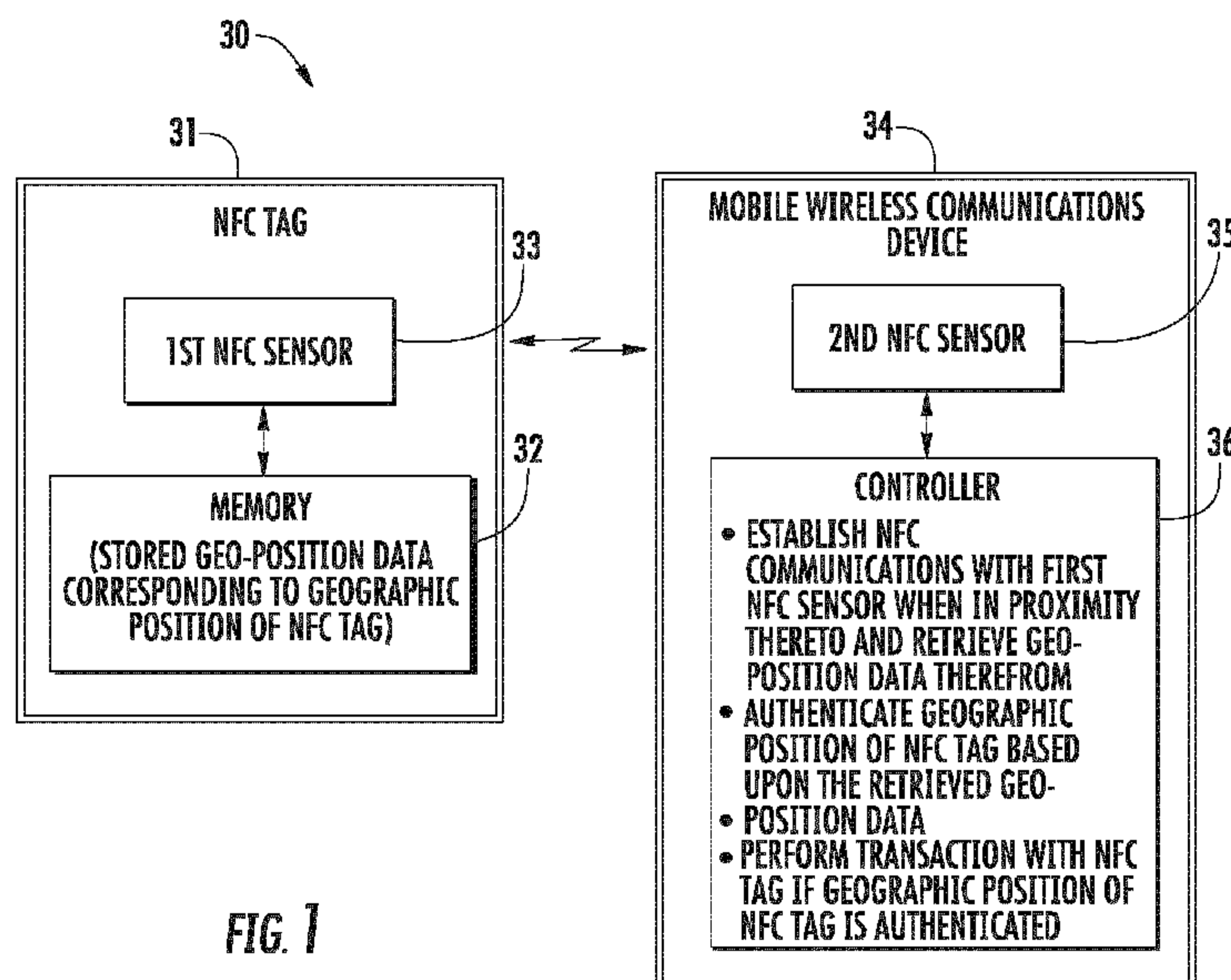


FIG. 1

(57) Abstract: A near-field communication (NFC) system may include an NFC tag comprising a memory configured to store geo-position data corresponding to a geographic position of the NFC tag, and a first NFC sensor coupled to the memory and configured to initiate a transaction based upon NFC communications. The NFC system may further include a mobile wireless communications device comprising a second NFC sensor and a controller coupled thereto. The controller may be configured to establish NFC communications with the first NFC sensor when in proximity thereto and retrieve the geo-position data therefrom, authenticate a geographic position of the NFC tag based upon the retrieved geo-position data, and perform the transaction with the NFC tag if the geographic position of the NFC tag is authenticated.

WO 2012/048426 A1

NEAR-FIELD COMMUNICATION (NFC) SYSTEM PROVIDING NFC TAG
GEOGRAPHIC POSITION AUTHENTICATION AND RELATED METHODS

5

10

15

Technical Field

[0001] This application relates to the field of communications, and more particularly, to mobile wireless communications devices and related methods that use Near Field Communication (NFC).

20

Background

[0002] Mobile communication systems continue to grow in popularity and have become an integral part of both personal and business communications. Various mobile devices now incorporate Personal Digital Assistant (PDA) features such as calendars, address books, task lists, calculators, memo and writing programs, media players, games, etc. These multi-function devices usually allow electronic mail (email) messages to be sent and received wirelessly, as well as access the internet via a cellular network and/or a wireless local area network (WLAN), for example.

25

30

[0003] Some mobile devices incorporate contactless card technology and/or near field communication (NFC) chips. NFC technology is commonly used for contactless short-range

35

communications based on radio frequency identification (RFID) standards, using magnetic field induction to enable communication between electronic devices, including mobile wireless communications devices. This short-range high
5 frequency wireless communications technology exchanges data between devices over a short distance, such as only a few centimeters.

Brief Description of the Drawings

10 [0004] FIG. 1 is a schematic block diagram of a near field communication (NFC) system providing NFC tag authentication based upon geographic position in accordance with an example embodiment.

[0005] FIG. 2 is a schematic block diagram showing the
15 system of FIG. 1 in greater detail.

[0006] FIGS. 3 and 4 are flow diagrams illustrating method aspects associated with the systems of FIGS. 1 and 2.

[0007] FIG. 5 is a schematic block diagram of an NFC system in accordance with an alternative embodiment providing NFC tag
20 geographic position determination.

[0008] FIG. 6 is a schematic block diagram showing the system of FIG. 5 in greater detail.

[0009] FIG. 7 is a schematic block diagram of an alternative embodiment of the system of FIG. 6.

25 [0010] FIGS. 8 and 9 are flow diagrams illustrating method aspects associated with the systems of FIGS. 5-7.

[0011] FIG. 10 is a schematic block diagram illustrating example components of a mobile wireless communications device that may be used with the example NFC systems of FIGS. 1-2 and
30 5-7.

Detailed Description

[0012] The present description is made with reference to the accompanying drawings, in which embodiments are shown.

However, many different embodiments may be used, and thus the description should not be construed as limited to the embodiments set forth herein. Rather, these embodiments are provided so that this disclosure will be thorough and
5 complete. Like numbers refer to like elements throughout, and prime notation is used to indicate similar elements or steps in alternative embodiments.

[0013] Generally speaking, a near-field communication (NFC) system is disclosed herein which may include an NFC tag
10 comprising a memory configured to store geo-position data corresponding to a geographic position of the NFC tag, and a first NFC sensor coupled to the memory and configured to initiate a transaction based upon NFC communications. The NFC system may further include a mobile wireless communications
15 device comprising a second NFC sensor and a controller coupled thereto. The controller may be configured to establish NFC communications with the first NFC sensor when in proximity thereto and retrieve the geo-position data therefrom, authenticate a geographic position of the NFC tag based upon
20 the retrieved geo-position data, and perform the transaction with the NFC tag if the geographic position of the NFC tag is authenticated. As such, the mobile wireless communications device may advantageously verify that the NFC tag is in its proper geographic position or location, and thus authenticate
25 the NFC tag as being secure.

[0014] More particularly, the mobile wireless communications device may further include a position determining device coupled to the controller, and the controller may be configured to authenticate the geographic
30 position of the NFC tag based upon the position determining device. By way of example, the position determining device may comprise a global positioning system (GPS) device. In other example embodiments, the position determining device may be capable of determining a position using techniques such as

radio tower triangulation, wireless network triangulation, or the like.

[0015] In addition, the mobile wireless communications device may further include a wireless transceiver coupled to the controller. Also, the controller may be further configured to communicate with an authentication server via the wireless transceiver and a wireless communications network to authenticate the geographic position of the NFC tag. By way of example, the wireless transceiver may comprise a cellular transceiver.

