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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
24 May 2012 (24.05.2012)

WIPO | PCT

(10) International Publication Number
WO 2012/068045 A2

(51) International Patent Classification:
H04L 9/00 (2006.01)

(21) International Application Number:
PCT/US2011/060694

(22) International Filing Date:
15 November 2011 (15.11.2011)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
61/413,538 15 November 2010 (15.11.2010) US
61/441,375 10 February 2011 (10.02.2011) US

(71) Applicant *(for all designated States except US)*: **TRILLIANT HOLDINGS INC.** [US/US]; 1100 Island Drive, Redwood City, CA 94065 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **OTA, Nathan** [US/US]; 380 Arkansas Street, San Francisco, CA 94107 (US). **CONANT, Robert** [US/US]; 1810 Barroilhet, Burlingame, CA 94010 (US). **VEILLETTE, Michel** [CA/CA]; 109 Des Flandres, Waterloo, ON J0E 2N0 (CA). **BEMMEL, Vincent** [US/US]; 7403 Las Palmas Way, Dublin, CA 94568 (US). **ENNS, Frederick** [US/US]; 545 Hobart Street, Menlo Park, CA 94025 (US).

(74) Agent: **BEY, Dawn-MARIE**; King & Spalding LLP, 1700 Pennsylvania Avenue, N.W., Suite 200, Washington, DC 20006 (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, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

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

[Continued on next page]

(54) Title: SYSTEM AND METHOD FOR SECURELY COMMUNICATING ACROSS MULTIPLE NETWORKS USING A SINGLE RADIO

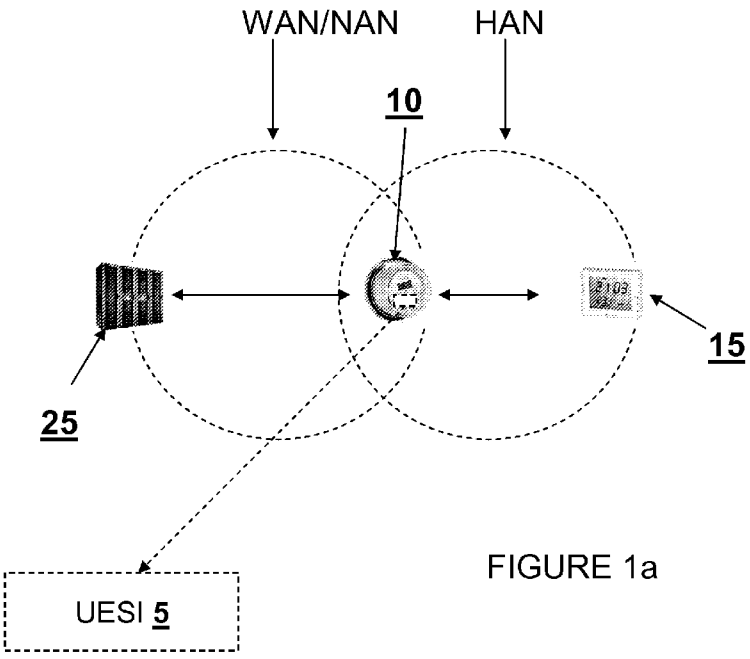


FIGURE 1a

(57) Abstract: A communications module for facilitating secure communications on a first network and a second network includes: a single transceiver for receiving and transmitting first network messages from and to the first network and at least transmitting second network messages to the second network; at least a first processor connected to the single transceiver for processing one or more first network messages and second network messages; the at least a first processor including first network logic for processing first network messages and second network logic for processing second network messages; and the second network logic including instructions for securing second network messages such that decryption of the second network messages is limited to a particular receiving device on the second network. The second network messages may include commodity pricing and use information.

WO 2012/068045 A2

Published:

— *without international search report and to be republished upon receipt of that report (Rule 48.2(g))*

SYSTEM AND METHOD FOR SECURELY COMMUNICATING ACROSS MULTIPLE NETWORKS USING A SINGLE RADIO

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] The present application claims benefit of U.S. provisional patent application No. 61/413,538 titled "SYSTEMS AND METHODS FOR SINGLE RADIO USE ACROSS MULTIPLE NETWORKS" filed November 15, 2010, which is incorporated herein by reference in its entirety and U.S. provisional patent application No. 61/441,375 titled "DEVICE AND METHOD FOR FACILITATING SECURE COMMUNICATIONS OVER A CELLULAR NETWORK" filed February 10, 2011, also incorporated by reference herein in its entirety.

BACKGROUND OF THE INVENTION

Field of Embodiments

[0002] The present embodiments relate generally to a system and process that utilizes a single radio, i.e., a single transceiver, to bridge communications between multiple independent networks and facilitates secure one-way communication of information to devices on a single-hop network. More particularly, the various embodiments relate to making use of a single radio existing within a node of a network to facilitate secure communication from a back-end processor to both the node as part of a first network, e.g., neighbourhood area network ("NAN"), and end-use devices that are part of a second network, e.g., home area network ("HAN"). Additionally, various embodiments relate generally to a system and process that facilitates secure one-way and two-way communication of private information over a one-hop network such as a home area network (HAN).

Description of Related Art

[0003] In the utility delivery space, there have been numerous advances in technology in efforts to provide improved methods and systems for monitoring and controlling the delivery and use of various utilities, e.g., electricity, water, gas, etc. By way of specific example, advanced metering infrastructures ("AMIs") have been developed which incorporate smart meters or existing meters retrofitted with a communications component that include at least a radio, i.e., transceiver, and configurable microprocessor. These meters may be more generically referred to as nodes and are configured to communicate using predetermined protocols with other nodes in the AMI across what is commonly referred to as a neighbourhood area network ("NAN"). One

primary function of the AMI is to monitor delivery, i.e., is delivery occurring at all as in the case of power outages, as well as reporting back meter readings to back-end systems. The ability to achieve this monitoring automatically and wirelessly is an important advancement over the wired, drive by or house-to-house meter reading methodologies of the past.

[0004] While the AMIs have vastly improved the flow of information to the utility companies regarding utility usage based on the meter readings, the utility usage associated with a single meter, e.g., within a particular residence or building can theoretically be further broken down according to individual load, e.g., by appliance. With the development of smart appliances, consumers are able to monitor and even control energy usage within their homes and businesses. Such appliances are also referred to as demand-side management ("DSM") devices or in-home devices ("IHDs"). A network of multiple smart appliances or individual load monitors is often referred to as a home area network ("HAN").

