US 20170311154A1

(19) **United States**

(12) **Patent Application Publication** (10) **Pub. No.: US 2017/0311154 A1**

Nandanavanam et al. (43) **Pub. Date: Oct. 26, 2017**

(54) **SECURITY HUB UTILIZING NEAR FIELD COMMUNICATION TO ONBOARD SENSORS**

(71) Applicant: **Samsung Electronics Co., Ltd.**, Suwon-si (KR)

(72) Inventors: **Venkata Naga Vamsi Nandanavanam**, Fremont, CA (US); **Kenny Chui**, Campbell, CA (US)

(21) Appl. No.: **15/346,652**

(22) Filed: **Nov. 8, 2016**

Related U.S. Application Data

(60) Provisional application No. 62/327,795, filed on Apr. 26, 2016.

Publication Classification

(51) **Int. Cl.**

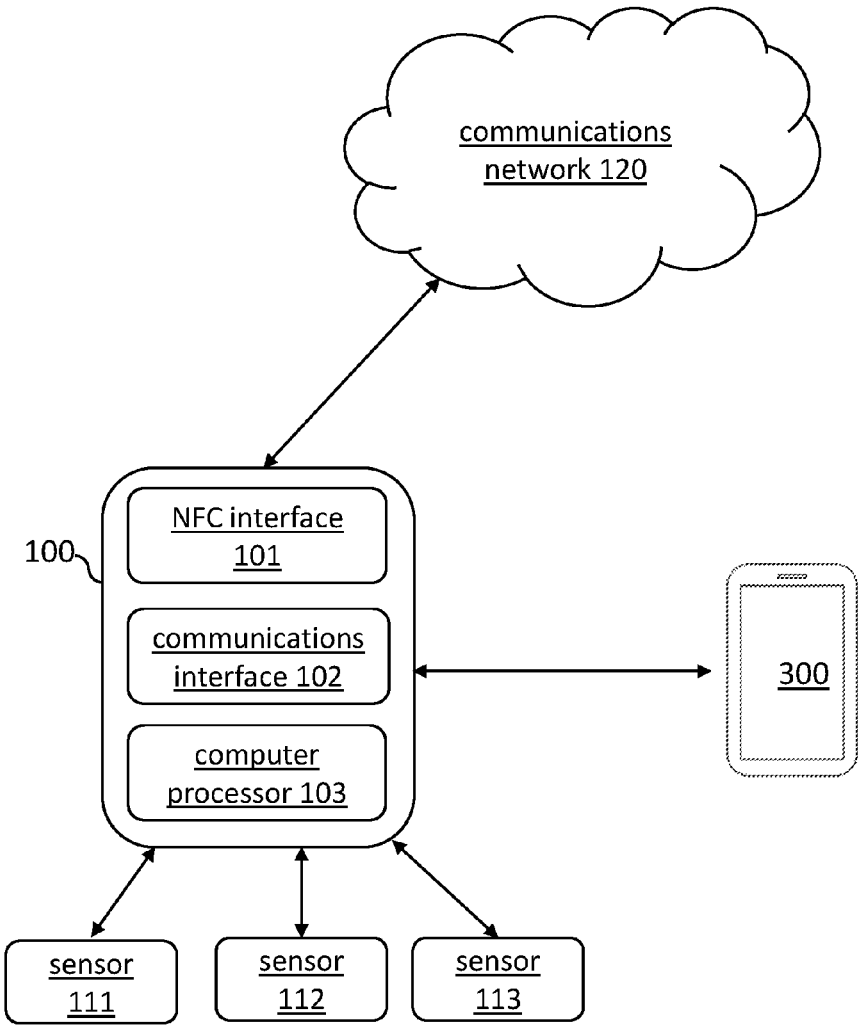
H04W 12/02	(2009.01)
H04L 29/08	(2006.01)
H04W 4/00	(2009.01)
H04W 12/08	(2009.01)

(52) **U.S. Cl.**

CPC ***H04W 12/02*** (2013.01); ***H04W 12/08*** (2013.01); ***H04L 67/12*** (2013.01); ***H04W 4/008*** (2013.01)

(57) **ABSTRACT**

According to an embodiment of the present disclosure, a security hub includes a near field communication (NFC) interface, a communications interface, and a computer processor. The NFC interface is configured to detect an NFC-enabled sensor. The communications interface is configured to establish communication with the NFC-enabled sensor, a communications network, and an electronic device. The computer processor is operatively connected to the NFC interface and the communications interface and configured to: onboard the NFC-enabled sensor, analyze detection information received from the NFC-enabled sensor, and perform an action in response to the analysis of the detection information.



