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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
10 November 2022 (10.11.2022)

WIPO | PCT

(10) International Publication Number
WO 2022/236137 A1

(51) International Patent Classification:
H04W 12/06 (2021.01)

(21) International Application Number:
PCT/US2022/028194

(22) International Filing Date:
06 May 2022 (06.05.2022)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
17/314,016 06 May 2021 (06.05.2021) US

(71) Applicant: **NILE GLOBAL, INC.** [US/US]; 3590 North 1st Street, Suite 300, San Jose, CA 95134 (US).

(72) Inventors: **RAMAN, Gopal**; c/o Nile Global, Inc., 3590 North 1st Street, Suite 300, San Jose, CA 95134 (US). **KATUKAM, Suresh**; c/o Nile Global, Inc., 3590 North 1st Street, Suite 300, San Jose, CA 95134 (US). **NEDUNGADI, Promode**; c/o Nile Global, Inc., 3590 North 1st Street, Suite 300, San Jose, CA 95134 (US). **DAMODARAM, Sathish**; c/o Nile Global, Inc., 3590 North 1st Street, Suite 300, San Jose, CA 95134 (US). **TRISNO, Tjandra**; c/o Nile Global, Inc., 3590 North 1st Street, Suite 300, San Jose, CA 95134 (US). **ALEXANDER, Steve**; c/o Nile Global, Inc., 3590 North 1st Street, Suite 300, San Jose, CA 95134 (US). **KUMAR, Avinash**; c/o Nile Global, Inc., 3590 North 1st Street, Suite 300, San Jose, CA 95134 (US).

(74) Agent: **WILSON, Mark, A.**; Loza & Loza, LLP, 305 N. Second Ave, #127, Upland, CA 91786 (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, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

(54) **Title:** METHODS AND SYSTEMS OF WIRELESS SENSOR AUTHENTICATION

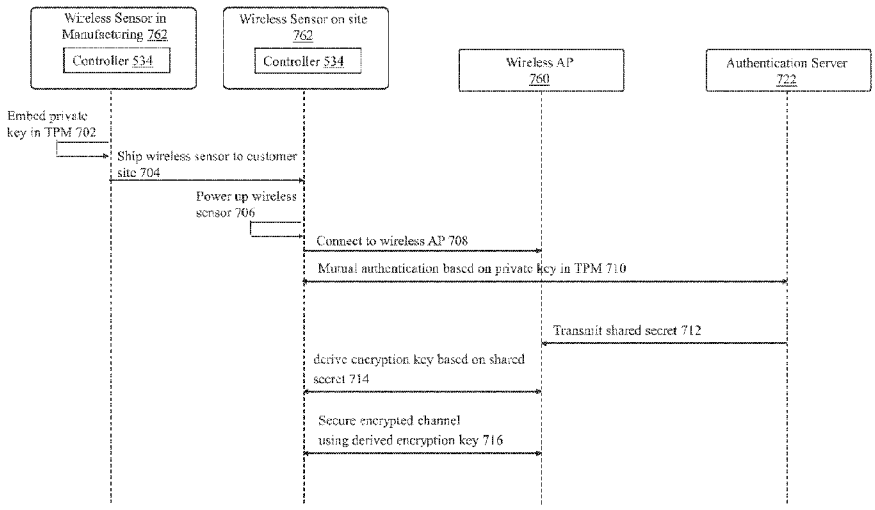

FIG. 7

(57) **Abstract:** Embodiments of a device and method are disclosed. In an embodiment, a method of communications involves from a wireless sensor deployed at a customer site, connecting to a wireless access point (AP) deployed at the customer site and based on a private key stored in the wireless sensor, performing mutual authentication between the wireless sensor and an authentication server connected to the wireless AP.

[Continued on next page]

WO 2022/236137 A1

Declarations under Rule 4.17:

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

Published:

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

METHODS AND SYSTEMS OF WIRELESS SENSOR AUTHENTICATION

BACKGROUND

[0001] A sensor can be used to monitor a network and perform both active and passive testing of the network. For example, a wireless sensor can be used to monitor a wireless network and perform both active and passive testing of the wireless network. Typically, a wireless network (e.g., WiFi) vendor or service provider installs sensors to monitor the health of a wireless network, which may include Access Points (APs), switches, and other network elements that work together to provide a customer with wireless access. For example, a sensor may behave similarly to a client of a WiFi network and check the health and performance of the WiFi network and report collected data for analysis. However, sensors such as wireless sensors may be susceptible to Man-in-the-Middle (MITM) attacks, which allows an attacker to gain knowledge of an encryption key. Once an encryption key is compromised, an attacker can decrypt traffic and/or alter and inject traffic. Therefore, there is a need for sensor and authentication technology that is resilient to MITM attacks.

SUMMARY

[0002] Embodiments of a device and method are disclosed. In an embodiment, a method of communications involves from a wireless sensor deployed at a customer site, connecting to a wireless access point (AP) deployed at the customer site and based on a private key stored in the wireless sensor, performing mutual authentication between the wireless sensor and an authentication server connected to the wireless AP. Other embodiments are described.

[0003] In some embodiments, the method further includes deriving an encryption key for communications between the wireless sensor and the wireless AP in response to the mutual authentication.

[0004] In some embodiments, the method further includes at the wireless sensor deployed at the customer site, conducting wireless communications with the wireless AP using the encryption key.

[0005] In some embodiments, deriving the encryption key for communications between the wireless sensor and the wireless AP in response to the mutual authentication includes deriving the encryption key for communications between the wireless sensor and the wireless AP in response to a shared secret generated as a result of the mutual authentication.

[0006] In some embodiments, the method further includes transmitting the shared secret from the authentication server to the wireless AP.

[0007] In some embodiments, the shared secret includes a Pre-Master Key (PMK).

[0008] In some embodiments, the encryption key includes a Pairwise Transient Key (PTK).

[0009] In some embodiments, the private key is stored in a Trusted Platform Module (TPM) of the wireless sensor.

[0010] In some embodiments, based on the private key stored in the wireless sensor, performing the mutual authentication between the wireless sensor and the authentication server connected to the wireless AP includes based on the private key stored in the wireless sensor, performing the mutual authentication between the wireless sensor and the authentication server connected to the wireless AP using a Transport Layer Security (TLS) protocol where a TLS client is the wireless sensor.

[0011] In some embodiments, based on the private key stored in the wireless sensor, performing the mutual authentication between the wireless sensor and the authentication server connected to the wireless AP includes exchanging a server certificate, a server signature, a client certificate, and a client signature between the wireless sensor and the authentication server.

[0012] In some embodiments, based on the private key stored in the wireless sensor, performing the mutual authentication between the wireless sensor and the authentication server connected to the wireless AP includes from the wireless sensor, transmitting a client message to the authentication server, at the wireless sensor, receiving a server message, a server certificate, and a server signature

from the authentication server in response to the client message, at the wireless sensor, verifying the server signature, and from the wireless sensor, transmitting a client certificate to the authentication server when the server signature is successfully verified.

[0013] In some embodiments, based on the private key stored in the wireless sensor, performing the mutual authentication between the wireless sensor and the authentication server connected to the wireless AP further includes transmitting a signature request to a TPM of the wireless sensor in which the private key is stored and receiving a client signature from the TPM of the wireless sensor, wherein the client signature is generated based on the private key.

[0014] In some embodiments, based on the private key stored in the wireless sensor, performing the mutual authentication between the wireless sensor and the authentication server connected to the wireless AP further includes from the wireless sensor, transmitting the client signature to the authentication server and at the authentication server, verifying the client signature.

[0015] In some embodiments, a wireless sensor deployed at a customer site includes a wireless transceiver configured to connect to a wireless AP deployed at the customer site and a controller configured to store a private key and to, based on the private key, perform mutual authentication with an authentication server connected to the wireless AP.

[0016] In some embodiments, the controller is further configured to derive an encryption key for communications between the wireless sensor and the wireless AP in response to the mutual authentication.

[0017] In some embodiments, the controller is further configured to conduct wireless communications with the wireless AP using the encryption key.

[0018] In some embodiments, the controller includes a TPM configured to store the private key.

[0019] In some embodiments, the controller includes a TLS unit configured to, based on the private key stored in the wireless sensor, perform the mutual authentication with the authentication server connected to the wireless AP using a TLS protocol where a TLS client is the wireless sensor.

[0020] In some embodiments, the controller includes a cryptographic engine configured to receive a message digest and generate a client signature of the message digest based on the private key.

[0021] In some embodiments, a method of communications involves from a wireless sensor deployed at a customer site, connecting to a wireless AP deployed at the customer site, based on a private key stored in a TPM of the wireless sensor, performing mutual authentication between the wireless sensor and an authentication server connected to the wireless AP, deriving a PTK for communications between the wireless sensor and the wireless AP in response to a PMK generated as a result of the mutual authentication, and at the wireless sensor deployed at the customer site, conducting wireless communications with the wireless AP using the PTK.

[0022] Other aspects in accordance with the invention will become apparent from the following detailed description, taken in conjunction with the accompanying drawings, illustrated by way of example of the principles of the invention.

BRIEF DESCRIPTION OF THE DRAWINGS

[0023] Fig. 1 depicts a communications system in accordance to an embodiment of the invention.

[0024] Fig. 2 depicts an embodiment of a network device of the communications system depicted in Fig. 1.

[0025] Fig. 3 depicts an embodiment of a network that can be deployed at a customer site.

[0026] Fig. 4 depicts an embodiment of a wireless sensor that can be installed in the customer site to monitor the health and performance of a wireless network at the customer site.

[0027] Fig. 5 depicts a controller, which is an embodiment of a controller of the wireless sensor depicted in Fig. 4.

[0028] Fig. 6 illustrates an authentication configuration in which that a controller of a wireless sensor interacts with authentication servers through wireless APs and a wired switch.

[0029] Fig. 7 shows a swim-lane diagram illustrating an example authentication procedure between a wireless sensor, a wireless AP, and an authentication server.

[0030] Fig. 8 shows a swim-lane diagram illustrating an example mutual authentication procedure between a wireless sensor and an authentication server.

[0031] Fig. 9 is a process flow diagram of a method of communications in accordance to an embodiment of the invention.

[0032] Fig. 10 is a process flow diagram of a method of communications in accordance to an embodiment of the invention.

[0033] Throughout the description, similar reference numbers may be used to identify similar elements.

DETAILED DESCRIPTION

[0034] It will be readily understood that the components of the embodiments as generally described herein and illustrated in the appended figures could be arranged and designed in a wide variety of different configurations. Thus, the following more detailed description of various embodiments, as represented in the figures, is not intended to limit the scope of the present disclosure, but is merely representative of various embodiments. While the various aspects of the embodiments are presented in drawings, the drawings are not necessarily drawn to scale unless specifically indicated.