[0005] Various protocols, methodologies and system configurations have been developed in order to facilitate information and data transmission within the NAN, within the HAN and to and from a back-end system, usually requiring either a wired connection or transmission over another network, e.g., wide area network ("WAN"). Due to the differing protocols and methodologies, the hardware is quite often different or duplicative or requires complex programming in order to facilitate secure communication across varying devices and multiple networks.

[0006] It is desired to provide and request/receive communications including data related to utility consumption, rates and cost in real-time or quasi-real-time. Current configurations for facilitating such communication require additional components and/or software installation and complex routing in order to bridge the NAN-HAN. For example, US Patent No. 7,317,404 requires the addition of a specific transmitter to utility meters in order to transmit consumption data to a display module within the HAN. Further, US Patent No. 7,545,285 requires a master controller to listen in on communications between a meter and a reading system and perform various actions, such as load interrupt, depending on the communication particulars. Further still, US Patent No. 7,427,927 requires a display with separate radio for listening to or requesting communications between a meter and a reading system and capturing certain meter data in a memory of the display for display to the user. Heretofore, all configurations for bridging the HAN-NAN communication gap require at least three radios: two in the meter (NAN and HAN)

and one in a home device (HAN) for an architecture wherein the meter acts as the gateway; or one in meter (NAN) and two in the home device (HAN and NAN) for an architecture wherein a HAN device acts as the gateway.

[0007] Additionally, the Zigbee Smart Energy Profile (ZSE) version 1.0 supports a method for delivering information to DSM devices called Inter-PAN. This method consists of an IEEE 802.15.4 point to point communication between an Inter-PAN ZSE server and Inter-PAN ZSE clients. In version 1.0, this mechanism is limited to the transmission of public pricing information and public messages using a polling method. This means that each Inter-PAN ZSE client needs to request the information needed from one of the accessible Inter-PAN ZSE servers. There are no criteria in the selection of the Inter-PAN ZSE server used by an Inter-PAN client. This Inter-PAN configuration does not utilize any security, it is dependent on client requests to pull information from the server, information is limited to public messages and there is no guarantee that this server is associated the same premise.

[0008] The existing systems for providing and/or requesting communications including data related to utility consumption, rates and cost do not provide for secure wireless communication, electricity pricing information, premise association, and use of existing infrastructure. Accordingly, there is a need in the art for a method and system to provide price and energy usage information from an AMI network into the HAN in a way that reduces complexity, increases cybersecurity, and preserves consumer privacy.

[0009] Additionally, there is a need in the art for a mechanism to allow for secure, wireless communication between field tools and one or more nodes of a secure one-hop network, e.g., HAN, in an ad hoc fashion for performance of various tasks, e.g., operations and maintenance services (O&M services such as installations, configuration changes, firmware upgrades, etc.). There is a need in the art for a process and system for facilitating secure connection and communication with networked devices without requiring joinding with or creation of a network.

SUMMARY

In a first embodiment, a communications module for facilitating secure communications on a first network and a second network includes: a single transceiver for receiving and transmitting first network messages from and to the first network and at least transmitting second

network messages to the second network; at least a first processor connected to the single transceiver for processing one or more first network messages and second network messages; the at least a first processor including first network logic for processing first network messages and second network logic for processing second network messages; and the second network logic including instructions for securing second network messages such that decryption of the second network messages is limited to a particular receiving device on the second network.

In a second embodiment, a process for registering a device located on a home area network with a communications module to facilitate receipt at the device of messages from the communications module that originated outside of the home area network includes: receiving a device registration key that is unique to the device at a head end system that is not on the home area network; receiving at the communications module the device registration key from the head end system; transmitting by the communications module a registration message encrypted with a version of the device registration key on multiple communication channels; listening by the device for registration messages on a particular communication channel within the multiple communication channels; and upon receiving on the particular communication channel the registration message encrypted with the device's registration key, decrypting the registration message to retrieve a shared link key for decrypting application messages from the communications module.

In a third embodiment, a process for registering multiple devices located on a home area network with a communications module to facilitate receipt at the multiple devices of messages from the communications module that originated outside of the home area network includes: receiving a unique device registration key for each of the multiple devices at a head end system that is not on the home area network; receiving at the communications module each of the unique device registration keys from the head end system; transmitting by the communications module on multiple communication channels individual registration messages each encrypted with a version of one the multiple device registration keys; listening by each of the multiple devices for registration messages on a particular communication channel within the multiple communication channels; upon receiving on the particular communication channel the registration message encrypted with an individual of the multiple device's registration key, decrypting the registration message to retrieve one of a first or second shared link key for decrypting application messages encrypted with one of the first or second shared link keys from the communications module;

wherein each of the multiple devices on the home area network receives either the first or the second shared link key, but not both.

BRIEF DESCRIPTION OF THE FIGURES

[0010] **Figures 1a** through **1e** are schematics showing representative components and networks of a system in accordance with various embodiments described herein;

[0011] **Figures 2a** and **2b** are schematics showing a representative UESI in accordance with various embodiments described herein;

[0012] **Figure 3** is a schematic showing states of a client device in accordance with various embodiments described herein;

[0013] **Figures 4a** and **4b** are process flows for general steps in secure one-way and secure two-way inter-PAN processes in accordance with embodiments described herein;

[0014] **Figure 5** is a schematic showing communication flow between various components and networks in accordance with various embodiments described herein;

[0015] **Figure 6** illustrates process steps for client device from non-commissioned state to registered and active in accordance with various embodiments described herein;

[0016] **Figure 7** is a schematic showing registration communication flow between various components and networks in accordance with various embodiments described herein;

[0017] **Figure 8** is a schematic showing registration and application message flow between various components and networks in accordance with various embodiments described herein;

[0018] **Figure 9** is an alternative schematic illustrating message flow and timing intervals in accordance with a secure one-way registration process;

[0019] **Figure 10** is a schematic showing overlapping sub-domains with a HAN for receiving messages in accordance with a secure one-way registration process;

[0020] **Figure 11** is a prior art exemplary message flow for SLK establishment in accordance with two-way Inter-PAN process; and

[0021] **Figure 12** is a schematic showing various architectures for managing security keys across networks in accordance with one or more embodiments described herein; and

DETAILED DESCRIPTION

[0022] This document includes the following acronyms.