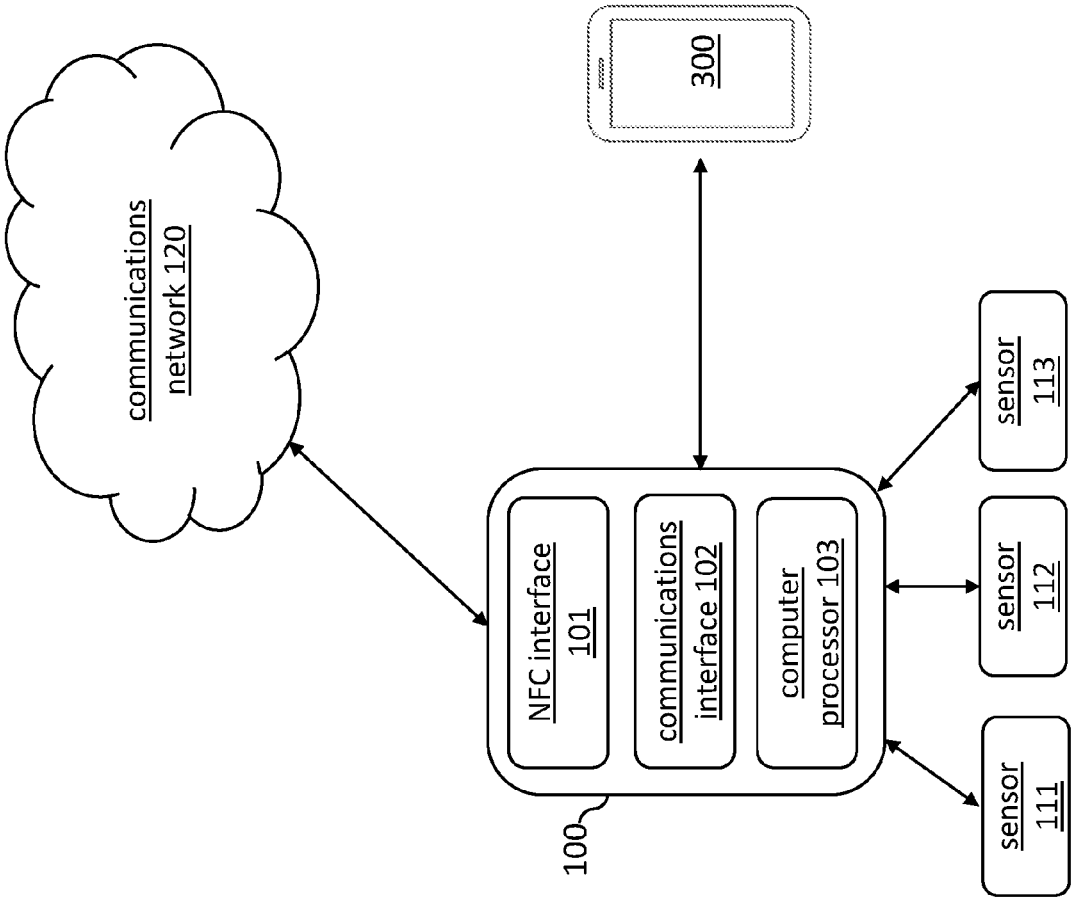

communications network 120
300
NFC interface 101
communications interface 102
computer processor 103
100
sensor 111
sensor 112
sensor 113