[0035] The present invention may be embodied in other specific forms without departing from its spirit or essential characteristics. The described embodiments are to be considered in all respects only as illustrative and not restrictive. The scope of the invention is, therefore, indicated by the appended claims rather than by this detailed description. All changes which come within the meaning and range of equivalency of the claims are to be embraced within their scope.

[0036] Reference throughout this specification to features, advantages, or similar language does not imply that all of the features and advantages that may be realized with the present invention should be or are in any single embodiment of the invention. Rather, language referring to the features and advantages is

understood to mean that a specific feature, advantage, or characteristic described in connection with an embodiment is included in at least one embodiment of the present invention. Thus, discussions of the features and advantages, and similar language, throughout this specification may, but do not necessarily, refer to the same embodiment.

[0037] Furthermore, the described features, advantages, and characteristics of the invention may be combined in any suitable manner in one or more embodiments. One skilled in the relevant art will recognize, in light of the description herein, that the invention can be practiced without one or more of the specific features or advantages of a particular embodiment. In other instances, additional features and advantages may be recognized in certain embodiments that may not be present in all embodiments of the invention.

[0038] Reference throughout this specification to "one embodiment", "an embodiment", or similar language means that a particular feature, structure, or characteristic described in connection with the indicated embodiment is included in at least one embodiment of the present invention. Thus, the phrases "in one embodiment", "in an embodiment", and similar language throughout this specification may, but do not necessarily, all refer to the same embodiment.

[0039] Fig. 1 depicts a communications system 100 in accordance to an embodiment of the invention. In the embodiment depicted in Fig. 1, the communications system includes a cloud server 102 and a deployed network 150 within a customer site 114. The cloud server and/or the network may be implemented in hardware (e.g., circuits), software, firmware, or a combination thereof. Although the illustrated communications system 100 is shown with certain components and described with certain functionality herein, other embodiments of the communications system may include fewer or more components to implement the same, less, or more functionality. For example, in some embodiments, the communications system includes more than one cloud server, more than one deployed network, and/or more than one customer site. In another example, although the cloud server and the deployed network are shown in Fig. 1 as being connected in certain topology, the network topology of the communications system 100 is not limited to the topology shown in Fig. 1.

[0040] The cloud server 102 can be used to provide at least one service to a customer site (e.g., to the deployed network 150 located at the customer site 114). The cloud server may be configured to facilitate or perform a security service (e.g., an authentication service) to network devices (e.g., the deployed network 150) at the customer site. Because the cloud server can facilitate or perform a security service to network devices at the customer site, network security can be improved. In addition, because the cloud server can facilitate or perform a security service to network devices at the customer site, a user or customer of the customer site can be notified of security issues. In some embodiments, the cloud server is configured to generate a user interface to obtain user input information regarding network security in a floor plan of a customer site. In some embodiments, the user interface includes a graphical user interface. The cloud server may be implemented in hardware (e.g., circuits), software, firmware, or a combination thereof. In some embodiments, the cloud server is implemented on a server grade hardware platform, such as an x86 architecture platform. For example, the hardware platform of the cloud server may include conventional components of a computing device, such as one or more processors (e.g., CPUs), system memory, a network interface, storage system, and other Input/Output (I/O) devices such as, for example, a mouse and a keyboard (not shown). In some embodiments, the processor is configured to execute instructions such as, for example, executable instructions that may be used to perform one or more operations described herein and may be stored in the memory and the storage system. In some embodiments, the memory is volatile memory used for retrieving programs and processing data. The memory may include, for example, one or more random access memory (RAM) modules. In some embodiments, the network interface is configured to enable the cloud server to communicate with another device via a communication medium. The network interface may be one or more network adapters, also referred to as a Network Interface Card (NIC). In some embodiments, the cloud server includes local storage devices (e.g., one or more hard disks, flash memory modules, solid state disks and optical disks) and/or a storage interface that enables the host to communicate with one or more network data storage systems, which are used to store information, such as executable instructions, cryptographic keys, virtual disks, configurations, and other data.

[0041] In the embodiment depicted in Fig. 1, the cloud server 102 includes an authentication module 110, a customer information portal 108 connected to the authentication module 110, and an authentication database 112 configured to store authentication data. The authentication module, the customer information portal, and/or the authentication database may be implemented in hardware (e.g., circuits), software, firmware, or a combination thereof. Although the illustrated cloud server is shown with certain components and described with certain functionality herein, other embodiments of the cloud server may include fewer or more components to implement the same, less, or more functionality. For example, in some embodiments, the cloud server includes more than one authentication module, more than one customer information portal, and/or more than one authentication database. In another example, although the authentication module, the customer information portal, and the authentication database are shown in Fig. 1 as being connected in certain topology, the network topology of the cloud server is not limited to the topology shown in Fig. 1. In addition, although the customer information portal 108 is shown in Fig. 1 as being a component of the cloud server 102, in other embodiments, the customer information portal may be implemented outside of the server. In some embodiments, the authentication module 110 is configured to facilitate or perform an authentication service to network devices (e.g., the deployed network 150) at the customer site 114, for example, using an authentication rule set 130. The authentication rule set 130 may include one or more authentication rules for network devices at the customer site 114, for example, for performing an authentication service to network devices at the customer site 114. In some embodiments, the authentication database 112 is configured to store authentication data for a network deployed and/or to be deployed at the customer site (e.g., a list of network devices deployed or to be deployed at the customer site). Because the authentication module can facilitate or perform an authentication service to network devices at the customer site, network security can be improved. In addition, because the authentication module can facilitate or perform an authentication service to network devices at the customer site, a user or customer (e.g., a layperson such as a worker on-site or an end-user such as an employee) at the customer site can be notified of authentication issues. The customer

information portal 108 is configured to receive customer input 128. In some embodiments, the customer information portal is configured to include or generate a user interface that allows a customer to input information associated with an authentication service for the customer site 114, such as one or more specific requirements or restrictions.

[0042] In the communications system 100 depicted in Fig. 1, the customer site 114 may include one or more buildings, and each building may include one or more floors. Network devices that can be deployed at the customer site may include any type of suitable network devices. For example, network devices may be designated to be deployed to a specific building, a specific floor within a building, and/or a specific location on a floor of a building. A network device that can be deployed at the customer site may be fully or partially implemented as an Integrated Circuit (IC) device. In the embodiment depicted in Fig. 1, the network 150 includes one or more network devices 104-1, ..., 104-N, where N is a positive integer. In some embodiments, at least one of the one or more network devices 104-1, ..., 104-N is a wired and/or wireless communications device that includes at least one processor (e.g., a microcontroller, a digital signal processor (DSP), and/or a central processing unit (CPU)), at least one wired or wireless communications transceiver implemented in one or more logical circuits and/or one or more analog circuits, at least one wired or wireless communications interface and that supports at least one wired or wireless communications protocol, and/or at least one antenna. For example, at least one of the one or more network devices 104-1, ..., 104-N may be compatible with Institute of Electrical and Electronics Engineers (IEEE) 802.3 protocol and/or one or more wireless local area network (WLAN) communications protocols, such as IEEE 802.11 protocol. In some embodiments, at least one of the one or more network devices 104-1, ..., 104-N is a wired communications device that is compatible with at least one wired local area network (LAN) communications protocol, such as a wired router (e.g., an Ethernet router), a wired switch, a wired hub, or a wired bridge device (e.g., an Ethernet bridge). In some embodiments, at least one of the one or more network devices 104-1, ..., 104-N is a wireless access point (AP) that connects to a local area network (e.g., a LAN) and/or to a backbone network (e.g., the Internet) through a wired connection and that wirelessly connects to wireless

stations (STAs), for example, through one or more WLAN communications protocols, such as an IEEE 802.11 protocol. In some embodiments, the network 150 includes at least one authentication server, at least one distribution switch (DS) or distribution layer switch that functions as a bridge between a core layer switch and an access layer switch, at least one head end (HE) or gateway, at least one access switch (AS) that can directly interact with a lower-level device (e.g., a wireless AP), at least one wireless AP, and/or at least one wireless sensor that wirelessly connects to a wireless AP. In some embodiments, at least one of the one or more network devices 104-1, …, 104-N is a wireless station (STA) that wirelessly connects to a wireless AP. For example, at least one of the one or more network devices 104-1, …, 104-N may be a wireless sensor, a laptop, a desktop personal computer (PC), a mobile phone, or other wireless device that supports at least one WLAN communications protocol (e.g., an IEEE 802.11 protocol)).

[0043] Fig. 2 depicts an embodiment of a network device 204 of the communications system depicted in Fig. 1. The network device 204 may be an embodiment of a network device that is included in the deployed network 150 depicted in Fig. 1. However, network devices that can be included in the deployed network 150 depicted in Fig. 1 are not limited to the embodiment depicted in Fig. 2. The network device 204 may be any suitable type of network device. For example, the network device 204 may be an authentication server, a distribution switch, a gateway, an access switch, a wireless access point, or a sensor, described in details with reference to Fig. 2. In the embodiment depicted in Fig. 2, a network device 204 includes a wireless and/or wired transceiver 232, a controller 234 operably connected to the transceiver 232, at least one optional antenna 236 operably connected to the transceiver 232, and at least one optional network port 238 operably connected to the transceiver 232. In some embodiments, the transceiver 232 includes a physical layer (PHY) device. The transceiver 232 may be any suitable type of transceiver. For example, the transceiver 232 may be a short-range communications transceiver (e.g., a Bluetooth) or a WLAN transceiver (e.g., a transceiver compatible with an IEEE 802.11 protocol). In some embodiments, the network device 204 includes multiple transceivers, for example, a short-range communications transceiver (e.g., a Bluetooth) and a WLAN transceiver (e.g., a transceiver compatible with an

IEEE 802.11 protocol). In some embodiments, the controller 234 is configured to control the transceiver 232 to process packets received through the antenna 236 and/or the network port 238 and/or to generate outgoing packets to be transmitted through the antenna 236 and/or the network port 238. In some embodiments, the controller 234 is configured to perform an authentication function for the network device 204. The antenna 236 may be any suitable type of antenna. For example, the antenna 236 may be an induction type antenna such as a loop antenna or any other suitable type of induction type antenna. However, the antenna 236 is not limited to an induction type antenna. The network port 238 may be any suitable type of port. For example, the network port 238 may be a local area network (LAN) network port such as an Ethernet port. However, the network port 238 is not limited to LAN network ports. In some embodiments, the network device 204 is a DS, a HE or gateway, an AS, a wireless AP, or a wireless sensor that wirelessly connects to a wireless AP.