AES	Advanced Encryption Standard
AMI	Advanced Metering Infrastructure
API	Application Programming Interface
APS	Application support sub-layer
CBKE	Certificate-based Key Establishment
CCM*	Modified 'Counter with Cipher Block Chaining Message Authentication Code' mode of operation for cryptographic block ciphers
CPP	Critical Peak Pricing
CSS	Customer Service System
ECC	Elliptic Curve Cryptography
EMS	Energy Management System
ENC-MIC-32	32-bit encryption mode composed of a combination of Encryption (ENC) and Message Integrity Code (MIC) modes.
UESI	Utility Energy Services Interface
ESP	Energy Services Portal – a ZSE embodiment of an ESI
EUI64	Extended Universal Identifier-64
HAN	Home Area Network
HES	Head-End Server (or System)
IHD	In-Home Display
ISO	Independent System Operator
LED	Light Emitting Diode
LSB	Least Significant Bit
MAC	Medium Access Control (referring to protocol stack sublayer)
MMO	Matyas-Meyer-Oseas one way hash function
NAN	Neighborhood Area Network
NWK	Network
OOB	Out-of-band
PAN	Personal area network
PCT	Programmable Communicating Thermostat
PEV	Plug-in Electric Vehicle
PHY	Physical Layer (referring to protocol stack sublayer)
RF	Radio Frequency
SE	Smart Energy
TOU	Time of Use pricing schedule
UTC	Coordinated Universal Time standard
UTF-8	8-bit Unicode Transformation Format Unicode Transformation Format
ZCL	ZigBee Cluster Library

ZSE	ZigBee Smart Energy

[0023] The following documents are incorporated herein by reference in their entirety: "UCAIug Home Area Network System Requirements Specification: A Work Product of the OpenHAN Task Force formed by the SG Systems Working Group under the Open Smart Grid (OpenSG) Technical Committee of the UCA International Users Group," Version 2.0 - August 30, 2010 (OHP Document); "ZigBee Smart Energy Profile Specification," ZigBee Profile: 0x0109; Revision 15, December 1, 2008, Document 075356r15 (SEP Document); ZigBee Smart Energy Test Specification, May 2008 ZigBee Document 075384r17; ZigBee Cluster Library Specification, ZigBee Document 075123r02ZB; and Institute of Electrical and Electronics Engineers, Inc., IEEE Std. 802.15.4- 2003 & 2006, IEEE Standard for Information Technology - Telecommunications and Information Exchange between Systems - Local and Metropolitan Area Networks - Specific Requirements - Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low Rate Wireless Personal Area Networks (WPANs).

[0024] Additionally, throughout the document, the terms and phrases HAN device, client device, Inter-PAN client device, Inter-PAN client and client are used interchangeably. Similarly, the terms and phrases Inter-PAN server and UESI are used interchangeably.

[0025] Referring to **Figure 1a**, a simplified schematic illustrates the various networks utilized in a system of the present invention, including wide area network (WAN)/ neighbourhood area network (NAN) (also referred to as an AMI network) and home area network (HAN) and representative components within each network. For example, the WAN/NAN communicates with the head end server (HES) for requesting, processing, transmitting communications to/from nodes including, e.g., a meter (also referred to as an AMI node), shown in **Figure 1a** as an electric meter; and the HAN includes end user devices such as thermostats. As discussed further below, the system has at least the following features: a single radio for both NAN and HAN communications; HAN device may exist on a separate logically secure HAN network; uses same MAC/PHY layer in both NAN and HAN; secure links between NAN nodes (e.g., meters, stand-alone, thermostats that are retrofitted or originally manufactured to include the Utility Energy Service Interface (UESI) hardware and logic described herein) into the HAN; secure communications between meter and NAN; and simplified commissioning process.

[0026] In operation, the AMI node receives a security key from AMI network that itself is encrypted using the AMI security which is at the application layer as described further in pending U.S. Patent Application No. Serial No. 12/554,135 entitled: A SYSTEM AND METHOD FOR IMPLEMENTING MESH NETWORK COMMUNICATIONS USING A MESH NETWORK PROTOCOL which is incorporated herein by reference in its entirety. The AMI node uses this security key to authenticate and encrypt communications to the HAN devices at the MAC layer. The encryption and authentication mechanisms may be different as between the AMI network and the HAN network.

[0027] Information is pushed from the AMI node using a single radio that simultaneously operates the AMI network and the HAN network. Information is automatically sent to the associated HAN devices using one-way communication (or two way communication in accordance with a particular embodiment). The transmission of information to HAN devices occurs even if these devices are not capable of sending messages back to the sending AMI node. The AMI node sends messages into the HAN on all channels in the communication band and this operation occurs simultaneously with AMI network communications. The communication is performed by a single radio in the AMI node, where the AMI network and the HAN operate on the same MAC/PHY layers but different routing protocols. In this configuration, a single radio in an AMI node (e.g. electric, gas, water meter) is used to transmit information into the HAN and potentially receive information from the HAN, where the single radio simultaneously supports communication protocols for both the NAN network and HAN network. The reduction from two to a single radio reduces costs for parts as well complexity of electronics. Additionally, the communications with the HAN are secured because the HAN key is not transmitted in the clear per secure key establishment using the pre-existing secure AMI communications. Secure communications between the AMI node and the HAN devices protect consumer information. Further, in one configuration, the flow of information is one-way from the AMI node into the HAN. This prevents unintended data flow of personal information from the HAN and into the AMI network.

[0028] Certain exemplary embodiments presented herein describe a Utility Energy Service Interface (UESI) that enables one-way (and two-way communications) of, e.g., private consumer-specific information to registered home area network (HAN) devices. Referring again to **Figure 1a**, the UESI **5** is part of an electric (or other utility) meter **10** capable of securely

broadcasting information, e.g., price and energy usage information, to a HAN device **15**. Specific embodiments further describe HAN device requirements for interaction with the UESI. In a representative embodiment, various ZigBee components used in this implementation include: ZigBee SEP Inter-PAN, ZigBee ZCL attribute reporting, the ZigBee SEP 1.0 Price cluster, and the Simple Meter cluster. Secure, originator-authenticated communication is achieved through the use of the ZigBee pre-configured application layer security.

[0029] Referring to **Figure 2a**, an exemplary UESI **5** includes at least a radio **100**, a processor **105** which includes separate communications logic for communicating with the NAN **105a** and HAN **105b**, a memory **110** which includes at least one database for storing table data, and a clock **115** for synchronization. Optionally, the UESI **5** is in communication with a user input component and a display device which are part of the node **10** (or other host device, e.g., stand-alone box, smart thermostat, etc.). Alternatively, the UESI **5** could include separate processors and databases for the NAN and HAN communications as shown in **Figure 2b**. The UESI clock is synchronized in accordance with the WAN/NAN clock as described in, for example, United States Patent Application No. 13/275,682 entitled "METHOD FOR SYNCHRONIZING METER CLOCKS IN A NETWORK" which is incorporated herein by reference in its entirety.