[0016] Also by way of example, the transaction may comprise an electronic commerce transaction. Moreover, the geo-position data may be stored in an NFC record type definition (RTD) field in an NFC Data Exchange Format (NDEF), for example. More particularly, NDEF is a binary data format that defines how RTD documents may be stored, which may include a geo-position field. The geo-position data may comprise position coordinates, or a unique identification (ID) associated with a geographic position, for example.

[0017] A related mobile wireless communications device, such as the one described briefly above, and NFC communications method are also provided. The method may include establishing NFC communications between a first NFC sensor of an NFC tag and a second NFC sensor of a mobile wireless communications device when in proximity with one another to retrieve geo-position data from a memory of the NFC tag to the mobile wireless communications device. The method may further include authenticating a geographic position of the NFC tag based upon the retrieved geo-position data at the mobile wireless communications device, and performing a transaction between the mobile wireless communications device and the NFC tag if the geographic position of the NFC tag is authenticated.

[0018] Referring initially to FIGS. 1 through 4, a near-field communication (NFC) system **30** illustratively includes an NFC tag **31** including a memory **32** configured to store geo-position data corresponding to a geographic position of the NFC tag (Blocks **50'** and **57'** of FIG. 4), and a first NFC sensor **33** coupled to the memory **32** and the first NFC sensor **33** being configured to initiate a transaction based upon NFC communications, as will be discussed further below. By way of example, the geo-position data may be stored in an NFC record type definition (RTD) field in an NFC Data Exchange Format (NDEF), although other suitable formats are also possible. The system **30** further illustratively includes a mobile wireless communications device **34** (also referred to as a "mobile device" herein) including a second NFC sensor **35** and a controller **36** coupled thereto.

[0019] By way of background, NFC is a short-range wireless communications technology in which NFC-enabled devices are "swiped," "bumped" or otherwise moved in close proximity to communicate. In one non-limiting example implementation, NFC may operate at 13.56 MHz and with an effective range of about 10cm, but other suitable versions of near-field communication which may have different operating frequencies, effective ranges, etc., for example, may also be used.

[0020] The controller **36** is configured to cause the second NFC sensor **35** to establish NFC communications with the first NFC sensor **33** when in proximity thereto and retrieve the geo-position data therefrom, at Blocks **51-52**. By way of example, the geo-position data may comprise position coordinates, such as latitude/longitude coordinates or scalar values, for example. Another approach is that the geo-position data may comprise a unique identification (ID) associated with a geographic position.

[0021] By way of example, as seen in FIG. 2, the mobile device **34** further illustratively includes a wireless

transceiver **37** and a position determining device **38** both coupled to the controller **36**. For example, the wireless transceiver **37** may comprise a cellular transceiver, although other suitable wireless communications formats (e.g., wireless LAN, WiMAX, etc.) may also be used. Moreover, the position determining device **38** may comprise a global positioning system (GPS) receiver, for example, although other suitable formats such as Galileo, GLONASS, etc., may also be used.

[0022] The unique ID may identify the NFC tag **31** itself (e.g., a serial number), or it may be a translated or encoded version of position coordinates. Thus, the unique ID may be used to inform the mobile device **34** where the mobile device **34** is supposed to be located, or corresponding position coordinates for the unique ID may be stored in an authentication server **40** with which the controller **36** communicates via the wireless transceiver **37**, a wireless communications network **41** (e.g., a cellular network), and a wide area network (WAN) **42**, such as the Internet. For example, the geographic position for the NFC tag **31** may be stored in a database at the authentication server **40** along with the unique ID. Using a unique ID to determine the appropriate position of given NFC tag may be advantageous in some implementation because of the relatively small memories provided on some NFC tags. For example, some NFC tags may have a 2 KB memory capacity or less, so using a relatively small unique ID helps to conserve the memory resources on the NFC tag for other data.

[0023] The controller **36** is also configured to authenticate a geographic position of the NFC tag **31** based upon the retrieved geo-position data, at Block **53**. This may be done in a variety of ways. For example, if the geo-position data stored in the memory **32** comprises position coordinates, then when the position coordinates are retrieved by the controller **36**, the controller may then compare the retrieved position

coordinates with a current geographic position provided by the position determining device **38** (Block **53'**). If the two sets of position coordinates are within a threshold distance of one another, then the position of the NFC tag **31** is authenticated.

5 In embodiments where the mobile device **34** does not include a position determining device **38**, position coordinates of the mobile device **34** may be provided by the wireless communications network **41** (such as from cellular or WiFi access point triangulation) to the controller **36** to compare
10 with the retrieved geographic position coordinates of the NFC tag **31**.

[0024] In other embodiments, the authentication of the geographic position of the NFC tag **31** may be performed by the authentication server **40**. That is, the controller **36** may be
15 further configured to communicate with the authentication server **40** via the wireless transceiver **37** and wireless communications network **41** (and, if appropriate, the wide area network **42**) to authenticate the geographic position of the NFC tag **31**. For example, if the geo-position data stored in the
20 memory **32** is a unique ID corresponding to geographic position coordinates for the NFC tag stored at the authentication server **40**, then the authentication server may compare these coordinates with the current position of the mobile device **34** (which may be obtained from the position determining device
25 **38**, triangulation, etc.) to authenticate the geo-position data, and more particularly, the geographic position of the NFC tag **31**.

[0025] If the geographic position of the NFC tag **31** is authenticated, at Block **54**, then the controller **36** performs
30 the above-noted transaction with the NFC tag **31**, at Block **55**, thus concluding the method illustrated in FIG. 3 (Block **56**). Otherwise, the controller **36** may avoid performing or participating in the transaction with the NFC tag **31**, and may also discontinue NFC communications with the NFC tag. By way

of example, the transaction may be an electronic commerce (e-commerce) transaction, such as if the NFC tag **31** is part of a ticket sales terminal, a terminal for paying fees or fares, etc. Other types of transactions may include opening a link in
5 a web browser (the link being provided by the NFC tag **31**, typically to view an advertisement - called a "smart poster"), pairing with a Bluetooth device to begin a Bluetooth session, reading a phone number to initiate a call or SMS, downloading a ringtone from the tag, etc. Also, the NFC tag **31** may provide
10 a clue as to the precise whereabouts of the mobile device **34** to help speed up GPS acquisition. More particularly, when a GPS receiver is missing, or has inaccurate estimates of, its position, velocity, or the current time, the receiver will then systematically search for all possible satellites to
15 obtain this information, which significantly increases a time to first fix (TTFF) of the current location. However, providing initial estimates of one or more of these values may provide a significant reduction in the TTFF.

[0026] Authenticating the geographic position of the NFC
20 tag **31** prior to engaging in a transaction therewith helps ensure that the NFC tag **31** is most likely in a geographic position assigned to the NFC tag **31** for security purposes, for example. That is, this authentication advantageously helps ensure that a "dummy" or otherwise unauthenticated tag is not
25 surreptitiously set up to defraud or scam mobile device users, but is instead a valid terminal known to be deployed by a trusted source (e.g., corporation, government, etc.) at the designated location. In some embodiments, both a unique ID and position coordinates may be verified for added security. Also,
30 this technique helps prevent a valid NFC tag from being stolen and re-located from its authorized location by a malicious party (and result in an unauthorized transaction taking place).

[0027] In accordance with an alternative embodiment now described with reference to FIGS. 5 through 8, an NFC system 30' illustratively includes a plurality of geographically distributed NFC tags 31', and a tag geo-position database 45' configured to store respective geographic positions of the NFC tags. As discussed above, the stored geographic positions may be latitude/longitude positions, for example.

[0028] The NFC system 30' further illustratively includes a plurality of mobile devices 34'. As similarly described above, each mobile device 34' is configured to communicate with a given NFC tag 31' when in proximity thereto, at Blocks 80-82, and determine its respective current geographic position, at Block 83. That is, upon initiating NFC communications with a respective NFC tag 31', each mobile device 34' may determine its current geographic position, for example, based upon a position determining device 38' thereof (if provided), or from a wireless communications network 41' (e.g., from triangulation), as discussed above. Considered alternatively, when a mobile device 34' is in sufficient proximity to communicate with a given NFC tag 31', their respective geographical positions may effectively be the same. That is, the above-described effective communication range for NFC may be much less than the margin of error of a typical position determining device, so when the two are engaged in NFC communications their respective geographic positions may be considered to be the same. It should be noted that the location of an NFC tag 31' may only need to be recorded when the NFC tag does not yet already have a location in its memory, or it has a location but it does not match the mobile device's location (through GPS) and there is a discrepancy that needs to be corrected. That is, once the location of a given NFC tag 31' is generally known, it need not be reported endlessly.