FIG. 1

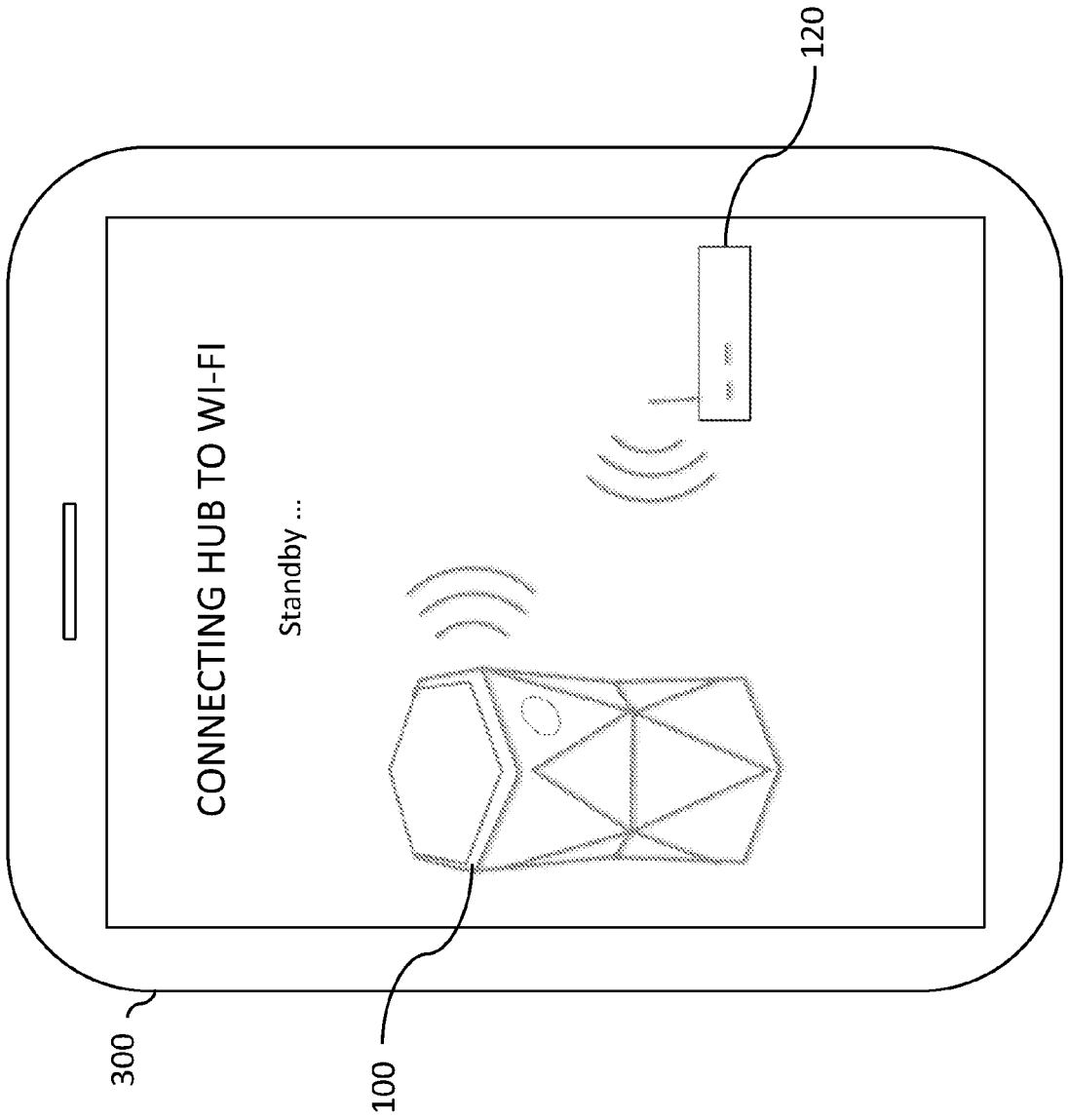


FIG. 2

FIG. 3

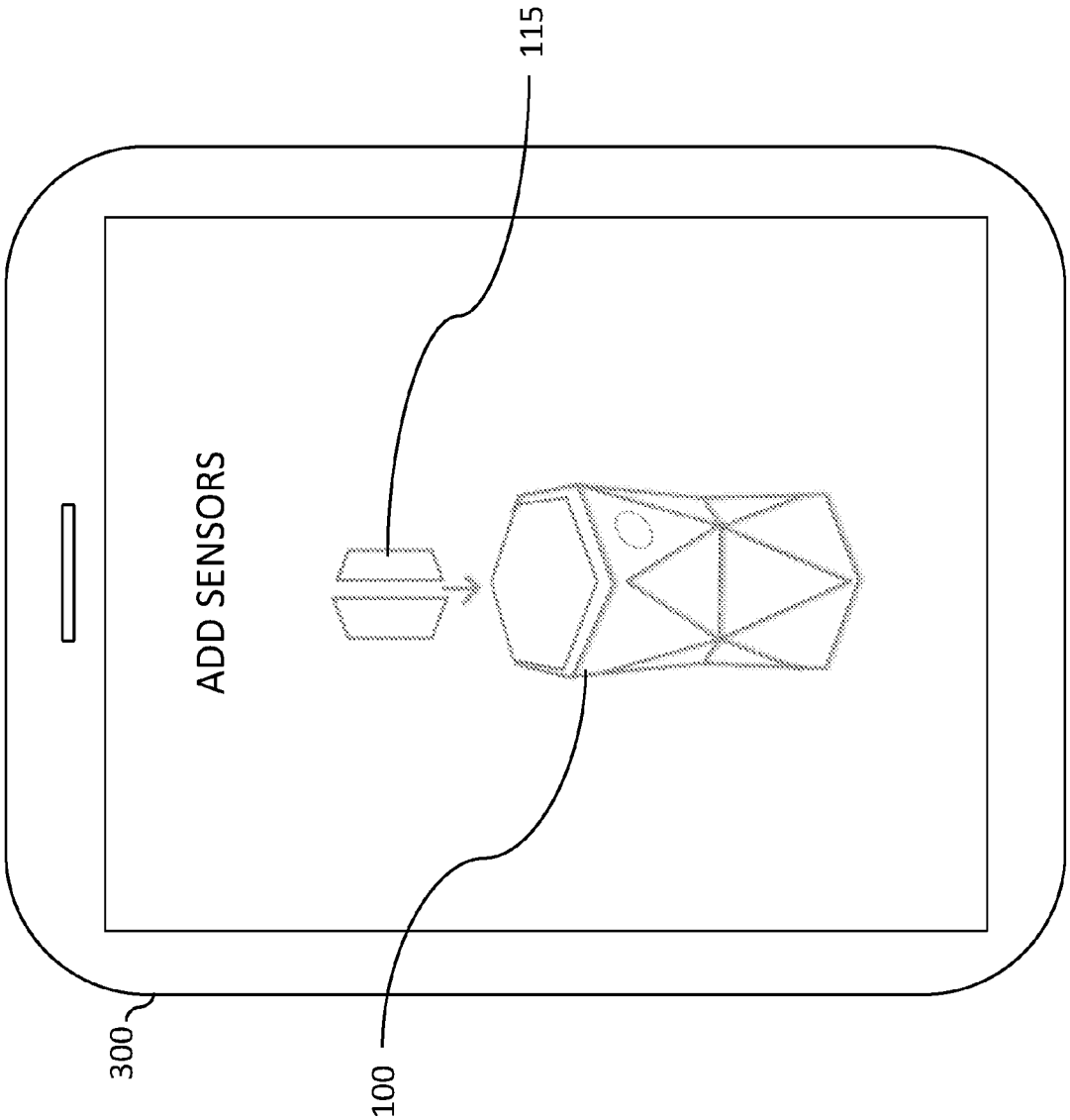
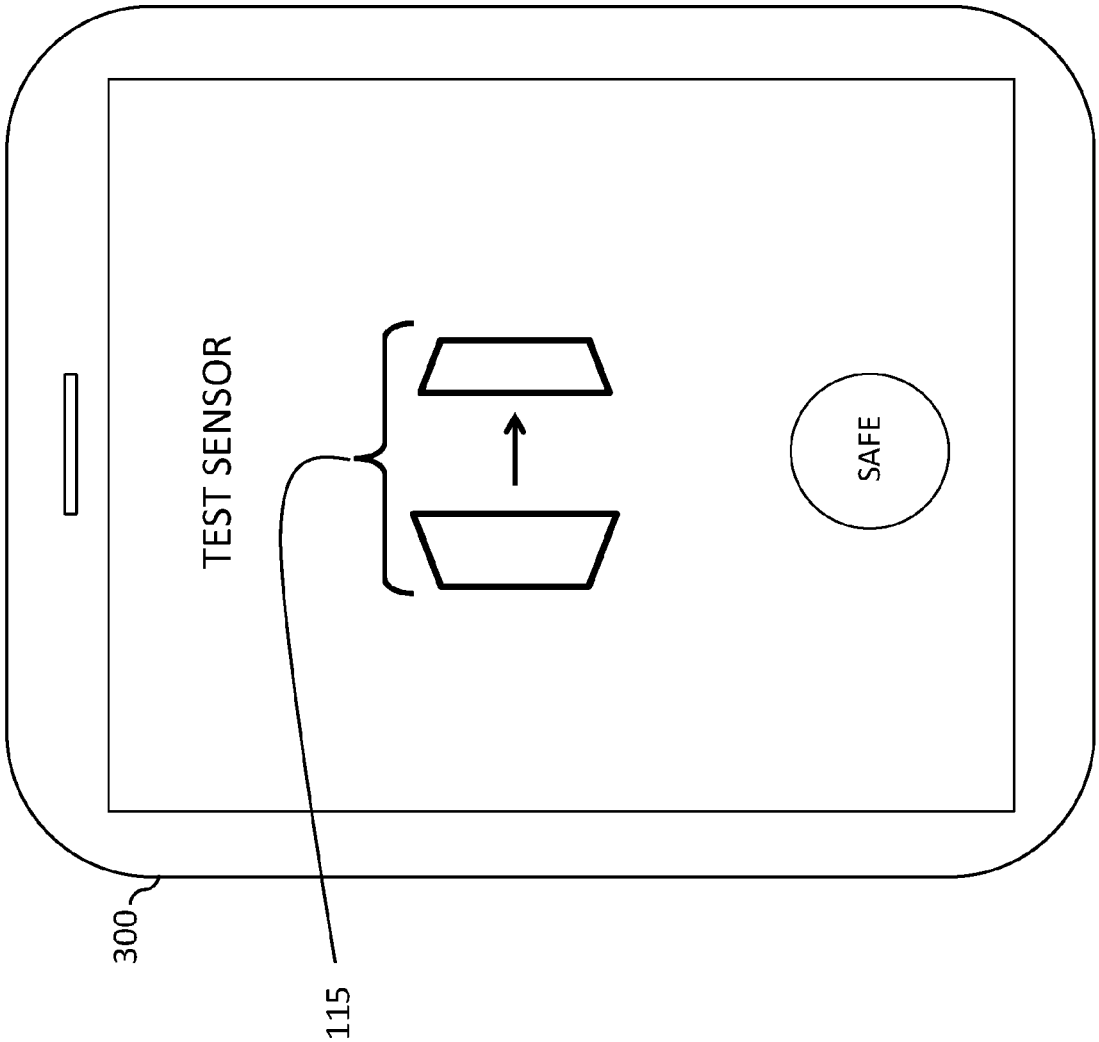