[0030] Coordination by the UESI of both NAN and HAN communications may occur autonomously in accordance with randomization processes implemented at the UESI or may be the result of predetermined coordination instructions passed down from, for example, the HES. Many messages are not based on relative time but on an absolute time mark. In an exemplary Time of Use (TOU) plan, tier switch occurs at, for example 5 PM and with it, a publish price message is broadcasted by UESIs currently using this TOU plan. Using randomization, a reduction of the strain on the WAN/NAN network of having all UESIs broadcasting and going "off the WAN/NAN network" simultaneously is achieved by introducing a random offset specific to each UESI for all transmissions. This offset is randomly generated between, for example, 0 and 60 seconds, and is applied to all transmissions so as to evenly spread out the transmission over the minute following the transmission request. An offset between 0 and 120 seconds is applied to registration packets as their impact on the network is greater considering they have to broadcast on all channels and that, under normal circumstances they request rebroadcasts less often than application messages.

[0031] Additionally, the UESI may be programmed with a soft switch, allowing for switching over from WAN/NAN only to dual use WAN/NAN and one-way HAN, or dual use WAN/NAN plus two-way HAN. The embodiments described herein are focused on descriptions of one-way HAN commissioning, registration and communications. Accordingly, the UESI can exist in three separate operational states controlled by the soft switch.

[0032] As described in the applicable OpenHAN 2.0 protocol (OHP), the UESI enables secure one-way interactions between commissioned HAN devices registered to the particular UESI and the UESI utility's advanced metering infrastructure (AMI). Security on this interface is robust and comprehensive in order to protect Utility assets (e.g. electric grid, AMI, etc.) and consumer information. The UESI is an interface for providing real-time energy usage information from the AMI meter or other node to HAN devices and is protected with cryptographic methods. The UESI is based on a secure one-way model where real-time information only flows from the UESI to registered HAN devices - an approach that inherently provides protection of Utility assets, as no HAN originated traffic flows upstream from the UESI into the AMI network.

[0033] The UESI is designed to do at least the following: register HAN devices, i.e., facilitate the OHP Commissioning process and Registration process for client devices to be able to successfully receive broadcast messages from the UESI; including updating the security keys and network parameters; broadcast price signals, i.e., broadcast electricity price information as received from the HES, or optionally based on a configured local schedule (e.g. every 10 minutes); broadcast energy usage, i.e., periodically broadcast energy usage information based on a configured local schedule (e.g. every 1 minute).

[0034] Implementation of an OHP compliant UESI that supports private broadcasts of consumer-specific information into a premise, requires some extensions to the current version of ZigBee SEP, as detailed below. UESI communications with client devices are based on the Inter-PAN transmission mechanism, which allows for communications via a special "stub" of the Application Support Sub-Layer, accessible through a special Service Access Point (SAP). Inter-PAN lends itself very well for this function because of its simplicity and effectiveness to address HAN devices. Unlike previous implementations wherein Inter-PAN was optional, it is a mandatory component of the processes described herein. **Table 1** below lists the extensions which facilitate secure Inter-PAN communications to support private broadcasts. **Table 1**

highlights differences between existing ZigBee Smart Energy (ZSE) Inter-PAN features and extensions required for UESI implementation pursuant to OHP requirements.

Table 1

Feature	ZSE version 1.0 Inter-PAN	Extensions
Communications mode	Uses IEEE 802.15.4 point-to-point communications between an Inter-PAN ZSE server and Inter-PAN ZSE client.	Uses IEEE 802.15.4 point-to-multipoint communications between a UESI and Inter-PAN client.
Security	Inter-PAN communications do not utilize security.	Communications are secured using the OOB Pre-Configured Link Key Process defined in the ZigBee Smart Energy Profile 1.0 specification, and uses AES-128/CCM* authenticated encryption to provide originator authentication as specified by the OHP specification security requirement for registered HAN devices.
Pull vs. Push	Inter-PAN communications rely on the ZSE client device to pull information from the ZSE server. This means that each Inter-PAN ZSE client needs to request the information needed from one of the accessible Inter-PAN ZSE servers.	Information is automatically pushed to the associated Inter-PAN clients. This approach allows for transmission of information to Inter-PAN clients, even if these clients are not capable of sending messages back to the server
Smart Energy application	In ZSE version 1.0, the Inter-PAN mechanism is limited to: Public Pricing information and Public Messages	Enables the support for private consumer information: Pricing information using the Price Cluster PublishPrice command. Energy usage information using the ZCL report attribute format to transmit Simple Metering Cluster server attributes.
Addressing	Inter-PAN supports the use of PAN ID in addition to MAC Address. Initial communications from the ZSE client device to ZSE server	All communication is from the UESI to the Inter-Pan client device, using the PAN ID, client device's MAC Address, and short broadcast MAC Address.

Feature	ZSE version 1.0 Inter-PAN	Extensions
	are broadcast to both the PAN ID and Destination Address, and are intended to facilitate the ZSE client device finding a ZSE server with the appropriate resource (i.e. availability to provide pricing or message information). Subsequent communications from the ZSE client device to the ZSE server may be unicast to both the PAN ID and Destination Address of the ZSE server. However, all communications from the ZSE server to the ZSE client device are unicast.	No direct communications from the client device to the server
Client-server binding within a premise	There are no defined criteria in the selection of the Inter-PAN ZSE server used by an Inter-PAN client device, and no guarantee that the selected server is associated with the same premise as the ZSE client device.	A defined registration mechanism enables service association with a specific premise

[0035] Referring to **Figure 1b** in a first embodiment facilitating one-way secure Inter-PAN communication to devices on a HAN, including a HES **5** which communicates over a WAN and NAN with a UESI (also referred to as a master smart energy information server) **10** which communicates information securely to one or more target devices **15** on a HAN. In this embodiment, the UESI provides secure smart energy information, e.g., publish price, energy usage information, load control information, text messages, directly to an subscribed target device. In the one-way Inter-PAN process, the objective is to provide sender authentication and confidentiality via encryption (as compared to two-way Inter-PAN, where the objective is to provide mutual authentication and confidentiality). As described further herein, for both one-way and two-way scenarios, there is an authentication phase followed by a phase where both parties arrive at a shared link key, which is then used to encrypt communications during the authorized session, and is valid until it times out.