[0029] Accordingly, the determined current geographic position of a mobile device **34'** may be used to update the geo-position database **45'**, i.e., to provide this determined geographic position as the geographic position of the given tag **31'**, at Block **84**, thus concluding the method illustrated in FIG. 8 (Block **85**). As such, the geographic positions of the NFC tags **31'** may advantageously be provided by mobile devices **34'** that interact with the NFC tags after deployment, which may advantageously reduce the time and expense associated with deployment of the NFC tags. That is, the NFC tags **31'** merely need to be positioned in the desired location, and through normal interaction with mobile devices **34'** their respective geographic positions will be populated in the tag geo-position database **45'**. This may also advantageously facilitate the addition of new NFC tags **31'** to the system **30'**, or redeployment of NFC tags to different geographical positions as necessary.

[0030] In some embodiments, the tag geo-position database **45'** may be configured to update the stored geographic position for a given NFC tag **31'** based upon a plurality of determined current geographic positions from different mobile devices **34'**, at Blocks **86'-87'**. That is, the tag geo-position database **45'** may continue to refine the geographic position for a given NFC tag **31'** as the tag geo-position database **45'** receives new geographic position coordinates for different mobile devices **34'**. For example, if an initial geographic position estimate for the given NFC tag **31'** is generated through triangulation, the accuracy of this position estimate may be fairly low. However, as one or more mobile devices **34'** with position determining devices **38'** (e.g., GPS) relay geographic position coordinates for the given NFC tag **31'**, which are typically much more accurate than those obtained from triangulation, then the geo-position database **45'** may advantageously be updated to reflect the more accurate coordinates. This may be

done by averaging the coordinates, or replacing prior stored coordinates with new ones known to have a greater accuracy. In addition, mobile devices using different location technologies may report the respective location technology being used, or
5 an expectation of its accuracy. This may add weight to reports made using more accurate techniques such as GPS, and less weight to less accurate methods like cell tower positioning, in the averaging calculation performed at the tag geo-position database 45', the stored coordinates may comprise a weighted
10 average of several coordinates.

[0031] In the example embodiment of FIG. 6, the controller 36' communicates with the tag geo-position database 45' via its wireless transceiver 37'. However, in other embodiments, such as the one shown in FIG. 7, the mobile device 34'', and
15 the controller 36'' may instead communicate with the tag geo-position database 45'' via the NFC tag 31'', which further includes a WAN interface 46'' for interfacing the WAN 42''. That is, the mobile device 34'' may communicate with the tag geo-position database 45'' via the NFC tag 31'', or the NFC
20 tag may communicate with the geo-position database directly, with the mobile device assisting by providing a precise location (such as with GPS).

[0032] Associating geographic positions with NFC tags, as described above, may advantageously allow other operations to
25 be performed. By way of example, an NFC tag may have available Wi-Fi access point information stored therein along with its respective geographic location. The mobile device may then use a map application to indicate where the access points (or other services) are located. Another operation is using the
30 geographic position of an NFC tag at a landmark to geocode information on the mobile device (e.g., geocode a picture taken in that location by swiping the mobile device with the NFC tag).

[0033] Yet another advantageous aspect is that of associating geographic position information with contacts, etc., for reader-to-reader applications. Thus, for example, when contact information is exchanged between mobile devices at a particular location, such as a trade show, etc., the location of the exchange is recorded along with the contact, allowing all contacts obtained from that location to be searched and grouped together accordingly. Another approach is to use the geographic position in an NFC tag to generate calendar appointments. For example, swiping a mobile device to an NFC tag at a doctor's office may assign a calendar entry to the mobile device with location information included for a next appointment.

[0034] Still another advantageous aspect of storing geographic position information for an NFC tag is that the NFC tag may be positioned at a location to convey direction information within a building, etc., where satellite position information is not available. For example, an NFC tag with its respective geographic position information stored therein may be positioned at a gate in an airport that faces north. When an arriving passenger exits the gate, swiping the NFC tag with the mobile device allows directions to be provided based upon the direction the mobile device is facing at that particular moment (i.e., north), so that the mobile device may present a prompt requesting a user of the mobile device to go "right" or "left" depending on whether the user's next destination is a connecting flight, ground transportation, etc. Such information is typically more helpful inside of a building than "east" or "west" directions, for example, as the direction of east or west within a building may not be readily apparent.

[0035] Still another application is storing multiple geographic positions on an NFC tag. By way of example, for an NFC tag at a customer service or point of sale (POS) station,

if a user swipes this NFC tag with a mobile device and the station in unattended or closed, directions to another station (e.g., the next closest station) are provided. Similarly, recording the location at a POS terminal may be used to later search a sales transaction by location, for expense reporting purposes, etc.

[0036] Example components of a mobile wireless communications device **1000** that may be used in accordance with the above-described embodiments are further described below with reference to FIG. 10. The device **1000** illustratively includes a housing **1200**, a keyboard or keypad **1400** and an output device **1600**. The output device shown is a display **1600**, which may comprise a full graphic LCD. Other types of output devices may alternatively be utilized. A processing device **1800** is contained within the housing **1200** and is coupled between the keypad **1400** and the display **1600**. The processing device **1800** controls the operation of the display **1600**, as well as the overall operation of the mobile device **1000**, in response to actuation of keys on the keypad **1400**.

[0037] The housing **1200** may be elongated vertically, or may take on other sizes and shapes (including clamshell housing structures). The keypad may include a mode selection key, or other hardware or software for switching between text entry and telephony entry.

[0038] In addition to the processing device **1800**, other parts of the mobile device **1000** are shown schematically in FIG. 10. These include a communications subsystem **1001**; a short-range communications subsystem **1020**; the keypad **1400** and the display **1600**, along with other input/output devices **1060**, **1080**, **1100** and **1120**; as well as memory devices **1160**, **1180** and various other device subsystems **1201**. The mobile device **1000** may comprise a two-way RF communications device having data and, optionally, voice communications capabilities. In

addition, the mobile device **1000** may have the capability to communicate with other computer systems via the Internet.

[0039] Operating system software executed by the processing device **1800** is stored in a persistent store, such as the flash memory **1160**, but may be stored in other types of memory devices, such as a read only memory (ROM) or similar storage element. In addition, system software, specific device applications, or parts thereof, may be temporarily loaded into a volatile store, such as the random access memory (RAM) **1180**.
5
10 Communications signals received by the mobile device may also be stored in the RAM **1180**.

[0040] The processing device **1800**, in addition to its operating system functions, enables execution of software applications **1300A-1300N** on the device **1000**. A predetermined set of applications that control basic device operations, such as data and voice communications **1300A** and **1300B**, may be installed on the device **1000** during manufacture. In addition, a personal information manager (PIM) application may be installed during manufacture. The PIM may be capable of
15
20 organizing and managing data items, such as e-mail, calendar events, voice mails, appointments, and task items. The PIM application may also be capable of sending and receiving data items via a wireless network **1401**. The PIM data items may be seamlessly integrated, synchronized and updated via the
25 wireless network **1401** with corresponding data items stored or associated with a host computer system.

[0041] Communication functions, including data and voice communications, are performed through the communications subsystem **1001**, and possibly through the short-range
30 communications subsystem. The communications subsystem **1001** includes a receiver **1500**, a transmitter **1520**, and one or more antennas **1540** and **1560**. In addition, the communications subsystem **1001** also includes a processing module, such as a digital signal processor (DSP) **1580**, and local oscillators

(LOs) **1601**. The specific design and implementation of the communications subsystem **1001** is dependent upon the communications network in which the mobile device **1000** is intended to operate. For example, a mobile device **1000** may include a communications subsystem **1001** designed to operate with the Mobitex™, Data TAC™ or General Packet Radio Service (GPRS) mobile data communications networks, and also designed to operate with any of a variety of voice communications networks, such as AMPS, TDMA, CDMA, WCDMA, PCS, GSM, EDGE, etc. Other types of data and voice networks, both separate and integrated, may also be utilized with the mobile device **1000**. The mobile device **1000** may also be compliant with other communications standards such as 3GSM, 3GPP, UMTS, 4G, etc.

[0042] Network access requirements vary depending upon the type of communication system. For example, in the Mobitex and DataTAC networks, mobile devices are registered on the network using a unique personal identification number or PIN associated with each device. In GPRS networks, however, network access is associated with a subscriber or user of a device. A GPRS device therefore typically involves use of a subscriber identity module, commonly referred to as a SIM card, in order to operate on a GPRS network.

[0043] When required network registration or activation procedures have been completed, the mobile device **1000** may send and receive communications signals over the communication network **1401**. Signals received from the communications network **1401** by the antenna **1540** are routed to the receiver **1500**, which provides for signal amplification, frequency down conversion, filtering, channel selection, etc., and may also provide analog to digital conversion. Analog-to-digital conversion of the received signal allows the DSP **1580** to perform more complex communications functions, such as demodulation and decoding. In a similar manner, signals to be transmitted to the network **1401** are processed (e.g. modulated

and encoded) by the DSP **1580** and are then provided to the transmitter **1520** for digital to analog conversion, frequency up conversion, filtering, amplification and transmission to the communication network **1401** (or networks) via the antenna

5 **1560**.