FIG. 4



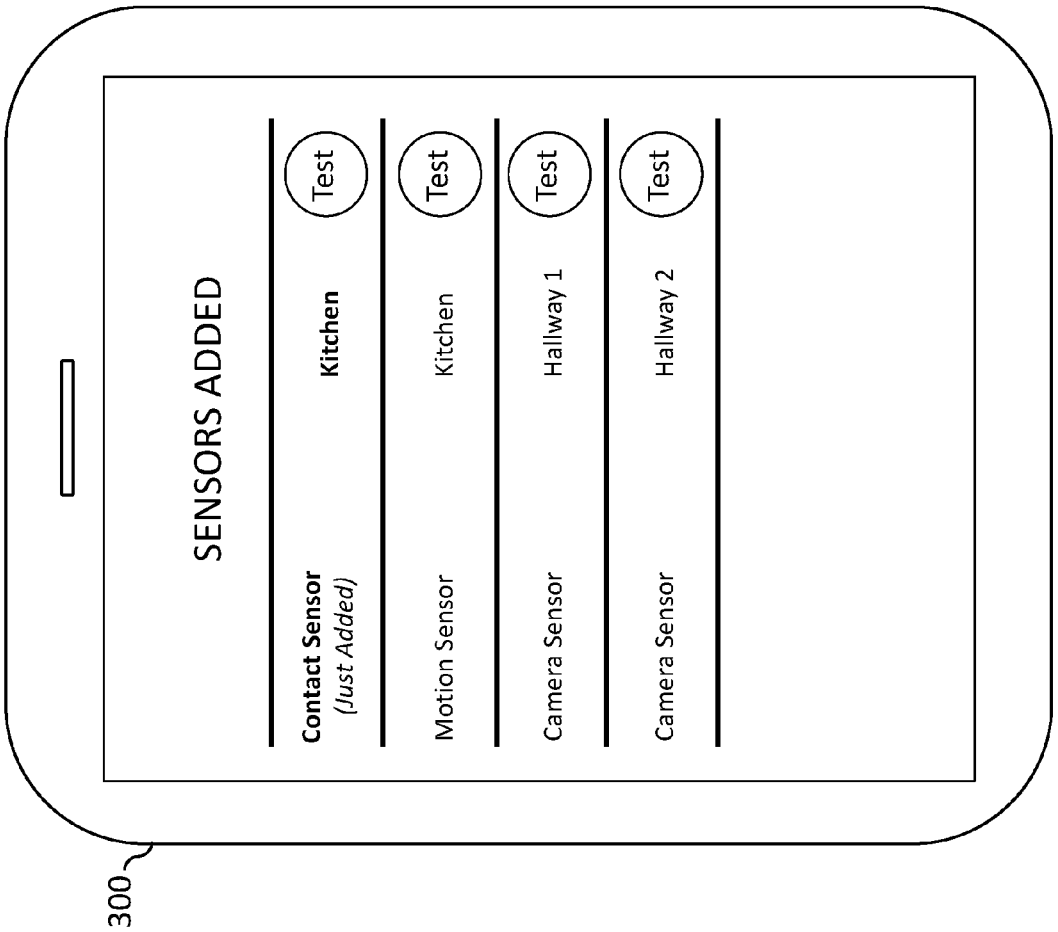
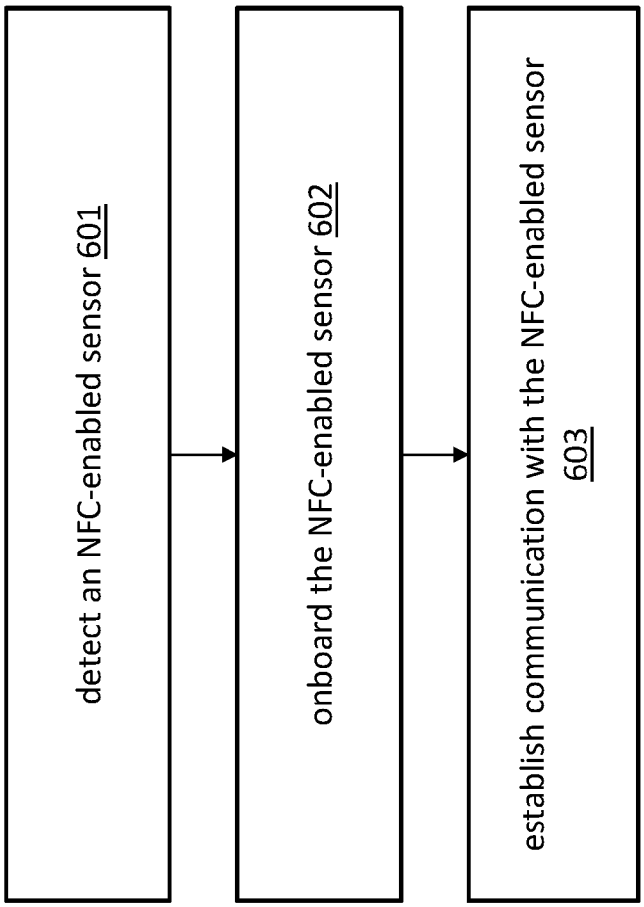