[0036] Referring to **Figure 4a**, for one-way Inter-PAN, sender authentication and key distribution is achieved via an out-of-band registration process ("OOB") **S5** using a pre-configured link key (PLK) which is unique to each target device. During registration, a shared link key ("SLK") is sent from the UESI to each registered target device as part of the payload of the registration message which is encrypted with the PLK **S10**. The SLK is then used by the sender, e.g., UESI, to encrypt each application message **S20**. An optional step **S15** includes a filter for verifying at the target device the MAC address of the UESI. The target device times out if it cannot process an application message with a predetermined amount of time **S25**. Optionally the sender could also sign its messages using its private key, if a public/private key system is supported (public keys could be embedded in target devices during manufacturing).

[0037] The prior art ZigBee processes and components provide for a stand-alone Energy Services Interface (ZESI) that communicates information to ZigBee HAN devices. In accordance with embodiments herein, the ZESI and the UESI are able to coexist in the same premises, in compliance with OHP. In this scenario, a HAN device (e.g., IHD) can communicate independently with two physically different devices: a UESI in meter and a standalone ZESI. The registering process between the UESI, ZESI and HAN devices is as follows: The ZESI registers with the UESI and receives a Shared Link Key, Channel Mask and PAN-ID. The ZESI shall avoid any channels reserved by the UESI, as indicated via the Channel Mask. The ZESI shall avoid the PAN-ID used by the UESI. One or more HAN devices can register with the UESI and receive the Shared Link Key, Channel Mask and PAN-ID. After the ZESI is registered with the UESI, each HAN device can register with the ZESI and negotiate to receive a Network Key, a different PAN-ID and channel, the Trust Center Link Key, and optional Application Link Keys. A HAN device that communicates with both the UESI and the ZESI requires support of frequency agility to switch between channels. Whenever the ZESI receives a Registration message from the UESI requiring changes to the Shared Link key, Channel Mask, and/or PAN-ID, the ZESI shall initiate updates of its client devices via procedures described in the SEP Document which is incorporated herein by reference.

[0038] Alternatively, as shown in **Figure 1c**, the ZESI may act as an intermediate smart energy server, communicating with the UESI using two-way secure inter-PAN while using one-way secure inter-PAN to communicate with other HAN devices.

[0039] Clients of the UESI shall support the Commissioning and Registration states that comply with the OHP as described further herein. Generally, commissioning refers to the process by which a HAN device obtains access to a specific physical network and allows the device to be discovered on that network. The process may involve the exchange of information based on security credentials required to establish network coordination, assign device addresses, and to route packets. Admission to the network allows the HAN device to communicate with peer devices on a network and receive public information from the UESI, but not information reserved for Registered devices. Generally, registration refers to the process by which a commissioned HAN device is authorized to communicate on a logical network. This involves the exchange of information based on security credentials with a UESI. The registration process is required for the exchange of information based on security credentials between a registered device and the UESI and among other devices registered to that UESI.

[0040] **Figure 3** illustrates the three primary supported states of devices and the transition flows between states in accordance with certain embodiments described herein. A non-commissioned device does not operate on the HAN. In order to become commissioned, a pre-configured link key established during manufacture of the device is shared with the UESI **S10**. After commissioning, registration may be achieved with a shared link key which establishes authentication between the individual device and the UESI **S15**. More particularly, when powered-on in the commissioned state, the device automatically enters a state ready to accept registration commands from the UESI, which includes the shared link key, as part of the registration process. In reverse, the device becomes unregistered in the event of a timeout, e.g., due to shared link key updates that exclude the particular device **S20**. And de-commissioning occurs as a result of a predetermined de-commission procedure or device reset procedure **S25**. Once registered, a client device is capable of receiving smart energy (SE) Application messages from the UESI. A registered client device shall receive all SE Application messages, i.e., there is no selective registration required for published pricing or energy usage messages. Upon receiving an SE Application message, the client device will read the Destination MAC (D-MAC) Address. If the D-MAC Address is the client device's own MAC Address, the client device shall process the message with the Pre-configured Link key. If the D-MAC Address is the broadcast short MAC Address, the client device shall process the message with the Shared Link Key.

[0041] In accordance with a one-way broadcast model, in **Figure 5**, the UESI **5** (i.e., Inter-PAN server) receives messages from a Utility HES **25** that are directed to one or more HAN devices **15** (i.e., Inter-PAN client) and broadcasts the messages on multiple IEEE 802.15.4 channels. This is a point-to-multipoint communication. This approach eliminates the need for explicit channel management and allows the HAN devices to select the most appropriate channel based on their own proprietary selection algorithms. The specific 802.15.4 channels, on which the UESI transmits each message, depend on whether it is a registration message or an application message.

[0042] Two types of messages are supported: registration messages for client registration and network parameter updates, i.e., channel mask and PAN ID, and application messages including the publish price and energy usage messages, as well as text messages. Each registration message is sent on all 802.15.4 channels in order to sequentially reach all client devices, regardless of the channels on which the individual client devices are listening. This registration message includes a two byte channel mask field that informs the client devices about the channels on which the application messages will be sent. Each application message, i.e., publish price or energy usage message, is sequentially broadcast on all 802.15.4 channels identified by the channel mask field. The client device must listen to one or more of the identified channels. In certain embodiments, the UESI has the possibility to change its channel and PAN ID if the need arises in order to work with a specific AMI network. A change in its channel selection or PAN ID will result in registration messages including a new channel mask field and PAN ID for the devices. Messages are addressed to Inter-PAN clients based on a combination of the RF Channel Mask, Destination PAN ID, and 802.15.4 Destination Address fields. In a particular exemplary embodiment, an addressing strategy is summarized as set forth in **Table 2**.

Table 2

Message type	**RF Channel**	**Destination PAN-ID**	**Destination Address**
Registration	All	Client's default PAN ID which is the CRC16 of its MAC Address	Client's MAC Address
Application	As specified via the RF Channel Mask	Server's selected PAN ID	0xFFFF

[0026] Exemplary values for the different communication intervals are shown in **Table 3** below:

Table 3

Interval	Description	Value (minutes)
Client Registration timeout	Period during which a Commissioned client waits for an initial Registration message. After this time expires, the client may need to be triggered again (e.g., via a reset or pushbutton)	180
Registration message period	Period between Registration messages	60
Publish Price message period	Period between Publish Price messages	5-15
Energy Usage message period	Period between Energy Usage messages	1
Application message timeout	Period after which a Registered client stops waiting for Application messages and resets to the Commissioned State to hunt for Registration messages	30

[0027] The Physical layer is defined in section 6.5 (2450 MHz PHY specifications) of the IEEE 802.15.4-2006 standard, the specification of which is incorporated herein by reference. Tables contain the list of fields in their order of transmission; the first field listed is transmitted first. All multi-bytes fields are encoded Least Significant Byte first (LSB). The definition of each field is not provided in this document but can be found in the different documents referenced herein which are incorporated by reference in their entirety. **Table 4** is representative of physical layer parameters.