[0044] Fig. 3 depicts an embodiment of a network 350 that can be deployed at the customer site 114. The network 350 depicted in Fig. 3 is one possible embodiment of the deployed network 150 at the customer site 114 depicted in Fig. 1. However, the deployed network 150 at the customer site 114 depicted in Fig. 1 are not limited to the embodiment shown in Fig. 3. In some embodiments, the network 350 is a replicable block that can be scaled (e.g., expanded) to meet any deployment. In the embodiment depicted in Fig. 3, the network 350 includes a pair of local authentication servers 322-1, 322-2, a number of access switches (ASs) 356-1, 356-2, 356-3, 356-4, 356-5, 356-6 that can directly interact with lower-level devices (e.g., wireless APs), a number of wireless APs 360-1, 360-2, 360-3, 360-4, 360-5, 360-6 connected to the ASs, and a number of wireless sensors 362-1, 362-2, 362-3 that wirelessly connect to the wireless APs. In some embodiments, at least one of the authentication servers 322-1, 322-2, the ASs 356-1, 356-2, 356-3, 356-4, 356-5, 356-6, the wireless APs 360-1, 360-2, 360-3, 360-4, 360-5, 360-6, and the wireless sensors 362-1, 362-2, 362-3 depicted in Fig. 3 is implemented as the network device 204 depicted in Fig. 2. In some embodiments, at least one of the authentication servers 322-1, 322-2 is implemented the same as or similar to the cloud server 102 depicted in Fig. 1. For example, at least one of the authentication servers 322-1, 322-2 includes an authentication module and an

authentication database configured to store authentication data, which may be implemented in hardware (e.g., circuits), software, firmware, or a combination thereof. In some embodiments, the authentication module is configured to facilitate or perform an authentication service to the wireless sensors 362-1, 362-2, 362-3, for example, using an authentication rule set, which may include one or more authentication rules.

[0045] In some embodiments, at least one wireless sensor (e.g., the wireless sensor 362-1, 362-2, or 362-3) is installed in the customer site 114 to monitor the network 150 and perform both active and passive testing of the network 150. For example, at least one wireless sensor behaves similarly to a client of a wireless network, checks the health and performance of the wireless network, and reports collected data for analysis. The at least one wireless sensor can be plugged directly into at least one wall power outlet and can be installed at ground level thus mimicking at least one real client device. In some embodiments, multiple wireless sensors are installed across the deployed network 150 (e.g., the network 350 depicted in Fig. 3) using a mobile app and connect seamlessly to at least one wireless AP to communicate with the cloud server 102 (e.g., the authentication module 110 in the cloud server 102) and/or a local authentication server at the customer site (e.g., the authentication server 322-1 or 322-2).

[0046] Fig. 4 depicts an embodiment of a wireless sensor 462 that can be installed in the customer site 114 to monitor the health and performance of a wireless network at the customer site 114. The wireless sensor 462 depicted in Fig. 4 is one possible embodiment of wireless sensors (e.g., the wireless sensor 362-1, 362-2, or 362-3) that can be installed at the customer site 114 depicted in Fig. 1. However, wireless sensors that can be installed at the customer site 114 depicted in Fig. 1 are not limited to the embodiment shown in Fig. 4. In the embodiment depicted in Fig. 4, the wireless sensor 462 includes a wireless transceiver 432, a controller 434 operably connected to the wireless transceiver 432, and at least one antenna 436 operably connected to the wireless transceiver 432. The wireless transceiver 432 may be any suitable type of transceiver. For example, the wireless transceiver 432 may be a short-range communications transceiver (e.g., a Bluetooth) or a WLAN transceiver (e.g., a transceiver compatible with an IEEE 802.11 protocol). In some embodiments, the wireless

sensor 462 includes multiple wireless transceivers, for example, a short-range communications transceiver (e.g., a Bluetooth) and a WLAN transceiver (e.g., a transceiver compatible with an IEEE 802.11 protocol). In some embodiments, the controller 434 is configured to control the wireless transceiver 432 to process packets received through the antenna 436 and/or to generate outgoing packets to be transmitted through the antenna 436. In some embodiments, the controller 434 is configured to perform an authentication function. The antenna 436 may be any suitable type of antenna. For example, the antenna 436 may be an induction type antenna such as a loop antenna or any other suitable type of induction type antenna. However, the antenna 436 is not limited to an induction type antenna.

[0047] In some embodiments, to protect the integrity of data collected by the wireless sensor 462 as well as prevent the wireless sensor 462 from being compromised by rogue actors, the wireless sensor 462 authenticates to an authentication server using a high grade of network security, which rules out un-encrypted connections and reliance on pre-configured shared secrets since these are known to be vulnerable. In some embodiments, the wireless sensor 462 is configured to implement an enterprise grade security mechanism built on an 802.1X framework that allows the use of certificate based mutual authentication between the wireless sensor 462 and an authentication server. In some embodiments, the wireless transceiver 432 is configured to connect to a wireless access point (AP) deployed at a customer site and the controller 434 is configured to store a private key and to, based on the private key, perform mutual authentication with an authentication server connected to the wireless AP. In some embodiments, the controller 434 is further configured to derive an encryption key for communications between the wireless sensor and the wireless AP in response to the mutual authentication. In some embodiments, the controller 434 is further configured to conduct wireless communications with the wireless AP using the encryption key. In some embodiments, the controller 434 includes a Trusted Platform Module (TPM) configured to store the private key. In some embodiments, the controller 434 includes a Transport Layer Security (TLS) unit configured to, based on the private key stored in the wireless sensor, perform the mutual authentication with the authentication server connected to the wireless AP using a Transport Layer Security (TLS) protocol where a TLS client is the

wireless sensor. In some embodiments, the controller 434 includes a cryptographic engine 580 configured to receive a message digest from the TLS unit 572 and to generate a client signature of the message digest based on the private key 578 stored in the TPM 570.

[0048] Fig. 5 depicts a controller 534, which is an embodiment of the controller 434 of the wireless sensor 462 depicted in Fig. 4. The controller 534 depicted in Fig. 5 is one possible embodiment of the controller 434 of the wireless sensor 462 depicted in Fig. 4. However, the controller 434 of the wireless sensor 462 depicted in Fig. 4 is not limited to the embodiment shown in Fig. 5. In the embodiment depicted in Fig. 5, the controller 534 includes a Trusted Platform Module (TPM) 570, a Transport Layer Security (TLS) unit 572 operably connected to the TPM 570, and an Extensible Authentication Protocol (EAP) unit 574 operably connected to the TLS unit 572 and configured to perform an EAP function.

[0049] In some embodiments, the controller 534 is configured to store a private key and to, based on the private key, perform mutual authentication with an authentication server connected to a wireless AP. In some embodiments, the controller 534 is further configured to derive an encryption key for communications between the wireless sensor and a wireless AP in response to the mutual authentication. In some embodiments, the controller 534 is further configured to conduct wireless communications with the wireless AP using the encryption key. In some embodiments, the controller 434 includes a cryptographic engine configured to receive a message digest and generate a client signature of the message digest based on the private key. The TLS unit 572 is configured to interact with the TPM 570 to perform operations that require the private key 578. In some embodiments, the TLS unit 572 is configured to, based on the private key stored in the wireless sensor, perform a mutual authentication with an authentication server connected to a wireless AP using a TLS protocol where a TLS client is the wireless sensor. The TPM 570 includes a secure storage unit 576 that is configured to store a private key 578 and a cryptographic engine 580 that is configured to perform cryptographic operations. For example, the TLS unit 572 transmits a digest 582 to the cryptographic engine 580 and receives a signature 584 from the cryptographic engine 580. In some embodiments, the

cryptographic engine is configured to receive a message digest and to generate a client signature of the message digest based on the private key stored in the TPM 570.

[0050] The controller 534 uses an EAP scheme (e.g., implemented in the EAP unit 574) that is based on a TLS suite (e.g., implemented in the TLS unit 572), which may require the use of both client and server certificates. By using the controller 534, a wireless sensor (e.g., the wireless sensor 462) is resilient to a Man-in-the-Middle (MITM) attack, which allows an attacker to gain knowledge of an encryption key derived between the wireless sensor 462 and the network 150. Once an encryption key is compromised, an attacker can decrypt traffic and/or alter and inject traffic. However, for an MITM attack to succeed, an attacker needs the private key 578 that is stored in the TPM 570. Because the private key 578 is stored in the secure storage unit 576 of the TPM 570, MITM attacks become infeasible. In some embodiments, the TPM 570 is a tamper proof hardware (e.g., a tamper proof IC chip) that performs operations using the private key 578 without revealing the private key 578 to outside entities. In some embodiments, the TPM is replaced by a hardware security module (HSM). By using the controller 534, a wireless sensor (e.g., the wireless sensor 462) is also resilient to impersonation. In some embodiments, the certificate stored in a wireless sensor (e.g., the wireless sensor 462) is unique to the wireless sensor and is, for example, tied to the serial number and other unique identity of the wireless sensor, such as the Ethernet MAC address of the wireless sensor. Impersonating the wireless sensor requires an attacker to gain access the private key 578. By storing the private key 578 in the TPM 570, impersonation attacks become more difficult or even infeasible.