[0044] In addition to processing communications signals, the DSP **1580** provides for control of the receiver **1500** and the transmitter **1520**. For example, gains applied to communications signals in the receiver **1500** and transmitter **1520** may be

10 adaptively controlled through automatic gain control algorithms implemented in the DSP **1580**.

[0045] In a data communications mode, a received signal, such as a text message or web page download, is processed by the communications subsystem **1001** and is input to the

15 processing device **1800**. The received signal is then further processed by the processing device **1800** for an output to the display **1600**, or alternatively to some other auxiliary I/O device **1060**. A device may also be used to compose data items, such as e-mail messages, using the keypad **1400** and/or some
20 other auxiliary I/O device **1060**, such as a touchpad, a rocker switch, a thumb-wheel, or some other type of input device. The composed data items may then be transmitted over the communications network **1401** via the communications subsystem **1001**.

25 [0046] In a voice communications mode, overall operation of the device is substantially similar to the data communications mode, except that received signals are output to a speaker **1100**, and signals for transmission are generated by a microphone **1120**. Alternative voice or audio I/O subsystems,
30 such as a voice message recording subsystem, may also be implemented on the device **1000**. In addition, the display **1600** may also be utilized in voice communications mode, for example to display the identity of a calling party, the duration of a voice call, or other voice call related information.

[0047] The short-range communications subsystem enables communication between the mobile device **1000** and other proximate systems or devices, which need not necessarily be similar devices. For example, the short-range communications subsystem may include an infrared device and associated circuits and components, a Bluetooth™ communications module to provide for communication with similarly-enabled systems and devices, or a near field communications (NFC) sensor for communicating with a NFC device or NFC tag via NFC communications.

[0048] Many modifications and other embodiments will come to the mind of one skilled in the art having the benefit of the teachings presented in the foregoing descriptions and the associated drawings. Therefore, it is understood that various modifications and embodiments are intended to be included within the scope of the appended claims.

THAT WHICH IS CLAIMED IS:

CLAIMS:

- 5 1. A near-field communication NFC system (30)
comprising:
 a NFC tag (31) comprising
 a memory (32) configured to store geo-position
 data corresponding to a geographic position of said
10 NFC tag, and
 a first NFC sensor (33) coupled to said memory
 and configured to initiate a transaction based upon
 NFC communications; and
 a mobile wireless communications device (34)
15 comprising a second NFC sensor (35) and a controller (36)
 coupled thereto, the controller being configured to
 cause said second NFC sensor to establish NFC
 communications with said first NFC sensor when in
 proximity thereto and retrieve the stored geo-
20 position data therefrom,
 authenticate a geographic position of said NFC
 tag based upon a comparison between the retrieved
 geo-position data and a current geographic position,
 and
25 perform the transaction with said NFC tag if
 the geographic position of said NFC tag is
 authenticated.
2. The NFC system (30) of Claim 1 wherein said
30 mobile wireless communications device (34) further comprises a
 position determining device (38) coupled to said controller
 (36) and configured to determine the current geographic
 position.

3. The NFC system (30) of Claim 2 wherein said position determining device (38) comprises a global positioning system GPS device.

5 4. The NFC system (30) of Claim 1 wherein said mobile wireless communications device further comprises a wireless transceiver (37) coupled to said controller (36); and wherein said controller (30) is further configured to
10 wireless transceiver and a wireless communications network (41) to authenticate the geographic position of said NFC tag (31).

15 5. The NFC system (30) of Claim 4 wherein said wireless transceiver (37) comprises a cellular transceiver.

20 6. The NFC system (30) of Claim 4 wherein said wireless transceiver (37) comprises a wireless local area network WLAN transceiver.

7. The NFC system (30) of Claim 1 wherein the transaction comprises an electronic commerce transaction.

25 8. The NFC system (30) of Claim 1 wherein the geo-position data is stored in an NFC record type definition RTD field in an NFC Data Exchange Format NDEF.

9. A mobile wireless communications device (34) comprising:
30 a near field communications ~~(NFC)~~ device (35); and
a controller (36) coupled with the NFC device, the controller being configured to
cause the NFC device to establish NFC
communications with a NFC tag (31) when in proximity

thereto and retrieve stored geo-position data
therefrom,

5 authenticate a geographic position of the NFC
tag based upon a comparison between the retrieved
geo-position data and a current geographic position,
and

 perform a transaction with the NFC tag if the
geographic position of the NFC tag is authenticated.

10 10. The mobile wireless communications device (34)
of Claim 9 further comprising a position determining device
(38) coupled to said controller (36) and configured to
determine the current geographic position.

15 11. The mobile wireless communications device (34)
of Claim 9 further comprising a wireless transceiver (37)
coupled to said controller (36); and wherein said controller
is further configured to communicate with an authentication
server (40) via said wireless transceiver and a wireless
20 communications network (41) to authenticate the geographic
position of the NFC tag.

 12. A near-field communication NFC method
comprising:

25 establishing NFC communications between a first NFC
sensor (33) of a NFC tag (31) and a second NFC sensor (35) of
a mobile wireless communications device (34) when in proximity
with one another to retrieve stored geo-position data from a
memory (32) of the NFC tag to the mobile wireless
30 communications device;

 authenticating a geographic position of the NFC tag
based upon a comparison between the retrieved geo-position
data and a current geographic position at the mobile wireless
communications device; and

performing a transaction between the mobile wireless communications device and the NFC tag if the geographic position of the NFC tag is authenticated.

5 13. The method of Claim 12 wherein the mobile wireless communications device (34) further comprises a position determining device (38) coupled to the controller (36) and configured to determine the current geographic position.

10

 14. The method of Claim 13 wherein the position determining device (38) comprises a global positioning system GPS device.

15

 15. The method of Claim 12 wherein the mobile wireless communications device (34) further comprises a wireless transceiver (37); and wherein authentication comprises communicating with an authentication server (40) via the wireless transceiver and a wireless communications network (41) to authenticate the geographic position of the NFC tag (31).