300
SENSORS ADDED
Contact Sensor (Just Added)
Kitchen
Test
Motion Sensor
Kitchen
Test
Camera Sensor
Hallway 1
Test
Camera Sensor
Hallway 2
Test

FIG. 5

FIG. 6


detect an NFC-enabled sensor 601
onboard the NFC-enabled sensor 602
establish communication with the NFC-enabled sensor 603

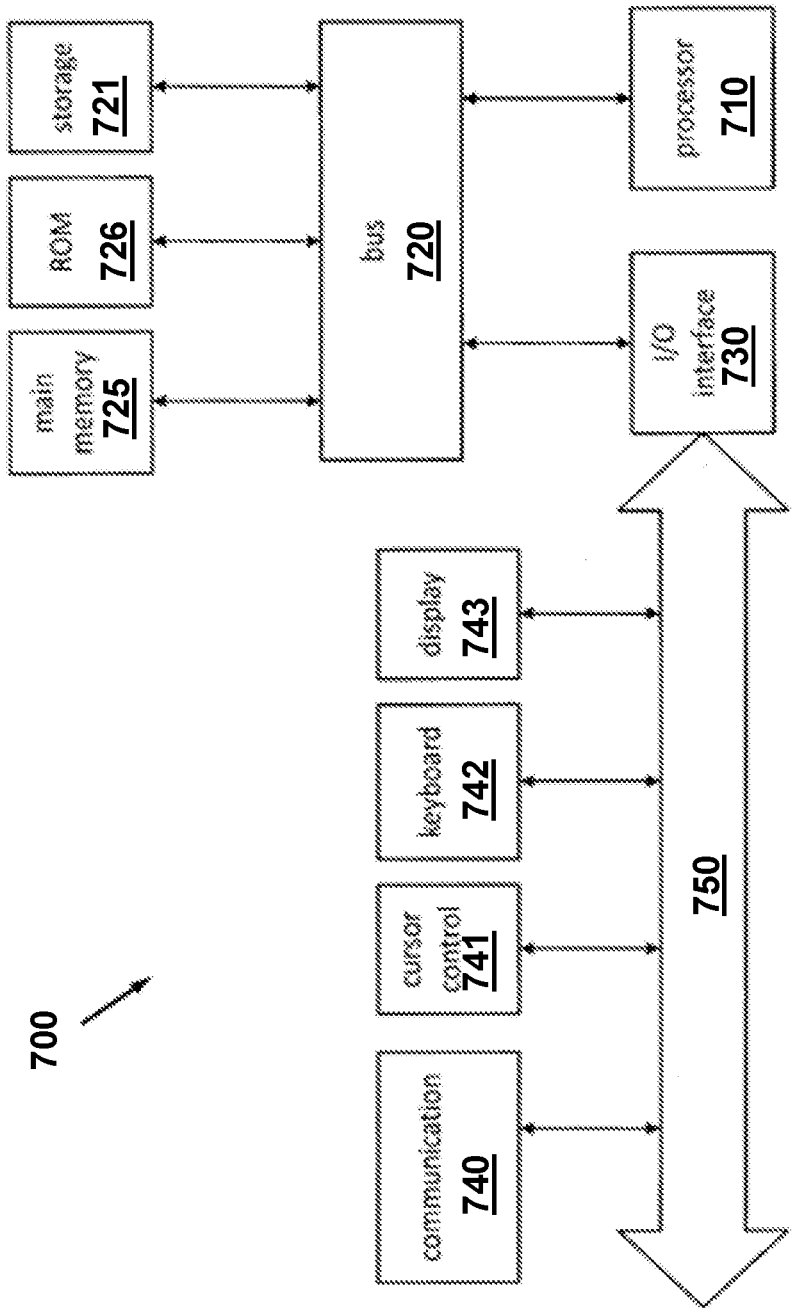

700
storage 721
ROM 726
main memory 725
bus 720
processor 710
I/O interface 730
display 743
keyboard 742
cursor control 741
communication 740
750