[0051] Fig. 6 illustrates an authentication configuration 600 in which that the controller 534 of a wireless sensor (e.g., the wireless sensor 462) interacts with authentication servers 622-1, 622-2, 622-3 through wireless APs 660-1, 660-2 and a wired switch 656. In the embodiment depicted in Fig. 6, the controller 534 communicates with the wireless APs 660-1, 660-2 through wireless links, while the wireless APs 660-1, 660-2 are connected to the wired switch, which are connected to the authentication servers 622-1, 622-2, 622-3. The authentication servers 622-1, 622-2, 622-3 can either reside on premise (e.g., implemented in the

customer site 114 depicted in Fig. 1) or in the cloud (e.g., implemented as or in the cloud server 102 depicted in Fig. 1). In some embodiments, the TLS unit 572 is configured to, based on the private key 578 stored in the secure storage unit 576, perform mutual authentication with the authentication server 622-1, 622-2, or 622-3 using a TLS protocol where a TLS client is the wireless sensor. In some embodiments, the authentication servers 622-1, 622-2, 622-3 are local authentication servers that reside on premise (e.g., implemented as or in the customer site 114 depicted in Fig. 1). In some embodiments, the authentication servers 622-1, 622-2, 622-3 are remote authentication servers that reside in the cloud (e.g., implemented as or in the cloud server 102 depicted in Fig. 1). In some embodiments, the authentication servers 622-1, 622-2, 622-3 includes at least one local authentication server that resides on premise (e.g., implemented as or in the customer site 114 depicted in Fig. 1) and at least one remote authentication server that resides in the cloud (e.g., implemented as or in the cloud server 102 depicted in Fig. 1). The controller authenticates with the authentication servers 622-1, 622-2, 622-3 through the wireless APs 660-1, 660-2 and the wired switch 656. The wireless APs 660-1, 660-2 may be embodiments of the wireless APs 360-1, 360-2, 360-3, 360-4, 360-5, 360-6 depicted in Fig. 3. The authentication servers 622-1, 622-2, 622-3 may be embodiments of the authentication servers 322-1, 322-2 depicted in Fig. 3. The wired switch 656 may be an embodiment of the ASs 356-1, 356-2, 356-3, 356-4, 356-5, 356-6 depicted in Fig. 3. Although the controller 534, the authentication servers 622-1, 622-2, 622-3, the wireless APs 660-1, 660-2, and the wired switch 656 are shown in Fig. 1 as being connected in certain topology, the network topology in which the controller 534, the authentication servers 622-1, 622-2, 622-3, the wireless APs 660-1, 660-2, and the wired switch 656 are connected is not limited to the topology shown in Fig. 1. For example, in some embodiments, at least one of the authentication servers 622-1, 622-2, 622-3 connects to at least one of the wireless APs 660-1, 660-2 directly or wirelessly connects to the wireless sensor (e.g., the wireless sensor 462) that includes the controller 534.

[0052] Fig. 7 shows a swim-lane diagram illustrating an example authentication procedure between a wireless sensor 762, a wireless AP 760, and an authentication server 722. In the authentication procedure depicted in Fig. 7,

the wireless sensor 762 is shipped from a manufacturer (e.g., a factory) to a customer site (e.g., the customer site 114) needs no further configuration for the wireless sensor to become functional. Because certificate-based authentication is used, there is no need to configure a password or other pre-shared secret on the wireless sensor 762. In addition, because the certificate has the unique identity of the wireless sensor 762, there is no need to provision a unique name into the wireless sensor 762. The wireless sensor 762, which may be an embodiment of the wireless sensor 462 depicted in Fig. 4, includes the controller 534 depicted in Fig. 5. The wireless AP 760 may be an embodiment of the wireless AP 660-1, 660-2 depicted in Fig. 6. The authentication server 722 can either reside on premise (e.g., implemented in the customer site 114 depicted in Fig. 1) or in the cloud (e.g., implemented as or in the cloud server 102 depicted in Fig. 1). The authentication server 722 may be an embodiment of the cloud server depicted in Fig. 1, the authentication servers 322-1, 322-2 depicted in Fig. 3, and/or the authentication servers 622-1, 622-2, 622-3 depicted in Fig. 6. Although operations in the example procedure in Fig. 7 are described in a particular order, in some embodiments, the order of the operations in the example procedure may be altered so that certain operations may be performed in an inverse order or so that certain operations may be performed, at least in part, concurrently with other operations.

[0053] In operation 702, in a secure manner during sensor manufacturing, a private key is embedded into the wireless sensor 762 (e.g., into the TPM 570 of the controller 534). In operation 704, the wireless sensor 762 is shipped to a customer site (e.g., the customer site 114). In operation 706, the wireless sensor 762 is powered up. When the wireless sensor 762 is powered up, the wireless sensor 762 runs the software programmed into the wireless sensor 762 during manufacturing. The software looks for a well-known WLAN network name, such as an IEEE 802.11 service set identifier (SSID) that is advertised by wireless APs and establishes a wireless link to the wireless AP 760 in operation 708. At this point, the wireless sensor 762, the authentication server (AS) 722, and the wireless AP 760 exchange messages, for example, in accordance with the 802.1X protocol, in order for the wireless sensor 762 and the authentication server 722 to mutually authenticate themselves. In operation 710, the wireless sensor 762 and the

authentication server (AS) 722 perform mutual authentication based on the private key embedded into the wireless sensor 762 (e.g., the private key 578 stored in the TPM 570 of the controller 534).

[0054] In operation 712, a shared secret is transmitted from the authentication server 722 to the wireless AP 760. In some embodiments, once mutual authentication procedure between the wireless sensor 762 and the authentication server 722 succeeds, the wireless sensor 762 and the authentication server 722 generate a shared secret as a by-product of successful mutual authentication, which is referred to as the Pre-Master Key (PMK).

[0055] In operation 714, an encryption key is derived based on the shared secret. The wireless AP 760 may receive the PMK from the authentication server 722, which is considered secure because the wireless AP 760 and the authentication server 722 are on the same wired network. At this point, the wireless AP 760 and the wireless sensor 762 have the same PMK and engage in an exchange referred to as the 4-way handshake to derive a Pairwise Transient Key (PTK) from the PMK.

[0056] In operation 716, the wireless sensor 762 and the wireless AP 760 communicate to each other based on the derived encryption key. In some embodiments, all packets sent between the wireless AP 760 and the wireless sensor 762 are encrypted using the PTK.

[0057] Fig. 8 shows a swim-lane diagram illustrating an example mutual authentication procedure between the wireless sensor 762 and the authentication server 722. The authentication procedure shown in Fig. 8 correspond to the operation 710 depicted in Fig. 7. In the authentication procedure depicted in Fig. 8, the mutual authentication uses the TLS protocol where the TLS client is the wireless sensor 762. Although operations in the example procedure in Fig. 8 are described in a particular order, in some embodiments, the order of the operations in the example procedure may be altered so that certain operations may be performed in an inverse order or so that certain operations may be performed, at least in part, concurrently with other operations.

[0058] In operation 802, the client (i.e., the wireless sensor 762 (e.g., the TLS unit 572)) transmits or sends a "Client Hello" message with parameters that indicate its preferences such as supported ciphersuites to the authentication server

722. In operation 804, the authentication server 722 transmits or responds with its parameters, a server certificate, and a server signature. In operation 806, the client (i.e., the wireless sensor 762 (e.g., the TLS unit 572 or the cryptographic engine 580)) verifies the server signature using the server certificate. If the verification succeeds, the client (i.e., the wireless sensor 762) transmits or sends its client certificate along with the client signature. Specifically, in operation 808, the client (i.e., the wireless sensor 762 (e.g., the TLS unit 572)) transmits or sends "Client Hello" parameters and the client certificate to the authentication server 722. The client signature is typically obtained by computing a digest of all the messages that the client has sent and generating a signature of the digest using the private key of the client. This signature operation is performed by a wireless sensor TPM 770, which may be an embodiment of the TPM 570 of the controller 534 depicted in Fig. 5, because only the wireless sensor TPM 770 has the private key (e.g., the private key 578 being stored in a secure storage unit 576 of the TPM 570). In operation 810, the client (i.e., the wireless sensor 762 (e.g., the TLS unit 572)) transmits a signature request to the wireless sensor TPM 770 (e.g., the cryptographic engine 580). In operation 812, the wireless sensor TPM 770 (e.g., the cryptographic engine 580) transmits or responds with the client signature to the client (i.e., the wireless sensor 762 (e.g., the TLS unit 572)). In operation 814, the client (i.e., the wireless sensor 762 (e.g., the TLS unit 572)) transmits the client signature to the authentication server 722. The authentication server 722 verifies the client signature sent by the client (i.e., the wireless sensor 762 (e.g., the TLS unit 572)) in operation 816. If the client signature is verified correctly, the mutual authentication is successful.

[0059] In some embodiments, once mutual authentication procedure between the wireless sensor 762 and the authentication server 722 succeeds, the wireless sensor 762 and the authentication server 722 generate a shared secret as a by-product of successful mutual authentication, which is referred to as the PMK. The wireless AP 760 needs to obtain the PMK such that the wireless AP 760 and the wireless sensor 762 can engage in another round of communication to derive an encryption key called the PTK. If the PTK is generated successfully, the wireless sensor 762 has the assurance that it is talking to an authorized AP. In some embodiments, all packets sent between the wireless AP 760 and the wireless

sensor 762 are encrypted using the PTK. The wireless AP 760 may receive the PMK from the authentication server 722, which is considered secure because the wireless AP 760 and the authentication server 722 are on the same wired network. At this point, the wireless AP 760 and the wireless sensor 762 have the same PMK and engage in an exchange referred to as the 4-way handshake. The purpose of this handshake is to derive the PTK from the PMK. Subsequently, the PTK can be used to encrypt all the traffic between the wireless AP 760 and the wireless sensor 762. The operations described above correspond to the operations 712, 714, 716 depicted in Fig. 7.

[0060] Fig. 9 is a process flow diagram of a method of communications in accordance to an embodiment of the invention. According to the method, at block 902, from a wireless sensor deployed at a customer site, a wireless access point (AP) deployed at the customer site is connected to. At block 904, based on a private key stored in the wireless sensor, mutual authentication between the wireless sensor and an authentication server connected to the wireless AP is performed. In some embodiments, an encryption key for communications between the wireless sensor and the wireless AP is derived in response to the mutual authentication. In some embodiments, at the wireless sensor deployed at the customer site, wireless communications are conducted with the wireless AP using the encryption key. In some embodiments, the encryption key for communications between the wireless sensor and the wireless AP is derived in response to a shared secret generated as a result of the mutual authentication. In some embodiments, the shared secret is transmitted from the authentication server to the wireless AP. In some embodiments, the shared secret includes a Pre-Master Key (PMK). In some embodiments, the encryption key includes a Pairwise Transient Key (PTK). In some embodiments, the private key is stored in a Trusted Platform Module (TPM) of the wireless sensor. In some embodiments, based on the private key stored in the wireless sensor, the mutual authentication between the wireless sensor and the authentication server connected to the wireless AP is performed using a Transport Layer Security (TLS) protocol where a TLS client is the wireless sensor. In some embodiments, a server certificate, a server signature, a client certificate, and a client signature are exchanged between the wireless sensor and the authentication server. In some embodiments, from the

wireless sensor, a client message is transmitted to the authentication server, at the wireless sensor, a server message, a server certificate, and a server signature are received from the authentication server in response to the client message, at the wireless sensor, the server signature is verified, and from the wireless sensor, a client certificate is transmitted to the authentication server when the server signature is successfully verified. In some embodiments, a signature request is transmitted to a Trusted Platform Module (TPM) of the wireless sensor in which the private key is stored, and a client signature is received from the TPM of the wireless sensor, wherein the client signature is generated based on the private key. In some embodiments, from the wireless sensor, the client signature is transmitted to the authentication server, and at the authentication server, the client signature is verified. The wireless sensor may be similar to, the same as, or a component of the wireless sensors 362-1, 362-2, 362-3 depicted in Fig. 3, the wireless sensor 462 depicted in Fig. 4, and/or the wireless sensor 762 depicted in Figs. 7 and 8. The customer site may be similar to, the same as, or a component of the customer site 114 depicted in Fig. 1. The wireless AP may be similar to, the same as, or a component of the wireless APs 360-1, 360-2, 360-3, 360-4, 360-5, 360-6 depicted in Fig. 3, the wireless APs 660-1, 660-2 depicted in Fig. 6, and/or the wireless AP 760 depicted in Figs. 7 and 8. The authentication server may be similar to, the same as, or a component of the authentication servers 322-1, 322-2 depicted in Fig. 3, the authentication servers 622-1, 622-2, 622-3 depicted in Fig. 6, and/or the authentication server 722 depicted in Figs. 7 and 8.