20

1/10

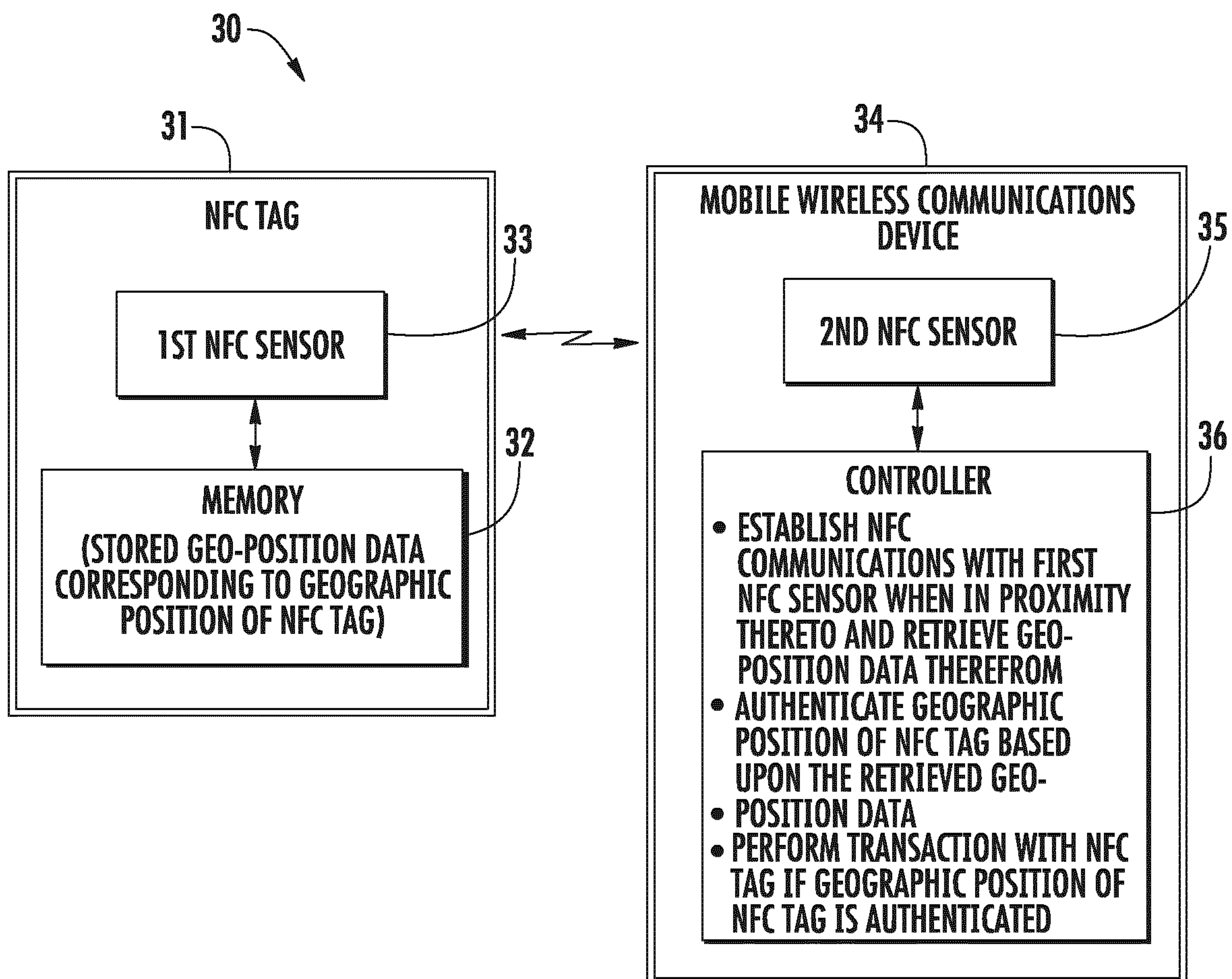


FIG. 1

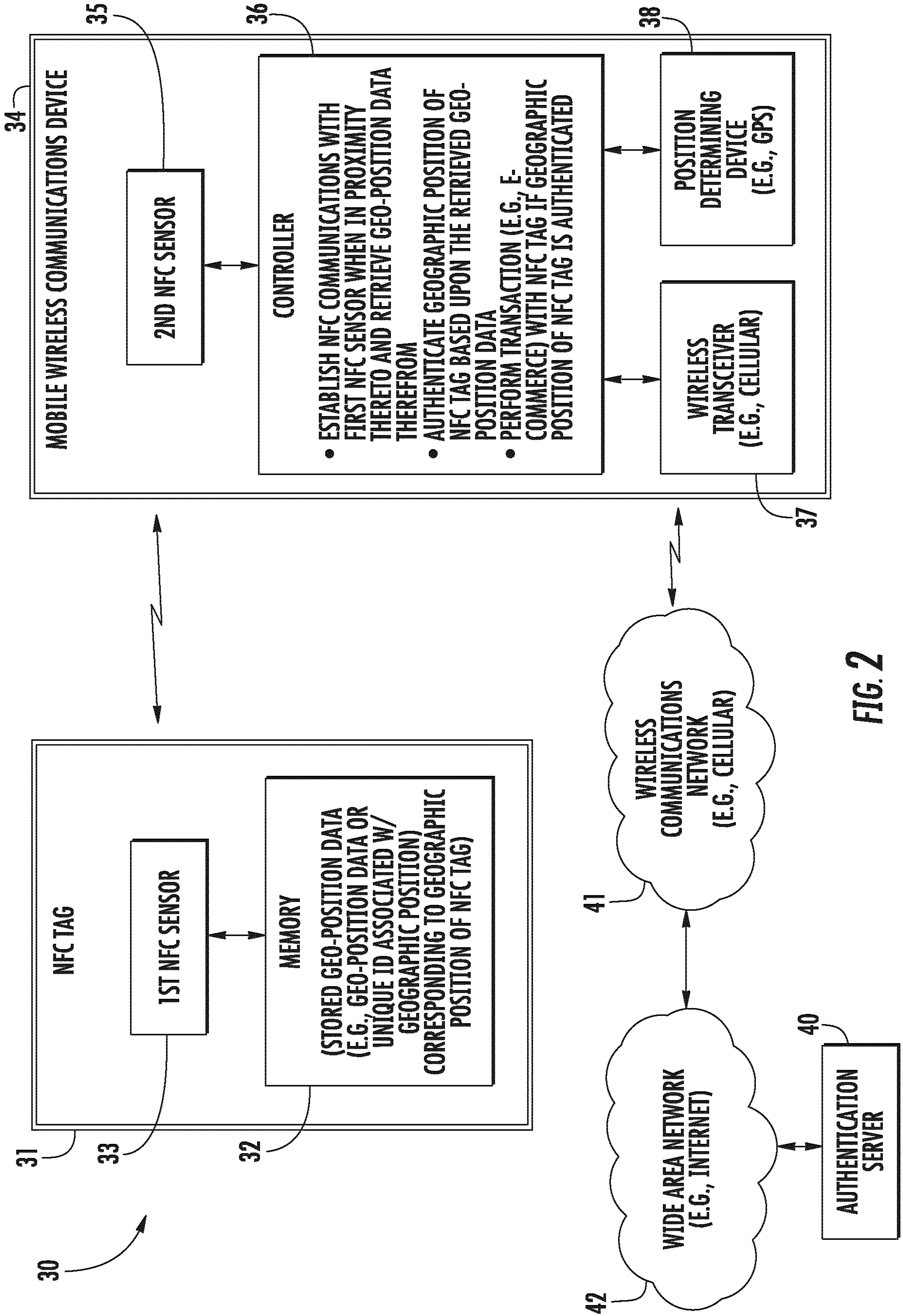
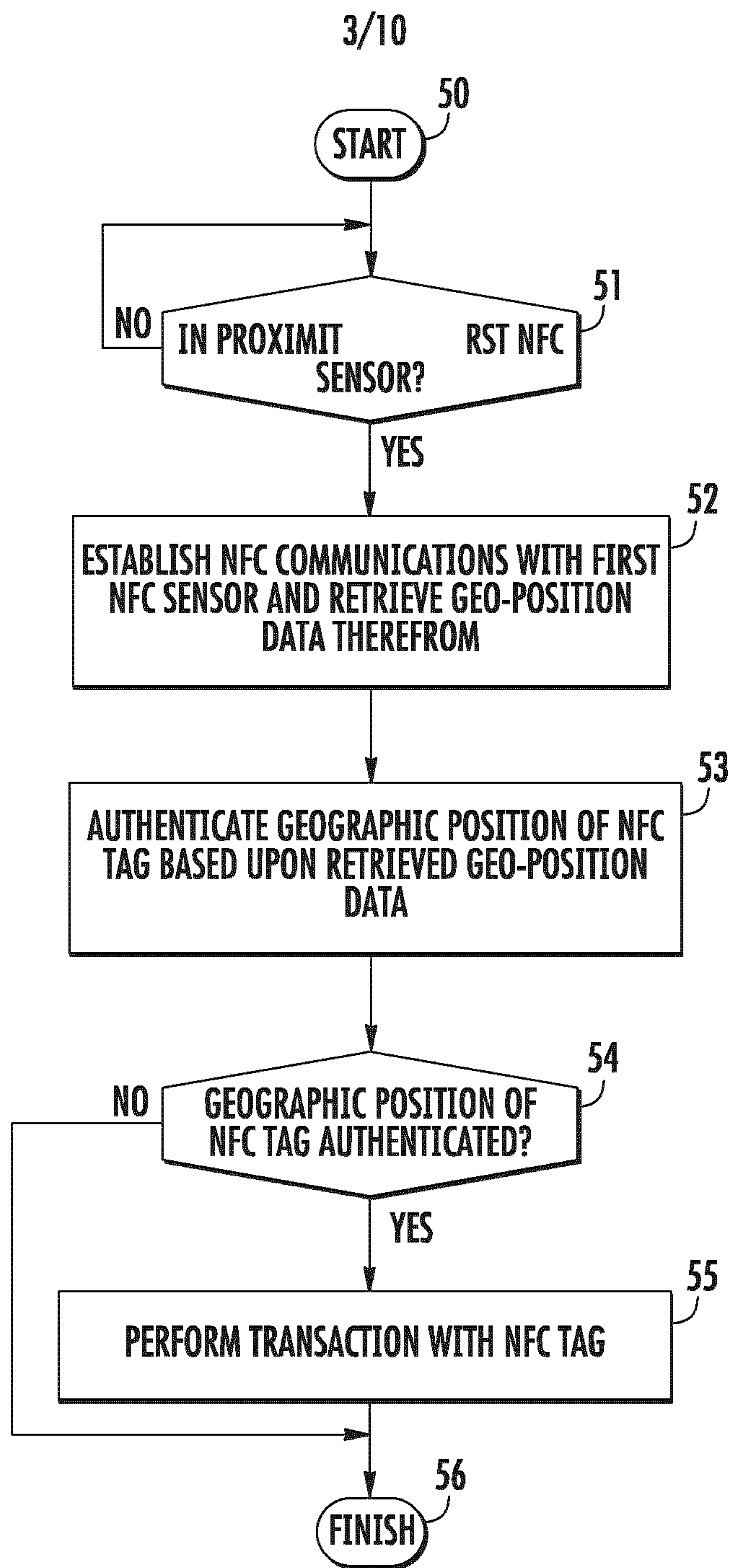