Table 4

Field names	Data type	Value
Preamble	4 bytes	
Start-of-Frame Delimiter (SFD)	1 byte	
Frame structure		See Data link layer defined below

[0028] The Data link layer is defined in section 7 (MAC sub-layer specification) of the IEEE 802.15.4-2006 standard. As indicated earlier, all messages are sent by the UESI and/or the ZESI in the particular embodiment wherein the ZESI is registered with the UESI as described

previously herein. Two frame types are defined: (1) Registration and (2) Application. Tables contain the list of fields in their order of transmission; the first field listed is transmitted first. All multi-bytes fields are encoded Least Significant Byte first (LSB). The definition of each field is not provided in this document but can be found in the different documents referenced herein which are incorporated by reference in their entirety. The frame format used by the Registration message is sent unicast to each client's MAC Address and default PAN ID which is the CRC16 of the client's MAC Address. **Table 5a** is representative of physical layer parameters.

Table 5a

Fields name	Data type	Value
Frame control	2 bytes	
Frame type	Bits 0 to 2	Data (001)
Security enabled	Bit 3	False (0)
Frame pending	Bit 4	False (0)
Ack. request	Bit 5	False (0)
Intra-PAN	Bit 6	False (0)
Dest. Addressing mode	Bits 10 to 11	Long address (11)
Source addressing mode	Bits 14 to 15	Long address (11)
Sequence number	1 byte	Unique identifier
Addressing fields		
Destination PAN identifier	2 bytes	Client's default PAN ID
Destination address	8 bytes	MAC address of the Inter-PAN client
Source PAN identifier	2 bytes	Pan ID of the Inter-PAN server
Source address	8 bytes	MAC address of the Inter-PAN server
Frame Payload		See Network layer defined below
MIC	4 bytes	Authenticator
FCS	2 bytes	Frame Check Sequence

[0029] **Table 5b** contains the list of fields in their order of transmission for the application layer message format for registration messages. The first field listed is transmitted first. All multi-bytes fields are encoded Least Significant Byte first (LSB).

Table 5b

Fields name	Data type	Description and value
ZigBee APS Header		

Fields name	Data type	Description and value
APS frame control	1 byte	
Frame type	Bits 0 to 1	Inter-PAN transmission (11)
Delivery Mode	Bits 2 to 3	Unicast (00)
Security	Bit 5	True (1)
ACK request	Bit 6	False (0)
Extended Header Present	Bit 7	False (0)
Cluster identifier	2 bytes	(0xfc00)
Profile identifier	2 bytes	ZigBee Smart Energy (0x0109)
Auxiliary Header		
Security control		
Security level	Bits 0 to 2	ENC-MIC-32 (101)
Key identifier	Bits 3 to 4	A data key(00)
Extended nonce	Bit 5	(0)
Frame counter	4 bytes	
ZCL header		
Frame control	1 byte	
Frame type	Bits 0 to 1	Command is specific to a cluster (01)
Manufacturer specific	Bit 2	True(1)
Direction	Bit 3	From the server(1)
Disable default response	Bit 4	True(1)
Manufacturer code	2 bytes	0x10C7 (Trilliant)
Transaction sequence number	1 byte	Unique ID generated by the Inter-PAN server
Command identifier	1 byte	0x00
ZCL payload		
PAN ID	2 bytes	PAN ID assigned to this Premise and used for Application messages
Channel Mask	2 byte bitmap	Bitmap representing IEEE 802.15.4 channel IDs (11 to 26) that the server will use for this Premise (LSB=11)
Shared Link key	16 bytes	AES-128 key assigned to this Premise and used for subsequent communications
Publish Price Message Period (seconds)	2 bytes	Interval between Publish Price messages, configured at the Server
Energy Usage Message Period (seconds)	2 bytes	Interval between Energy Usage messages, configured at the Server
Registration Message Period (seconds)	2 bytes	Interval between Registration messages, configured at the Server

[0030] This frame format is used for SE broadcast messages, i.e., Publish Price and Energy Usage Messages, which are sent from the Inter-PAN server to Inter-PAN clients. Tables contain the list of fields in their order of transmission; the first field listed is transmitted first. All multi-bytes fields are encoded Least Significant Byte first (LSB). The definition of each field is not provided in this document but can be found in the different documents referenced herein which are incorporated by reference in their entirety. **Table 6** is representative of application message parameters.

Table 6

Fields name	**Data type**	**Value**
Frame control	2 bytes	
Frame type	Bits 0 to 2	Data (001)
Security enabled	Bit 3	False (0)
Frame pending	Bit 4	False (0)
Ack. request	Bit 5	False (0)
Intra-PAN	Bit 6	False (0)
Dest. Addressing mode	Bits 10 to 11	Short address (10)
Source addressing mode	Bits 14 to 15	Long address (11)
Sequence number	1 byte	Unique identifier
Addressing fields		
Destination PAN identifier	2 bytes	PAN ID assigned to this Premise and used for subsequent application messages
Destination address	2 bytes	Broadcast address (0xFFFF)
Source PAN identifier	2 bytes	Pan ID of the Inter-PAN server
Source address	8 bytes	MAC address of the Inter-PAN server
Frame Payload		See Network layer defined bellow
MIC	4 bytes	Authenticator
FCS	2 bytes	Frame Check Sequence

[0031] The Network layer is defined in Annex B.4 (Frame Formats) of the ZigBee Smart Energy Profile version 1.0 revision 15 which is incorporated herein by reference it its entirety. The complete descriptions of each field contained in the list below can also be found in section 3.3.1 (General NPDU Frame Format) of the ZigBee Specification (053474r17). Tables contain the list of fields in their order of transmission; the first field listed is transmitted first. All multi-

bytes fields are encoded Least Significant Byte first (LSB). The definition of each field is not provided in this document but can be found in the different documents referenced herein which are incorporated by reference in their entirety. **Table 7** is representative of network layer parameters.