FIG. 7

SECURITY HUB UTILIZING NEAR FIELD COMMUNICATION TO ONBOARD SENSORS

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This application claims priority to and the benefit of U.S. Provisional Patent Application No. 62/327,795, titled "SYSTEM AND METHOD FOR PROVIDING A SECURITY HUB" and filed on Apr. 26, 2016, the entire content which is incorporated herein by reference

RELATED FIELD

[0002] The present disclosure relates in to a system and method of a security hub utilizing near field communication (NFC) to onboard sensors.

BACKGROUND

[0003] A security hub system may include one or more of a control panel and a plurality of sensors (e.g., a security camera, a motion sensor, and a contact). In recent years, there is an increasing popularity for low-cost, self-built security hub systems. However, such security hub systems are typically difficult and time-consuming to install/use. Thus, in view of the foregoing, there exists a need for the presently disclosed system and method of utilizing NFC to onboard sensors.

SUMMARY

[0004] According to an embodiment of the present disclosure, a security hub includes a near field communication (NFC) interface, a communications interface, and a computer processor. The NFC interface is configured to detect an NFC-enabled sensor. The communications interface is configured to establish communication with the NFC-enabled sensor, a communications network, and an electronic device. The computer processor is operatively connected to the NFC interface and the communications interface and configured to: onboard the NFC-enabled sensor, analyze detection information received from the NFC-enabled sensor, and perform an action in response to the analysis of the detection information.

[0005] According to an embodiment of the present disclosure, a method of connecting an NFC-enabled sensor to a security hub comprises: detecting the NFC-enabled sensor via a near field communication (NFC) interface of the security hub; establishing communication with the NFC-enabled sensor, a communications network, and an electronic device via a communications interface of security hub; onboarding the NFC-enabled sensor; and receiving detection information from the NFC-enabled sensor.

BRIEF DESCRIPTION OF THE DRAWINGS

[0006] The accompanying drawings, which are included as part of the present disclosure, illustrate various embodiments and together with the general description given above and the detailed description of the various embodiments given below serve to explain and teach the principles described herein.

[0007] FIG. **1** is a block diagram depicting an implementation of a security hub that utilizes NFC for onboarding sensors, according to an example embodiment of the disclosure.

[0008] FIG. **2** shows an example user interface of an application displaying a connection status of between a security hub and a communications network, according to an example embodiment of the present disclosure.

[0009] FIG. **3** shows an example user interface of an application displaying diagrammatic instructions for connecting sensors to the security hub using NFC, according to an example embodiment of the present disclosure.

[0010] FIG. **4** shows an example user interface of an application displaying diagrammatic instructions for testing connected sensors, according to an example embodiment of the present disclosure.

[0011] FIG. **5** shows an example user interface of an application displaying the location, type, and installation status of connected NFC-enabled sensors, according to an example embodiment of the present disclosure.

[0012] FIG. **6** shows a flowchart of high-level operations of a security hub that utilizes NFC to onboard sensors, according to an example embodiment of the present disclosure.

[0013] FIG. **7** illustrates an example computer architecture that may be used to implement embodiments of the present disclosure, for example, the security hub.

[0014] The figures in the drawings are not necessarily drawn to scale and elements of similar structures or functions are generally represented by like reference numerals for illustrative purposes throughout the figures. The figures are only intended to facilitate the description of the various embodiments described herein and do not describe every aspect of the teachings disclosed herein and do not limit the scope of the claims.

DETAILED DESCRIPTION

[0015] Each of the features and teachings disclosed herein may be utilized separately or in conjunction with other features and teachings to provide the present system and method. Representative examples utilizing many of these features and teachings, both separately and in combination, are described with reference to the attached figures. While the detailed description herein illustrates to a person of ordinary skill in the art further details for practicing aspects of the present teachings, it does not limit the scope of the claims. Therefore, combinations of features disclosed in the detailed description are representative examples of the present teachings and may not be necessary to practice the teachings in the broadest sense.

[0016] As discussed earlier, traditional security hubs are typically difficult and time-consuming to install/use. Embodiments of the present disclosure provide quick and efficient installation by allowing a user to quickly connect a security hub to a communications network (e.g., Wi-Fi), onboard one or more sensors with the security hub quickly using NFC, and test whether the sensors are connected to the security hub. NFC is a set of communications protocols that enable two devices, such as the security hub and a sensor, to establish communication by bringing them within a certain range (e.g., 4 cm) of each other.

[0017] FIG. **1** is a block diagram depicting an implementation of a security hub that utilizes NFC for onboarding sensors, according to an example embodiment of the disclosure. A security hub **100** includes an NFC interface **101**, a communications interface **102**, and a computer processor **103** (although only three components of the security hub are shown, the security hub of the present disclosure are not

limited thereto). The NFC interface **101** is configured to detect one or more NFC-enabled sensors. The NFC interface **101** may utilize the Thread network protocol.