[0061] Fig. 10 is a process flow diagram of a method of communications in accordance to an embodiment of the invention. According to the method, at block 1002, from a wireless sensor deployed at a customer site, a wireless access point (AP) deployed at the customer site is connected to. At block 1004, based on a private key stored in a Trusted Platform Module (TPM) of the wireless sensor, mutual authentication between the wireless sensor and an authentication server connected to the wireless AP is performed. At block 1006, a Pairwise Transient Key (PTK) for communications between the wireless sensor and the wireless AP is derived in response to a Pre-Master Key (PMK) generated as a result of the mutual authentication. At block 1008, at the wireless sensor deployed at the customer site, wireless communications are conducted with the wireless AP using

the PTK. The wireless sensor may be similar to, the same as, or a component of the wireless sensors 362-1, 362-2, 362-3 depicted in Fig. 3, the wireless sensor 462 depicted in Fig. 4, and/or the wireless sensor 762 depicted in Figs. 7 and 8. The customer site may be similar to, the same as, or a component of the customer site 114 depicted in Fig. 1. The wireless AP may be similar to, the same as, or a component of the wireless APs 360-1, 360-2, 360-3, 360-4, 360-5, 360-6 depicted in Fig. 3, the wireless APs 660-1, 660-2 depicted in Fig. 6, and/or the wireless AP 760 depicted in Figs. 7 and 8. The authentication server may be similar to, the same as, or a component of the authentication servers 322-1, 322-2 depicted in Fig. 3, the authentication servers 622-1, 622-2, 622-3 depicted in Fig. 6, and/or the authentication server 722 depicted in Figs. 7 and 8.

[0062] Although the operations of the method(s) herein are shown and described in a particular order, the order of the operations of each method may be altered so that certain operations may be performed in an inverse order or so that certain operations may be performed, at least in part, concurrently with other operations. In another embodiment, instructions or sub-operations of distinct operations may be implemented in an intermittent and/or alternating manner.

[0063] It should also be noted that at least some of the operations for the methods described herein may be implemented using software instructions stored on a computer useable storage medium for execution by a computer. As an example, an embodiment of a computer program product includes a computer useable storage medium to store a computer readable program.

[0064] The computer-useable or computer-readable storage medium can be an electronic, magnetic, optical, electromagnetic, infrared, or semiconductor system (or apparatus or device). Examples of non-transitory computer-useable and computer-readable storage media include a semiconductor or solid-state memory, magnetic tape, a removable computer diskette, a random-access memory (RAM), a read-only memory (ROM), a rigid magnetic disk, and an optical disk. Current examples of optical disks include a compact disk with read only memory (CD-ROM), a compact disk with read/write (CD-R/W), and a digital video disk (DVD).

[0065] Alternatively, embodiments of the invention may be implemented entirely in hardware or in an implementation containing both hardware and

software elements. In embodiments which use software, the software may include but is not limited to firmware, resident software, microcode, etc.

[0066] Although specific embodiments of the invention have been described and illustrated, the invention is not to be limited to the specific forms or arrangements of parts so described and illustrated. The scope of the invention is to be defined by the claims appended hereto and their equivalents.

WHAT IS CLAIMED IS:

1. A method of communications, the method comprising:

from a wireless sensor deployed at a customer site, connecting to a wireless access point (AP) deployed at the customer site; and

based on a private key stored in the wireless sensor, performing mutual authentication between the wireless sensor and an authentication server connected to the wireless AP.

2. The method of claim 1, further comprising deriving an encryption key for communications between the wireless sensor and the wireless AP in response to the mutual authentication.

3. The method of claim 2, further comprising at the wireless sensor deployed at the customer site, conducting wireless communications with the wireless AP using the encryption key.

4. The method of claim 2, wherein deriving the encryption key for communications between the wireless sensor and the wireless AP in response to the mutual authentication comprises deriving the encryption key for communications between the wireless sensor and the wireless AP in response to a shared secret generated as a result of the mutual authentication.

5. The method of claim 4, further comprising transmitting the shared secret from the authentication server to the wireless AP.

6. The method of claim 4, wherein the shared secret comprises a Pre-Master Key (PMK).

7. The method of claim 4, wherein the encryption key comprises a Pairwise Transient Key (PTK).

8. The method of claim 1, wherein the private key is stored in a Trusted Platform Module (TPM) of the wireless sensor.

9. The method of claim 1, wherein based on the private key stored in the wireless sensor, performing the mutual authentication between the wireless sensor and the authentication server connected to the wireless AP comprises based on the private key stored in the wireless sensor, performing the mutual authentication between the wireless sensor and the authentication server connected to the wireless AP using a Transport Layer Security (TLS) protocol where a TLS client is the wireless sensor.

10. The method of claim 1, wherein based on the private key stored in the wireless sensor, performing the mutual authentication between the wireless sensor and the authentication server connected to the wireless AP comprises exchanging a server certificate, a server signature, a client certificate, and a client signature between the wireless sensor and the authentication server.

11. The method of claim 1, wherein based on the private key stored in the wireless sensor, performing the mutual authentication between the wireless sensor and the authentication server connected to the wireless AP comprises:

from the wireless sensor, transmitting a client message to the authentication server;

at the wireless sensor, receiving a server message, a server certificate, and a server signature from the authentication server in response to the client message;

at the wireless sensor, verifying the server signature; and

from the wireless sensor, transmitting a client certificate to the authentication server when the server signature is successfully verified.

12. The method of claim 11, wherein based on the private key stored in the wireless sensor, performing the mutual authentication between the wireless sensor and the authentication server connected to the wireless AP further comprises:

transmitting a signature request to a Trusted Platform Module (TPM) of the wireless sensor in which the private key is stored; and

receiving a client signature from the TPM of the wireless sensor, wherein the client signature is generated based on the private key.

13. The method of claim 12, wherein based on the private key stored in the wireless sensor, performing the mutual authentication between the wireless sensor and the authentication server connected to the wireless AP further comprises:

from the wireless sensor, transmitting the client signature to the authentication server; and

at the authentication server, verifying the client signature.

14. A wireless sensor deployed at a customer site, the wireless sensor comprising:

a wireless transceiver configured to connect to a wireless access point (AP) deployed at the customer site; and

a controller configured to store a private key and to, based on the private key, perform mutual authentication with an authentication server connected to the wireless AP.

15. The wireless sensor of claim 14, wherein the controller is further configured to derive an encryption key for communications between the wireless sensor and the wireless AP in response to the mutual authentication.

16. The wireless sensor of claim 15, wherein the controller is further configured to conduct wireless communications with the wireless AP using the encryption key.

17. The wireless sensor of claim 14, wherein the controller comprises a Trusted Platform Module (TPM) configured to store the private key.

18. The wireless sensor of claim 14, wherein the controller comprises a Transport Layer Security (TLS) unit configured to, based on the private key stored in the wireless sensor, perform the mutual authentication with the authentication

server connected to the wireless AP using a TLS protocol where a TLS client is the wireless sensor.

19. The wireless sensor of claim 14, wherein the controller comprises a cryptographic engine configured to receive a message digest and generate a client signature of the message digest based on the private key.

20. A method of communications, the method comprising:

from a wireless sensor deployed at a customer site, connecting to a wireless access point (AP) deployed at the customer site;

based on a private key stored in a Trusted Platform Module (TPM) of the wireless sensor, performing mutual authentication between the wireless sensor and an authentication server connected to the wireless AP;

deriving a Pairwise Transient Key (PTK) for communications between the wireless sensor and the wireless AP in response to a Pre-Master Key (PMK) generated as a result of the mutual authentication; and

at the wireless sensor deployed at the customer site, conducting wireless communications with the wireless AP using the PTK.