Table 7

Fields name	**Data type**	**Value**
NWK frame control	2 bytes	(0x0b00)
Frame type	Bits 0 to 1	Inter-PAN transmission (11)
Protocol version	Bits 2 to 5	2 (0010)
Application Payload		See Application layer defined bellow

[0032] The UESI supports a variety of HAN devices, including battery-supported 'sleepy' devices. Sleepy devices are not always available to receive registration messages. When a non-commissioned sleepy device first starts up, it shall stay awake until it hears the registration message addressed to it (it may time-out after a reasonable long timeout period). The registration message provides three parameters that inform the client of message periodicities; allowing it to synchronize its wake cycles: registration message period, publish price message period, and energy usage message period. Typical values are shown in **Table 4** above.

[0033] The security of the UESI is based on two types of Link Keys: one pre-configured Link Key to secure individual Registration messages, and a shared Link Key to secure broadcast Application messages. The shared Link Key is distributed via the Registration message.

[0034] The security model utilizes features from ZSE 1.0 security, while simplifying the model as appropriate to achieve originator-authenticated communication as required by OHP. A comparison to the full ZSE 1.0 security is shown in the **Table 8**.

[0035] The Registration process establishes the authentication and security between the UESI and the device.

Table 8

	Prior Art ZigBee SEP 1.0 CBKE	**Present Embodiments Secure ZigBee SEP 1.0 Inter-PAN**
Authentication	Mutual authentication	Sender authentication
Key Establishment	OOB Pre-Configured Link Key Process; CBKE	OOB Pre-Configured Link Key Process

	Prior Art **ZigBee SEP 1.0 CBKE**	**Present Embodiments** **Secure ZigBee SEP 1.0 Inter-PAN**
Encryption	CCM* / AES-128	CCM* / AES-128
Security Layers	Network Layer security via a shared Network Key	n/a
	Application Layer Security via Application Link Keys: • One Trust Center link key per ZigBee client • Multiple application link keys between application pairs	Application Layer Security via Application Link Keys: • One Pre-configured Link key per ZigBee client • One Shared Link Key per UESI server
Key updates	Supported	Supported
Temporary Link key to secure initial Link key distribution	MMO of ZigBee client's Installation Code	MMO of ZigBee client's Installation Code
Key to secure subsequent key updates	Network Key + Trust Center Link Key	MMO of ZigBee client's Installation Code

[0036] The process of establishing security keys uses the out-of-band (OOB) pre-configured Link Key process and is summarized as follows (see also **Figure 7**). Initially, the HAN device is pre-commissioned. During the manufacturing process, a random Installation Code is created for each HAN device. This Installation Code is provided for the device (e.g., as a label on the packaging of the HAN device and/or configured into the device) to be referenced to during Commissioning and Registration of the HAN device to the UESI. The HAN device looks up the 'Pre-configured Link Key', or derives it using the MMO hashing function. During installation, the installer provides the Installation Code and MAC Address to the Utility's HES. These are then forwarded to the UESI, where they are stored. The UESI calculates the Pre-configured Link key as needed from the Installation Code and uses it to protect the distribution of the Shared Link Key to the associating HAN device. The Shared Link Key is in turn used to secure the distribution of network-wide application messages. Periodically, the UESI shall update the Shared Link Key by distributing a new one to registered HAN devices. All HAN devices receiving the key update (i.e., in the Commissioned state) will start using the new key immediately to process Application messages. Notice that this mechanism is also used to de-

register HAN devices if needed, by only updating the key of the remaining registered HAN devices.

[0037] The registration process establishes an association between an Inter-PAN server (UESI) and an Inter-PAN client, i.e., HAN device. Registration messages are used to: Commission and Register a HAN device to the UESI; De-Register a HAN device from a UESI; and update network parameters on the HAN device. The Registration message is sent by the UESI to each registered device's MAC Address, on all the IEEE 802.15.4 channels. The Registration process distributes the Shared Link Key (used by the UESI to encrypt Application messages), the PAN ID, and the Channel Mask. The HAN device, upon reception of a Registration message, shall immediately update its PAN ID, Channel Mask, and the Shared Link Key contained in the Registration message to process subsequent Application messages.

[0038] **Figure 6** illustrates a state diagram showing the transitions between Commissioned and Registered states for an Inter-PAN client (see also **Figure 7**). The triggers for state transition are described below: Power On / Reset - Initial transition after a power on or reset event **S15**; Registration timeout - upper limit to period of time without receiving a Registration message **S20**; Reception of a Registration message addressed to this client, and secured using its own pre-configured Link Key **S30**; Reception of Application message **S35**; Communication timeout - upper limit to period of time for which the Communicating indication is provided **S40**; Inactivity timeout - upper limit to short period of time without receiving an Application message **S45**; Application message timeout - upper limit to long period of time without receiving an Application message **S50**. Depending on its state, a client device can process either only Registration messages (in Commissioned state), or only Application messages (Registered state).

[0039] In an exemplary embodiment, Inter-PAN devices provide an indication of current state so that the end user of the device has an understanding of the state of the client device. For example, an LED indicator could be used during the Registration process to verify the status of the operation, and during the normal life of the device to verify the health of its communications. **Table 9** provides exemplary indicator parameters.

Table 9

State	Meaning	Exemplary LED indication	Explanation
Non-Commissioned	The device has not been Commissioned	n/a	A device cannot join the UESI until it is Commissioned with its pre-configured Link Key or Installation code.
Commissioned	The device has been Commissioned but is not Registering	n/a	The device needs to be triggered (e.g., powered-on) to start its Registration process
Commissioned and Registering	A device in the Commissioned state and listening for Registration messages	Slow (1000ms) red LED or equivalent	Refer to the OOB registration process
Registered & Active	A device is in the Registered state and receiving messages	Medium (500ms) green LED or equivalent	In OHP, a Registered device is by definition also Commissioned.
Registered & Communicating	A device is in the Registered state that is actively receiving a message	Fast (250ms) green LED or equivalent	In OHP, a Registered device is by definition also Commissioned.
Registered & Inactive	A device is in the Registered state that is not receiving messages	Fast (250ms) red LED or equivalent	This could indicate that e.g., the RF signal is weak, or that the device is de-registered