FIG. 2

**FIG. 3**

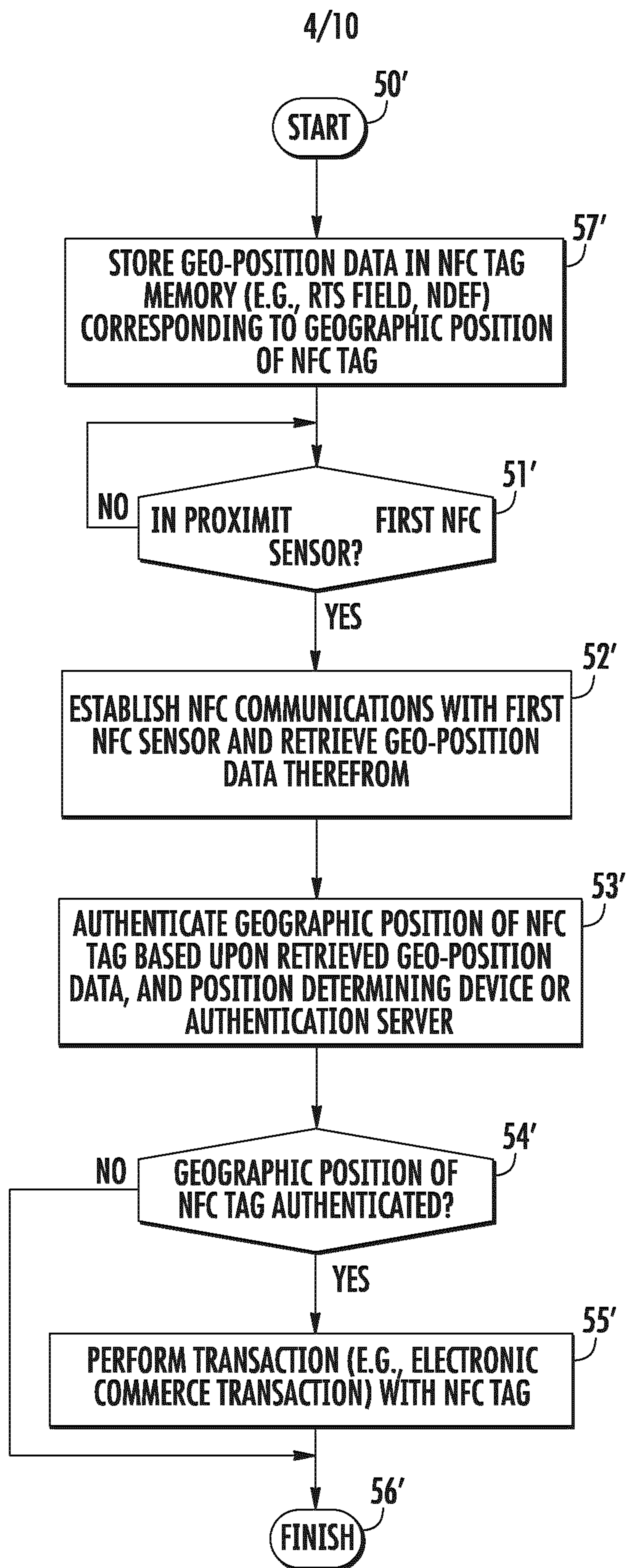


FIG. 4

5/10

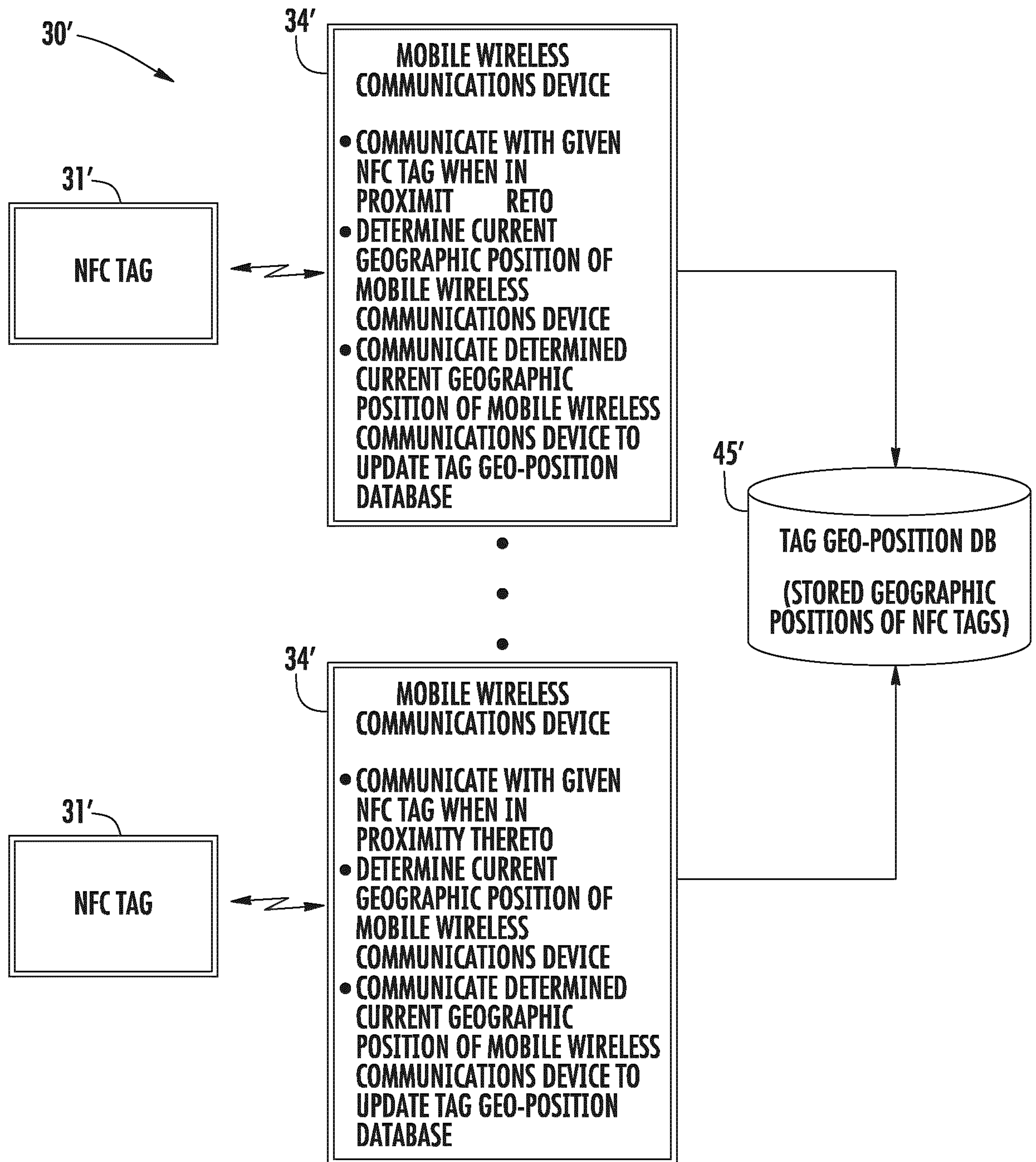


FIG. 5