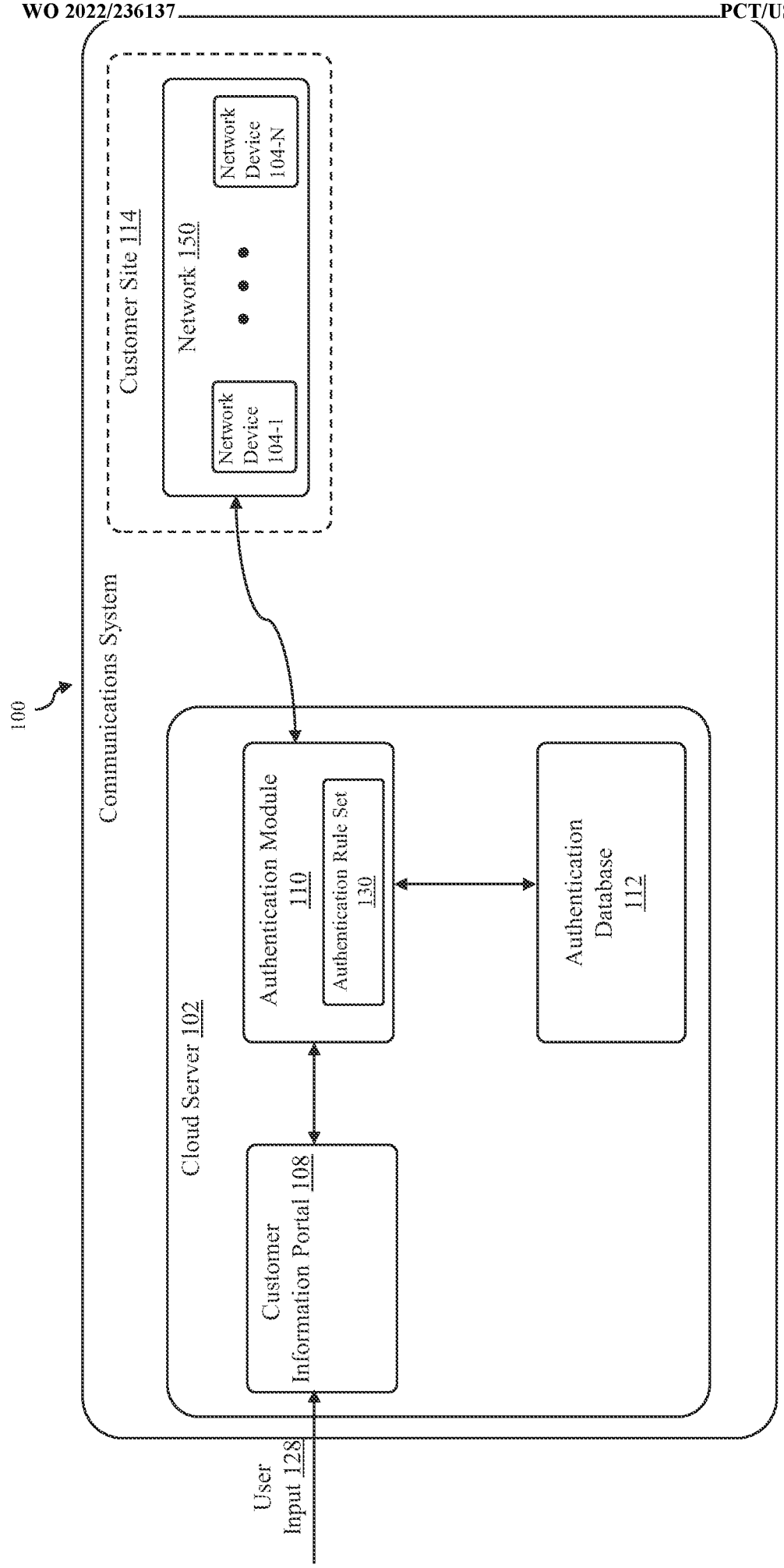
100
Communications System
Customer Site 114
Network 150
Network Device 104-1
Network Device 104-N
Cloud Server 102
Authentication Module 110
Authentication Rule Set 130
Authentication Database 112
Customer Information Portal 108
User Input 128

FIG. 1

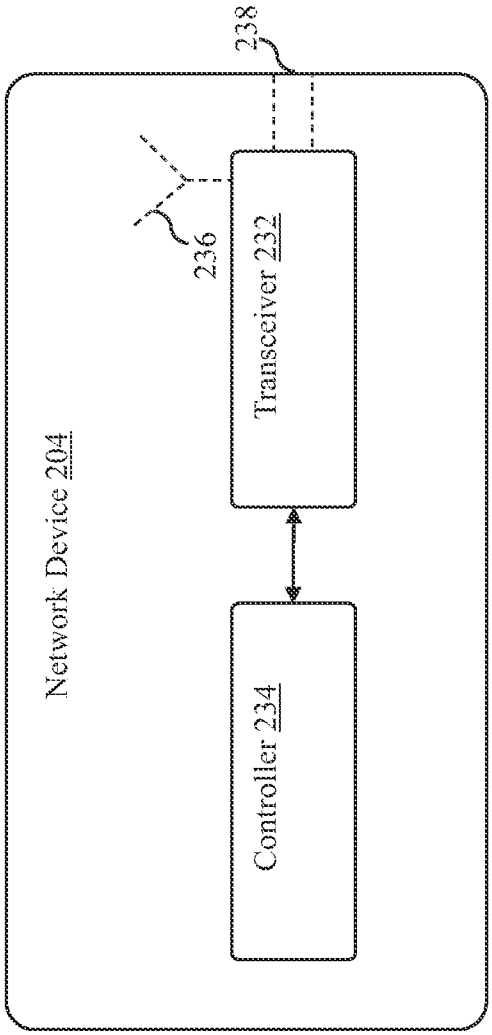

FIG. 2

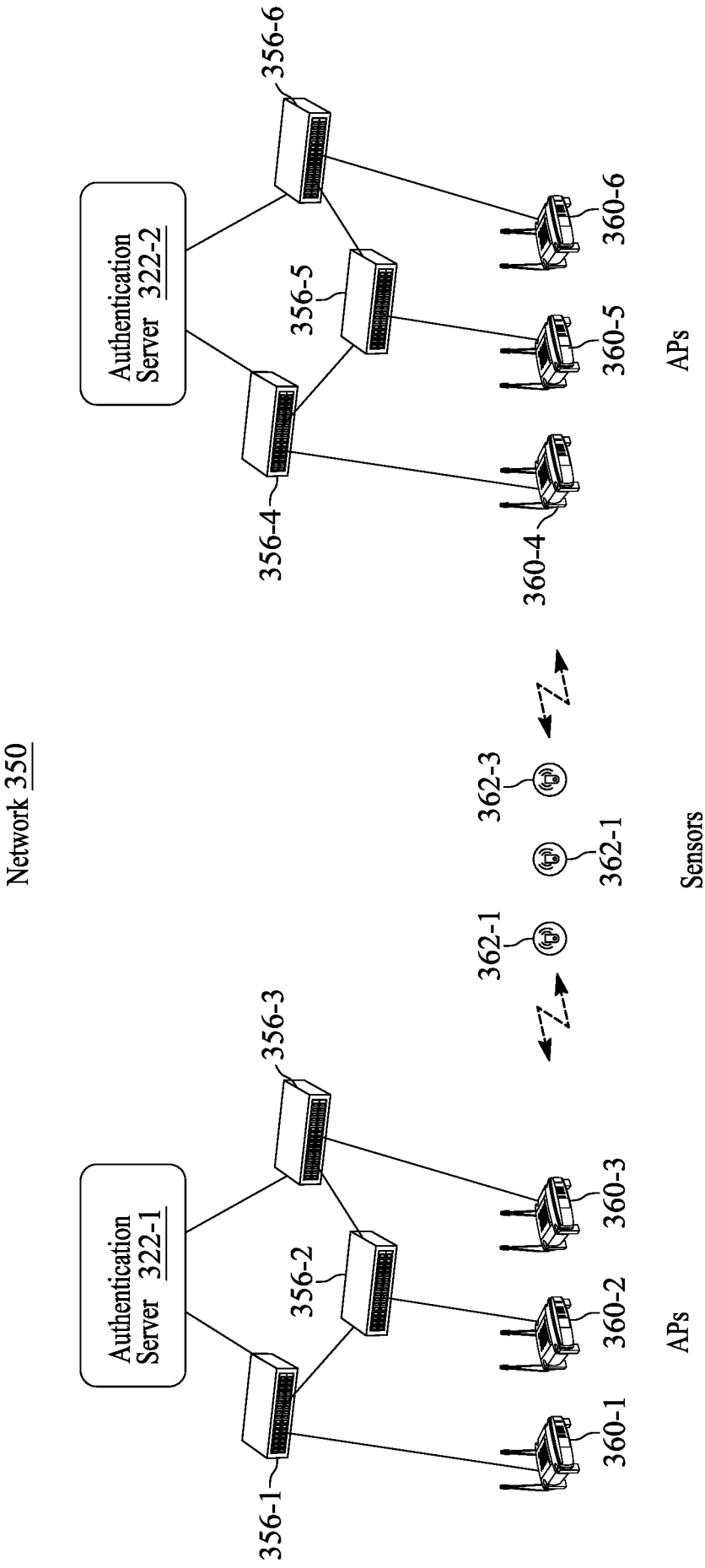
Network 350
Authentication Server 322-1
Authentication Server 322-2
356-1
356-2
356-3
356-4
356-5
356-6
360-1
360-2
360-3
360-4
360-5
360-6
APs
362-1
362-1
362-3
Sensors

FIG. 3

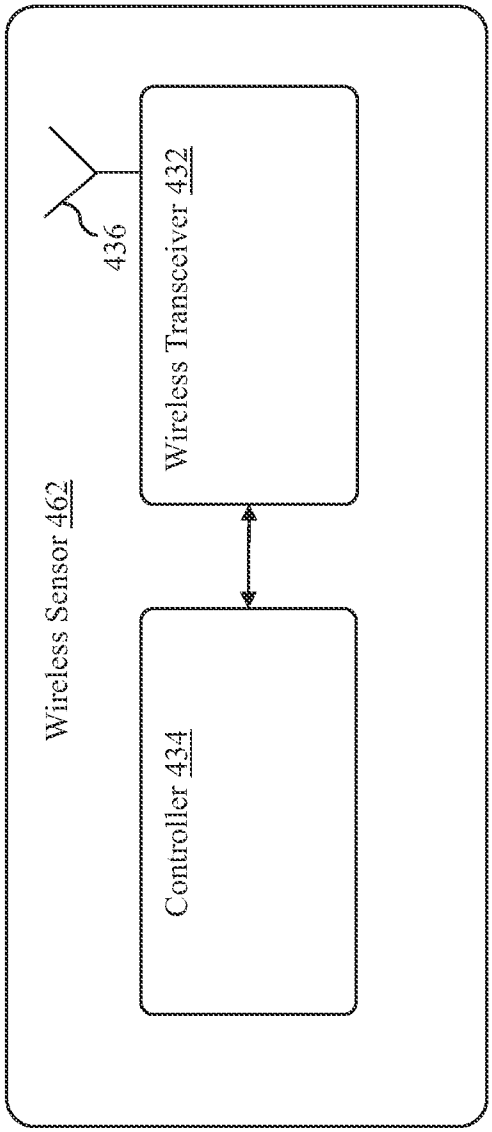
Wireless Sensor 462
436
Wireless Transceiver 432
Controller 434