[0018] The communications interface **102** is configured to establish communication with NFC-enabled sensors **111**, **112**, and **113**, which have already gone through the onboarding process. The communications interface **102** is also configured to establish communication with a communications network **120** (e.g., the Internet) and an electronic device **300** (e.g., a smart phone, a tablet).

[0019] The computer processor **103** is configured to onboard the detected NFC-enabled sensor. Onboarding the NFC-enabled sensor, for example, may include registering the NFC-enabled sensor and determining a communications protocol (e.g., Zigbee, Z-Wave) through which the NFC-enabled sensor transmits detection information. The computer processor **103** is also configured to analyze detection information received from the NFC-enabled sensor, and perform an action in response to the analysis of the detection information. For example, the computer processor may trigger an alarm in response to determining that there is a high security threat.

[0020] The electronic device **300** may execute and run an application that enables a user to interact with and/or control the security hub **100**. For example, the application may provide a user interface that enables the user to provide information (e.g., login information, a Wi-Fi router password) to the security hub **100** for connecting to the communications network **120**. The user interface may also displays the connection status between the security hub **100** and the communications network **120**, such as shown in FIG. **2**. The application may also provide a user interface that shows step-by-step instructions on how to onboard an NFC-enabled sensor **115** with the security hub **100**, such as shown in FIG. **3**, and/or how to connect the security hub **100** to the communications network **120**. The application may also provide a user interface that enables the user to test the operation and/or connectivity of connected NFC-enabled sensors, such as shown in FIG. **4**. The instructions may include diagrammatic instructions.

[0021] According to an example embodiment, the present system and method allow an NFC-enabled sensor (e.g., a contact sensor) to be onboarded with a security hub when the NFC-enabled sensor is brought within contact or within close proximity (e.g., within 4 centimeters (cm)) of the security hub, such as illustrated by the instructions of FIG. **3**. The security hub may receive information used for onboarding the NFC-enabled sensor entirely from the NFC-enabled sensor through its NFC interface. That is, the onboarding process between an NFC-enabled sensor and the security hub may be performed entirely without the aid of an electronic device, such as a smart phone, or an application running on the electronic device. Although not shown in FIG. **3**, the user interface may also display a connection status between the NFC-enabled sensor and the security hub.

[0022] According to an example embodiment, the present system and method allow the user to test an NFC-enabled sensor after it has been onboarded with the security hub. FIG. **4** shows an example user interface including diagrammatic instructions for testing connected sensors, according to an example embodiment of the present disclosure. For example, for testing a contact sensor, the user interface may instruct the user to place two contact parts of the sensor in contact with each other. The user interface may also provide an indication of whether contact sensor is connected and operating properly, for example, by displaying a message with the text "safe."

[0023] FIG. **5** shows an example user interface of an application displaying the location, type, and installation status of connected NFC-enabled sensors, according to an example embodiment of the present disclosure. After the user installs one or more sensors at various locations, the user interface of the application displays a type of each of the listed sensors, along with corresponding locations where the sensors are installed. The user interface also allows the user to test a working status of each of the listed sensors at each installed location. In one embodiment, the user interface further indicates an installation status (e.g., just added) of a sensor, for example, if the sensor was installed within a pre-defined period of time (e.g., previous 10 minutes).

[0024] FIG. **6** shows a flowchart of high-level operations of a security hub that utilizes NFC to onboard sensors, according to an example embodiment of the present disclosure. Although one or more components of the security hub are described below as performing the disclosed operations, the present system and method are not limited thereto, and other components of the security hub may perform those operations instead or in conjunction.

[0025] The NFC interface of the security hub detects an NFC-enabled sensor (at **601**). The computer processor of the security hub onboards the NFC-enabled sensor (at **602**). Onboarding the NFC-enabled sensor, for example, may include registering the NFC-enabled sensor and determining a communications protocol (e.g., Zigbee, Z-Wave) through which the NFC-enabled sensor transmits detection information. The communications interface of the security hub establishes communication with the NFC-enabled sensor (at **603**). For example, if the computer processor determines (at **603**) that NFC-enabled sensor transmits detection information using Zigbee, the communications interface may establish communication with the NFC-enabled sensor using Zigbee.

[0026] Accordingly, in view of the foregoing, embodiments of the present disclosure provide quick and efficient installation by allowing a user to quickly connect a security hub to a communications network (e.g., Wi-Fi), onboard one or more sensors with the security hub quickly using NFC, and test whether the sensors are connected to the security hub.

[0027] FIG. **7** illustrates an example computer architecture that may be used to implement embodiments of the present system and method. The example computer architecture may be used for implementing one or more components described in the present disclosure including, but not limited to, the security hub. One embodiment of architecture **700** comprises a system bus **720** for communicating information, and a processor **710** coupled to bus **720** for processing information. Architecture **700** further comprises a random access memory (RAM) or other dynamic storage device **725** (referred to herein as main memory), coupled to bus **720** for storing information and instructions to be executed by processor **710**. Main memory **725** also may be used for storing temporary variables or other intermediate information during execution of instructions by processor **710**. Architecture **700** may also include a read only memory (ROM) and/or other static storage device **726** coupled to bus **720** for storing static information and instructions used by processor **710**.

[0028] A data storage device **721** such as a magnetic disk or optical disc and its corresponding drive may also be coupled to architecture **700** for storing information and instructions. Architecture **700** can also be coupled to a second I/O bus **750** via an I/O interface **730**. A plurality of I/O devices may be coupled to I/O bus **750**, including a display device **743**, an input device (e.g., an alphanumeric input device **742**, a cursor control device **741**, and/or a touchscreen device).

[0029] The communication device **740** allows for access to other computers (e.g., servers or clients) via a network. The communication device **740** may comprise one or more modems, network interface cards, wireless network interfaces or other interface devices, such as those used for coupling to Ethernet, token ring, or other types of networks.