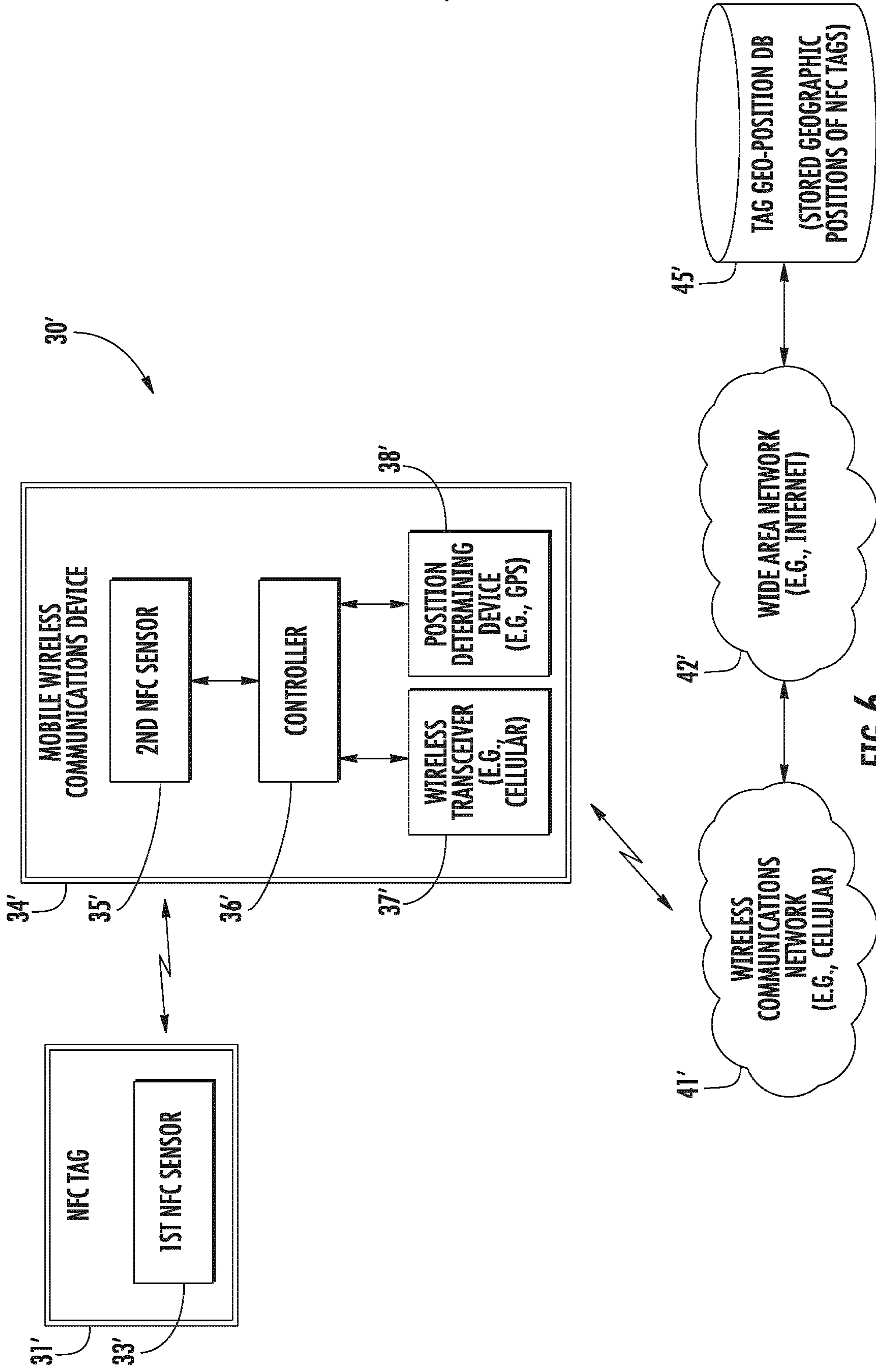


FIG. 6

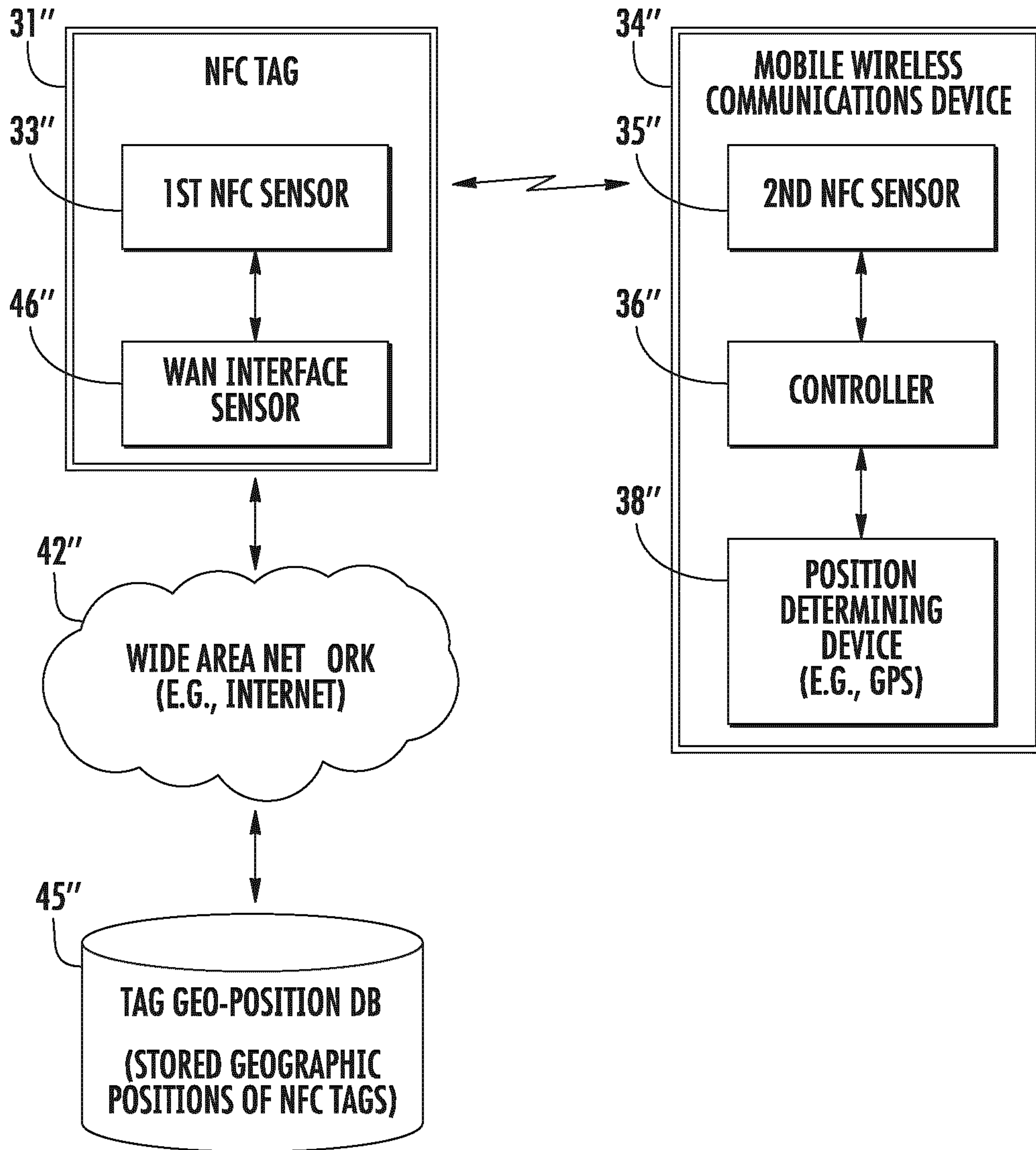
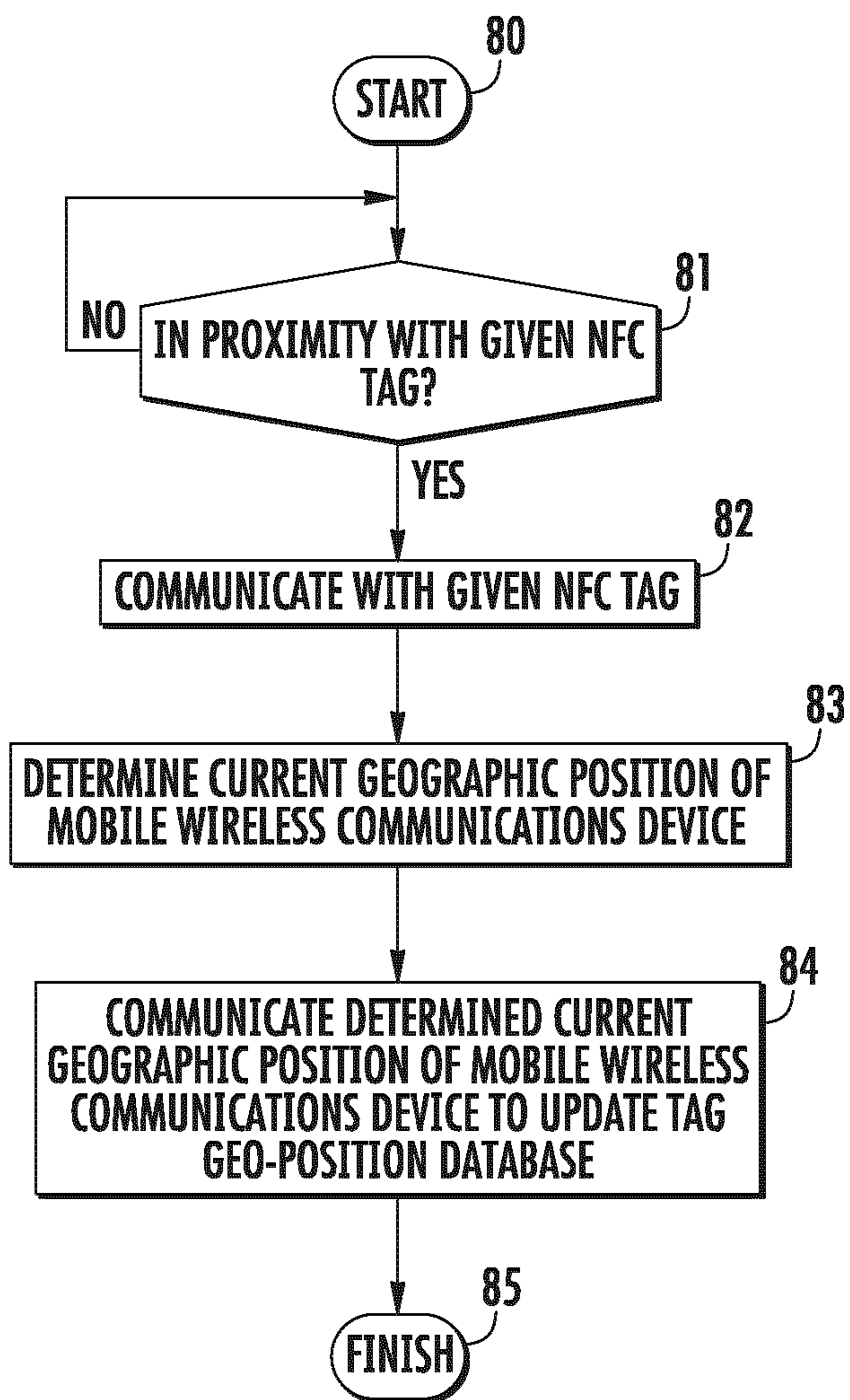