FIG. 4

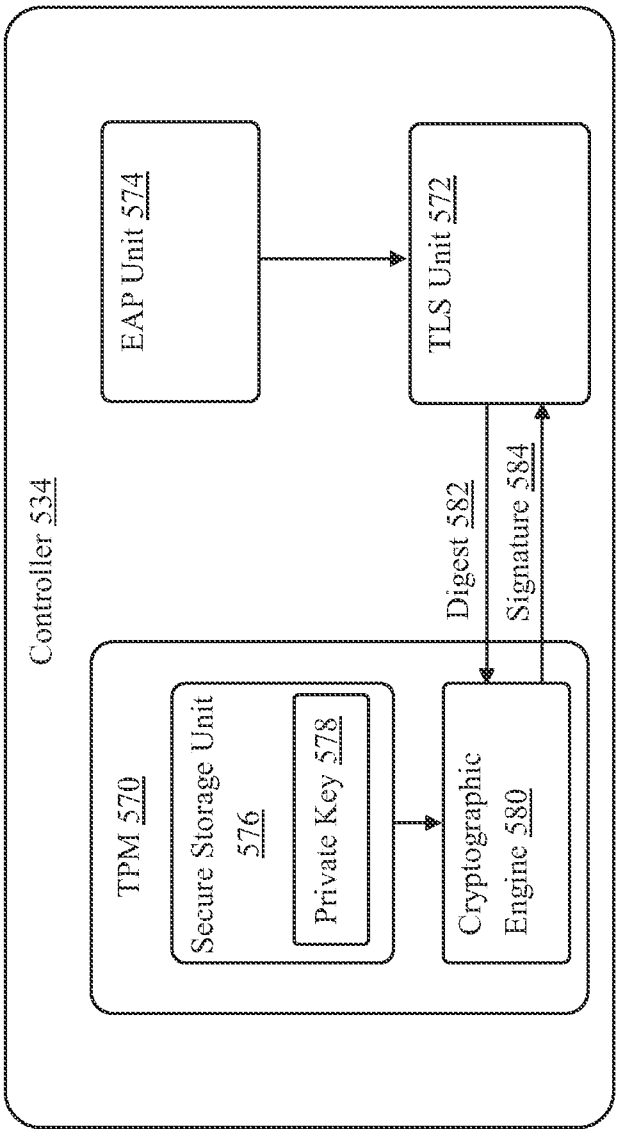
Controller 534
EAP Unit 574
TLS Unit 572
Digest 582
Signature 584
TPM 570
Secure Storage Unit 576
Private Key 578
Cryptographic Engine 580

FIG. 5

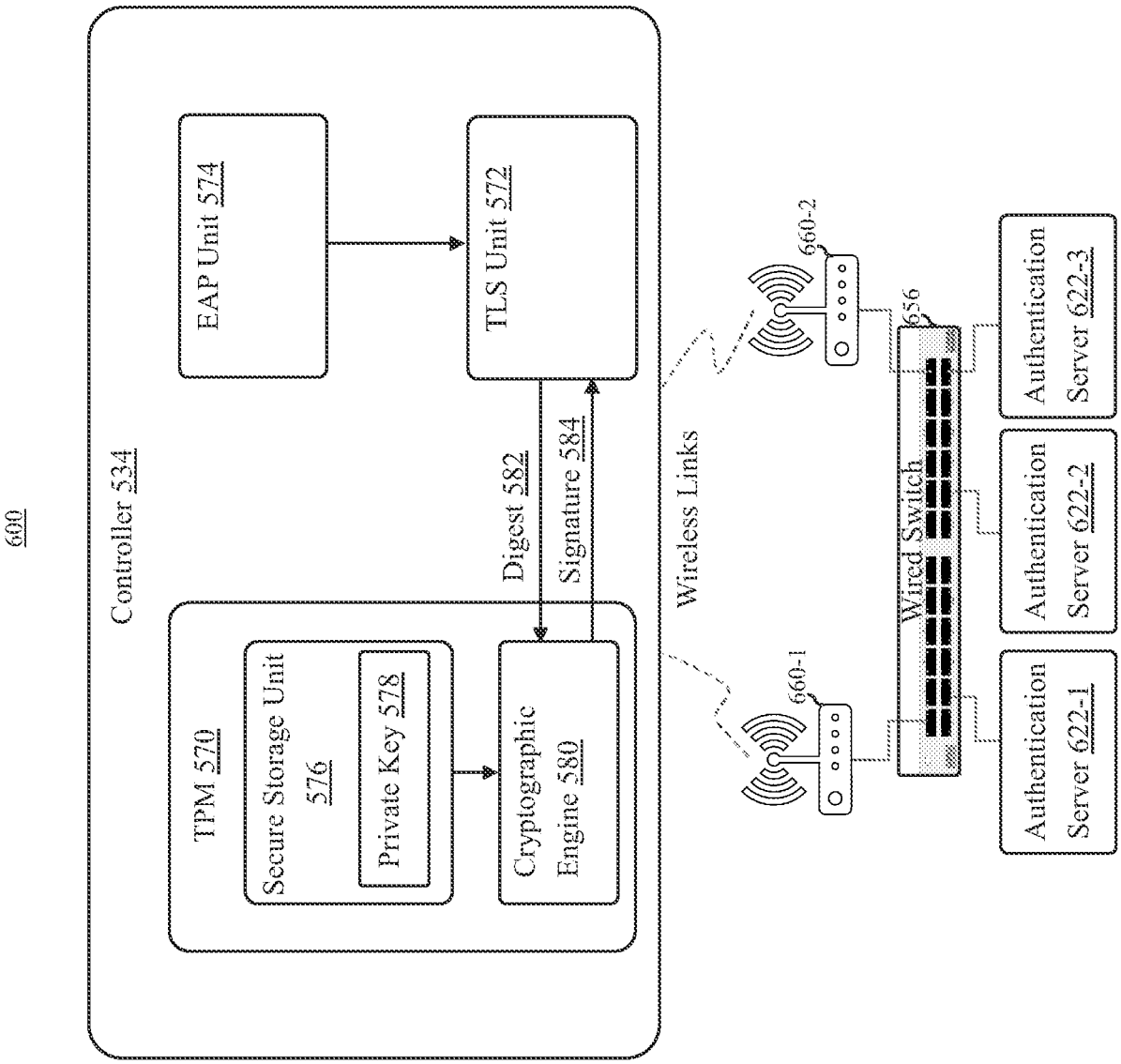
600
Controller 534
EAP Unit 574
TLS Unit 572
TPM 570
Secure Storage Unit 576
Private Key 578
Cryptographic Engine 580
Digest 582
Signature 584
Wireless Links
660-1
660-2
656
Wired Switch
Authentication Server 622-1
Authentication Server 622-2
Authentication Server 622-3

FIG. 6

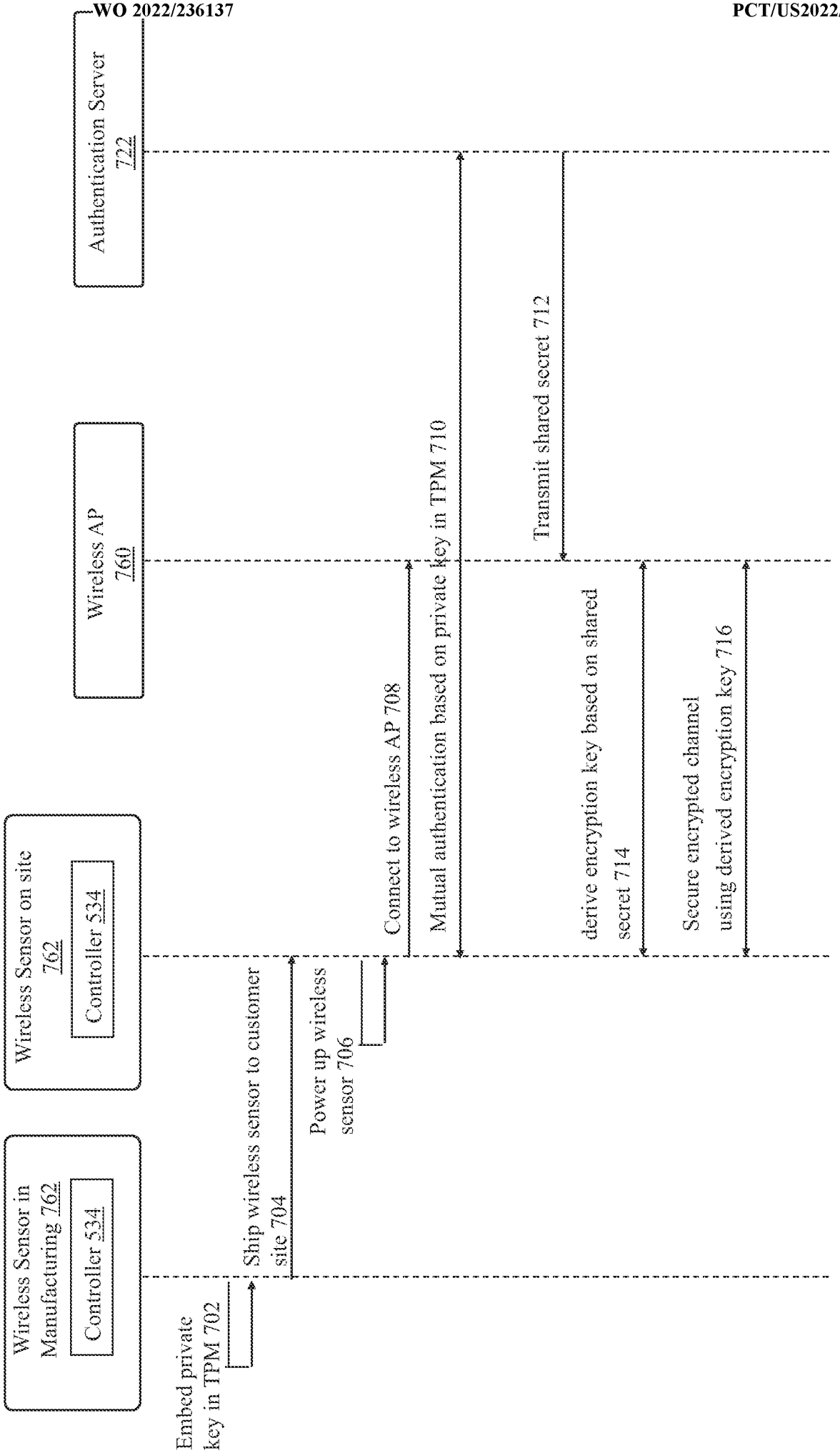
Wireless Sensor in Manufacturing 762
Controller 534
Wireless Sensor on site 762
Controller 534
Wireless AP 760
Authentication Server 722
Embed private key in TPM 702
Ship wireless sensor to customer site 704
Power up wireless sensor 706
Connect to wireless AP 708
Mutual authentication based on private key in TPM 710
Transmit shared secret 712
derive encryption key based on shared secret 714
Secure encrypted channel using derived encryption key 716