[0030] Some portions of the detailed description herein are presented in terms of algorithms and symbolic representations of operations on data bits within a computer memory. These algorithmic descriptions and representations are the means used by those skilled in the data processing arts to most effectively convey the substance of their work to others skilled in the art. An algorithm is here, and generally, conceived to be a self-consistent sequence of steps leading to a desired result. The steps are those requiring physical manipulations of physical quantities. Usually, though not necessarily, these quantities take the form of electrical or magnetic signals capable of being stored, transferred, combined, compared, and otherwise manipulated. It has proven convenient at times, principally for reasons of common usage, to refer to these signals as bits, values, elements, symbols, characters, terms, numbers, or the like.

[0031] It should be borne in mind, however, that all of these and similar terms are to be associated with the appropriate physical quantities and are merely convenient labels applied to these quantities. Unless specifically stated otherwise, as apparent from the below discussion, it is appreciated that throughout the description, discussions utilizing terms such as "processing" or "computing" or "calculating" or "determining" or "displaying" or the like, refer to the action and processes of a computer system, or similar electronic computing device, that manipulates and transforms data represented as physical (electronic) quantities within the computer system's registers and memories into other data similarly represented as physical quantities within the computer system memories or registers or other such information storage, transmission or display devices.

[0032] The present disclosure also relates to an apparatus for performing the operations herein. This apparatus may be specially constructed for the required purposes, or it may comprise a general purpose computer selectively activated or reconfigured by a computer program stored in the computer. Such a computer program may be stored in a computer readable storage medium, such as, but is not limited to, any type of disk, including floppy disks, optical disks, CD-ROMs, and magnetic-optical disks, read-only memories (ROMs), random access memories (RAMs), EPROMs, EEPROMs, magnetic or optical cards, or any type of media suitable for storing electronic instructions, and each coupled to a computer system bus.

[0033] The algorithms presented herein are not inherently related to any particular computer or other apparatus. Various general purpose systems, messaging servers, or personal computers may be used with programs in accordance with the teachings herein, or it may prove convenient to construct a more specialized apparatus to perform the required method steps. The required structure for a variety of these systems appears in the description above. A variety of programming languages may be used to implement the teachings of the disclosure as described herein.

[0034] Moreover, the various features of the representative examples and the dependent claims may be combined in ways that are not specifically and explicitly enumerated in order to provide additional embodiments of the present teachings. The dimensions and the shapes of the components shown in the figures are designed to help understand how the present teachings are practiced and do limit the dimensions and the shapes shown in the examples.

What is claimed is:

1. A security hub comprising:
- a near field communication (NFC) interface configured to detect an NFC-enabled sensor;
- a communications interface configured to establish communication with the NFC-enabled sensor, a communications network, and an electronic device; and
- a computer processor operatively connected to the NFC interface and the communications interface and configured to:
- onboard the NFC-enabled sensor;
- analyze detection information received from the NFC-enabled sensor, and
- perform an action in response to the analysis of the detection information.

2. The security hub of claim **1**, wherein to onboard the NFC-enabled sensor includes registering the NFC-enabled sensor and determining a communications protocol of the NFC-enabled sensor through which detection information is transmitted.

3. The security hub of claim **2**, wherein information used for onboarding the NFC-enabled sensor is received entirely from the NFC-enabled sensor through the NFC interface.

4. The security hub of claim **3**, wherein the NFC interface utilizes the Thread network protocol.

5. The security hub of claim **1**, further comprising an application running on the electronic device.

6. The security hub of claim **5**, wherein the application displays diagrammatic instructions for connecting the security hub to the communications network.

7. The security hub of claim **5**, wherein the application displays diagrammatic instructions for connecting the NFC-enabled sensor to security hub.

8. The security hub of claim **5**, wherein the application displays diagrammatic instructions for testing the operations of the NFC-enabled sensor.

9. The security hub of claim **8**, wherein the application displays an indication of whether the NFC-enabled sensor is connected and operating properly.

10. The security hub of claim **5**, wherein the application displays the location and installation status of the NFC-enabled sensor.

11. A method of connecting an NFC-enabled sensor to a security hub, the method comprising:
- detecting the NFC-enabled sensor via a near field communication (NFC) interface of the security hub;
- establishing communication with the NFC-enabled sensor, a communications network, and an electronic device via a communications interface of security hub;
- onboarding the NFC-enabled sensor; and

receiving detection information from the NFC-enabled sensor.

12. The method of claim **11**, wherein onboarding the NFC-enabled sensor includes registering the NFC-enabled sensor and determining a communications protocol of the NFC-enabled sensor through which detection information is transmitted.

13. The method of claim **12**, wherein information used for onboarding the NFC-enabled sensor is received entirely from the NFC-enabled sensor through the NFC interface.

14. The method of claim **13**, wherein the NFC interface utilizes the Thread network protocol.

15. The method of claim **11**, further comprising communicating with an application running on the electronic device.

16. The method of claim **15**, further comprising instructing the application to display diagrammatic instructions for connecting the security hub to the communications network.

17. The method of claim **15**, further comprising instructing the application to display diagrammatic instructions for connecting the NFC-enabled sensor to security hub.

18. The method of claim **15**, further comprising instructing the application to display diagrammatic instructions for testing the operations of the NFC-enabled sensor.

19. The method of claim **18**, further comprising instructing the application to display an indication of whether the NFC-enabled sensor is connected and operating properly.

20. The method of claim **15**, further comprising instructing the application to display the location and installation status of the NFC-enabled sensor.

* * * * *