FIG. 7

8/10

**FIG. 8**

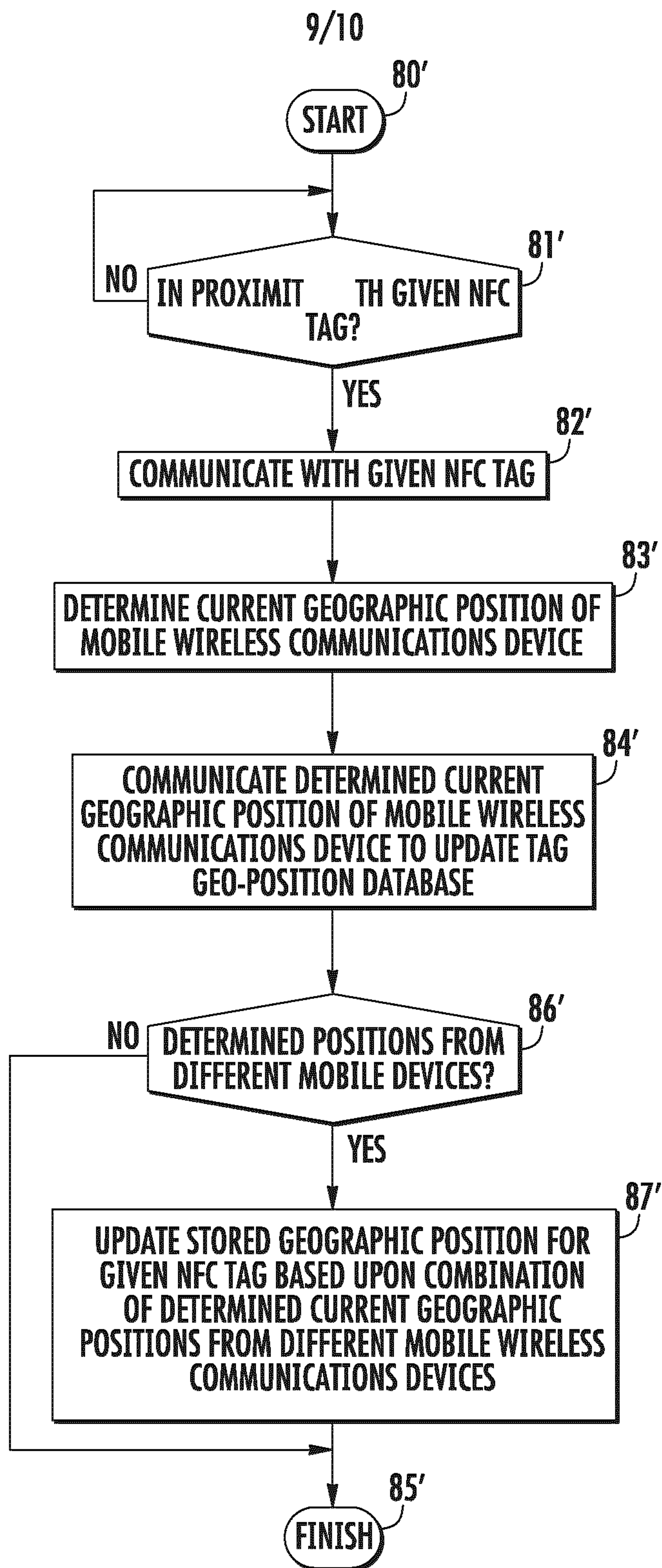


FIG. 9

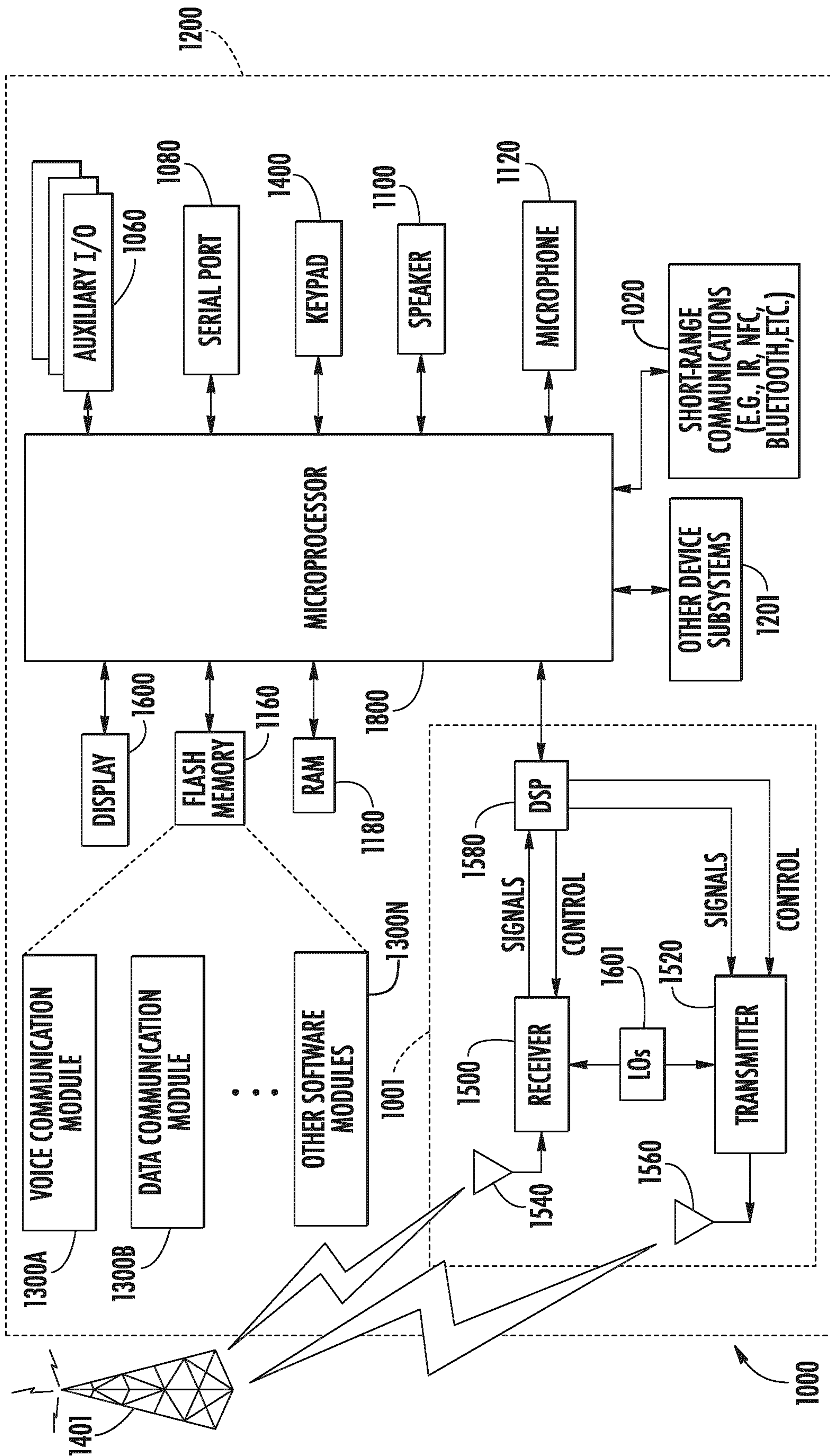


FIG. 10