FIG. 7

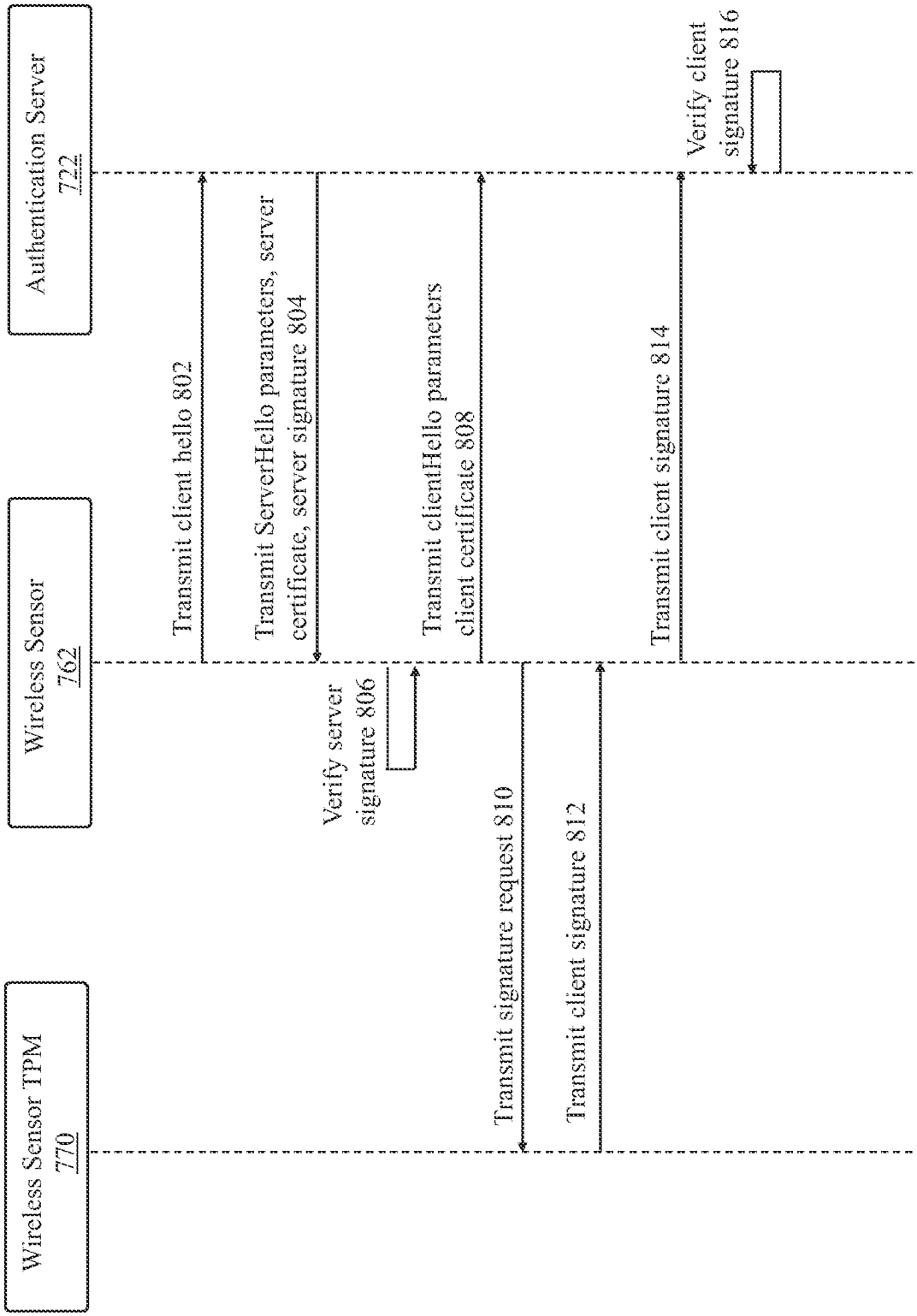
Wireless Sensor TPM 770
Wireless Sensor 762
Authentication Server 722
Transmit client hello 802
Transmit ServerHello parameters, server certificate, server signature 804
Verify server signature 806
Transmit clientHello parameters client certificate 808
Transmit signature request 810
Transmit client signature 812
Transmit client signature 814
Verify client signature 816

FIG. 8

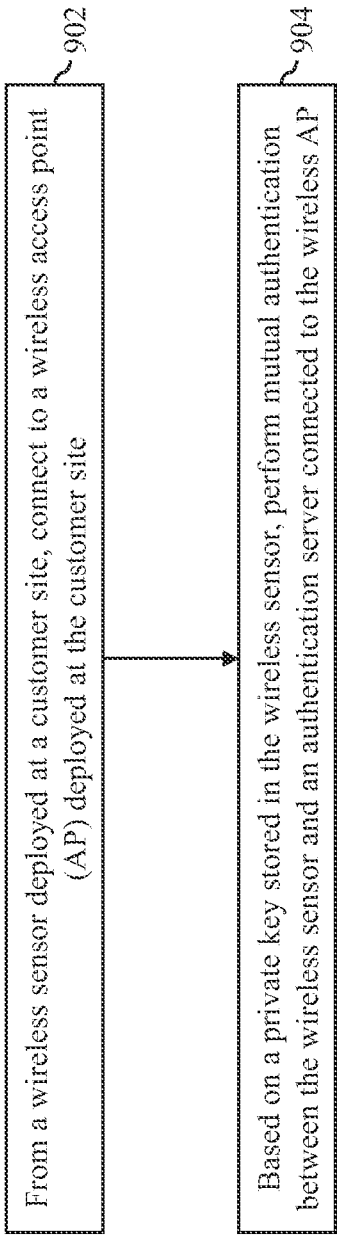
From a wireless sensor deployed at a customer site, connect to a wireless access point (AP) deployed at the customer site
902
Based on a private key stored in the wireless sensor, perform mutual authentication between the wireless sensor and an authentication server connected to the wireless AP
904

FIG. 9

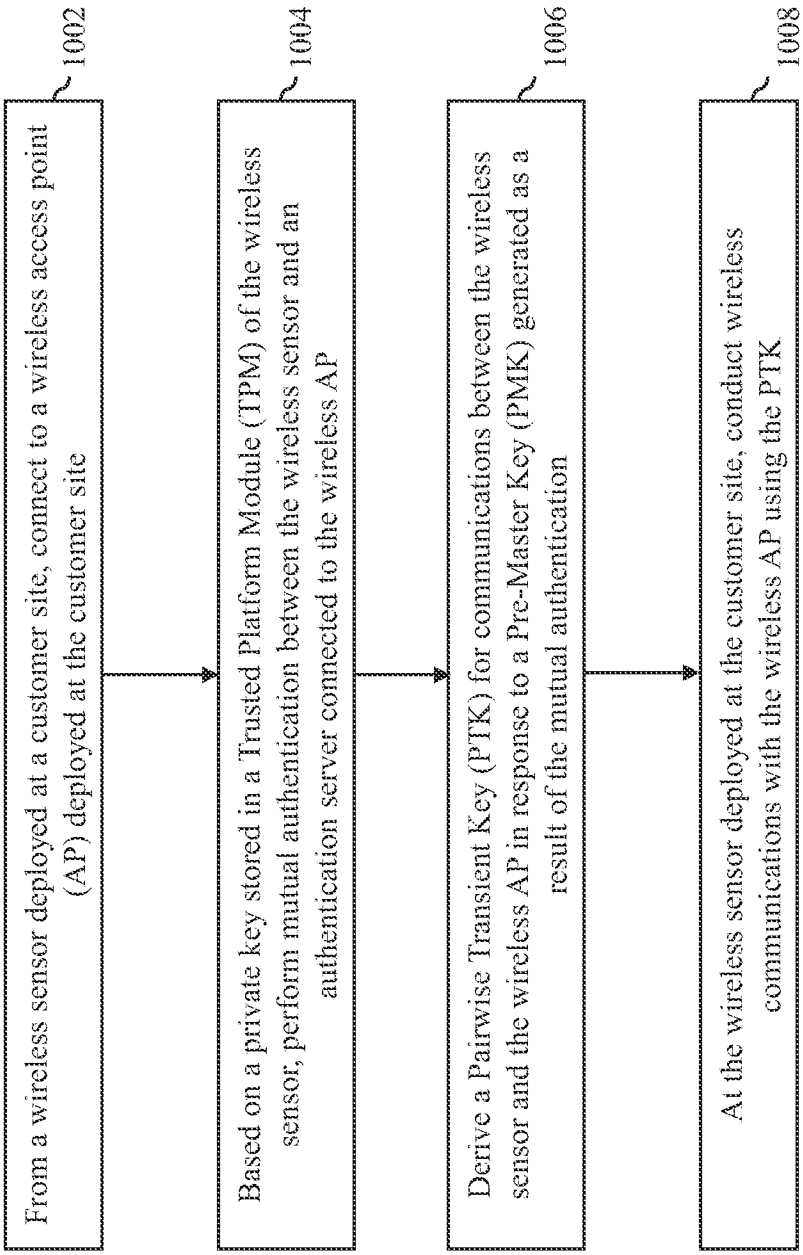
From a wireless sensor deployed at a customer site, connect to a wireless access point (AP) deployed at the customer site
1002
Based on a private key stored in a Trusted Platform Module (TPM) of the wireless sensor, perform mutual authentication between the wireless sensor and an authentication server connected to the wireless AP
1004
Derive a Pairwise Transient Key (PTK) for communications between the wireless sensor and the wireless AP in response to a Pre-Master Key (PMK) generated as a result of the mutual authentication
1006
At the wireless sensor deployed at the customer site, conduct wireless communications with the wireless AP using the PTK
1008

FIG. 10

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2022/028194

A. CLASSIFICATION OF SUBJECT MATTER

IPC: H04W 12/06
CPC: H04W 12/06

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

CPC: H04W 12/06, 12/03, 12/041, 8/18, 88/08; H04L 9/0819, 9/085, 9/0897, 9/3247, 9/3268, 63/0869, 63/166

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

USPC: 713/168, 169, 170, 171, 172, 190; 726/2, 27

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

US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB; Search Terms: wireless, device, mode, sensor, authentication, server, access, transient, key

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
	US 2018/0199205 A1 (ZHU ET AL.) 12 July 2018 (12.07.2018),	
X	entire document,	1-7, 9-11, 14-16 and 18-20
Y	entire document,	8 and 17
A	entire document.	12-13
	US 2003/0138105 A1 (CHALLENER ET AL.) 24 July 2003 (24.07.2003),	
Y	entire document,	8 and 17
A	entire document.	12-13

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

Date of the actual completion of the international search	Date of mailing of the international search report
30 June 2022 (30.06.2022)	JUL 05 2022
Name and mailing address of the ISA/US **COMMISSIONER FOR PATENTS MAIL STOP PCT, ATTN: ISA/US P.O. BOX 1450 ALEXANDRIA, VA 22313-1450, UNITED STATES OF AMERICA** Facsimile No. **(571)273-8300**	Authorized officer **HARRY C. KIM** Telephone No. **571-272-4300**