[0040] The initial registration message is authenticated using the device-specific encryption key derived from the installation code using the MMO hash function, as indicated by the Key Identifier field present at the data link, and is processed only by the owner of this key. This message flow is shown in **Figure 7a**. The Registration process flow includes the following steps: the HAN device **15** automatically enters a state ready to accept Registration commands from the Inter-PAN server (i.e., UESI) **5** when it is first powered-on (e.g. the Installer **20** plugs in an Inter-PAN client, e.g., IHD, into the wall socket for the first time). The Installation Code and MAC Address are provided by OOB methods to the Utility HES **25, S5** (e.g. using an Internet

consumer portal or a Call Center). The Installation Code is defined in section "5.4.8.1 Out of Band Pre-Configured Link Key Process" of the SEP Document. More specifically, during manufacturing, each client may provide a random Installation Code (unique per device for each vendor). This code is configured into the device, either as-is or through its MMO Hash, depending on the capabilities of the device, which will be required to (calculate and) use the MMO Hash to decrypt and authenticate registration messages directed to it as described herein. Additionally, the Installation Code is also provided, e.g., as a label on the packaging of each client device to facilitate the Registration process, where this code is presented out-of-band to the management tools that support provisioning it to the meter. The meter uses the stored Installation Codes to on-the-fly calculate the Pre-configured Link keys that are required to encrypt its Registration messages to specific clients.

[0041] The Utility HES first configures the Shared Link Key into the UESI (not shown). For each HAN device that is Registered, the Utility HES must also send the MAC Address and MMO Hash of the Installation Code to the UESI (not shown); alternatively the HES can send the Installation Code to the UESI where the MMO Hash is calculated **S60**. For each HAN device the UESI encrypts a Registration message using each client's MMO Hash, and then transmits it to the clients MAC Address and clients default PAN-ID, on all IEEE 802.15.4 channels **S65**. The Inter-PAN client locates the preconfigured link key that was pre-installed during manufacturing or calculates it via the MMO hash of its own Installation Code and uses that to decrypt the Registration message **S70**. Only the associated client that is able to authenticate and decrypt the received Registration message can receive the Shared Link key which is required to process Application messages.

[0042] Upon successful decryption of the Registration message, the Inter-PAN client immediately sets the PAN ID using the value specified in the Registration message. Pursuant to **Table 9**, an indicator may be set so that a user (e.g. homeowner or installer) knows that the device is registered **S75**. Then, the Inter-PAN client uses the Channel Mask field provided by the Inter-PAN server to select an available channel to receive its messages. This field represents a bitmap of channels that the server will broadcast SE Information messages on. The Inter-PAN client must use one of the enabled channels listed in the Channel Mask field. The Channel Mask field is a bit field of 15 bits where the least significant bit represents the channel 11. For example, if the Channel Mask value is represented in hexadecimal by the value 0x20D8 or in

binary by the value 0010 0000 1101 1000, then the following channels are safe to listen on: 14, 15, 17, 18 and 24. Further to channel selection processes, in a particular embodiments, a UESI may have the ability to calculate the optimal Channel Mask field and PAN ID which will be provided to the Inter-PAN clients along with the Shared Link key to be used for Application messages. The optimal Channel Mask field excludes all channels which should not be used by the UESI's communications and thus indicates to the Inter-PAN clients which channels they should not listen on.

[0043] Since the one-way communication model does not allow for acknowledgement or confirmation of receipt of transmitted messages, if a listening device misses a message, the embodiments described herein do not provide a mechanism for the UESI to track the success of each transmission and resend messages as needed. As described herein, when a device is unable to hear Application messages for a preconfigured period, it times-out and returns to its Commissioned & Registering state, ready to accept Registration messages from the Inter-PAN server. Registration messages are periodically transmitted at intervals as configured in the UESI. With this mechanism in place, a client that misses an update is able to re-sync, simply by listening to the next available Registration message. Registration messages also include three parameters that inform the clients of message transmission periods set by the server: Publish Price Message Period, Energy Usage Message Period, and Registration Message Period. These parameters can be used by a client for optimization purposes, e.g., a sleepy client can be programmed to synchronize its wake times with these periods.

[0044] Alternatively, in a specific implementation, UESI supports a configurable time period parameter for Registration messages, wherein a user at the HES can modify the broadcast time period parameter of the UESI, and then use the AMI network to send the update to the UESI. Further still, an on-demand feature may be provided through the HES to invoke an asynchronous Registration message. The HES user interface supports a button for each registered device to immediately invoke a Registration message to that device. This is in addition to the configurable periodic broadcast of the Registration messages. This on-demand feature is integrated to facilitate installation and troubleshooting of a device.

[0045] **Figure 8** illustrates the repetitive, point-to-multipoint nature of the transmission of Registration messages in accordance with certain embodiments described herein. As shown, the Inter-PAN server **10** transmits N individual registration messages encrypted using device

PLKs (MMO hash of each Installation Code), e.g., PLK1, PLK2, … PLKN at a first time on channels X, Y, Z. Each of the individual Inter-PAN devices (**15a, 15b, … 15n**) is listening on a Channel X, Y, Z. Pursuant to a pre-established iterative period set, the Inter-PAN server, i.e., UESI **10**, repeats this transmission every 60 minutes (1 hour). The Registration messages facilitate transmission of changes to the RF Channels and PAN ID as they may need to be changed; the Shared Link Key remains the same.

[0046] Periodic repetition of registration messages works to avoid the need for out-of-band re-registration, should a device miss a critical update. Per **Figure 8**, messages are transmitted on all channels, repeated over a preconfigured interval for each registered node, and secured via their respective pre-configured Link keys (i.e., MMO hash of pre-configured Installation codes). Whenever re-registration is required, the UESI will immediately send the new Registration messages, thereby restarting the inter-message intervals, repeating the new values until new changes are needed. From a device perspective, whenever it gets out of sync with these parameters, it times out and waits for the next Registration message protected with its own encryption key derived from the Installation code using MMO hash function. In order to de-register a device, the server does the following: sends a Registration message with Shared Link key = 0x0000 (all zeros) to that device, causing it to reset its registration state (optional step); sends an updated Shared Link key to the remaining clients; removes the pre-configured Link key of the de-registered client from its registration table.

[0047] Once registered, a client device is capable of receiving smart energy (SE) Application messages transmitted from the UESI on selected channels. A registered client device shall receive all SE Application messages, i.e., there is no selective registration required for published pricing or energy usage messages. Upon receiving an SE Application message, the client device will read the Destination MAC (D-MAC) Address. If the D-MAC Address is the client device's own MAC Address, the client device shall process the message with the devices PLK. If the D-MAC Address is the broadcast short MAC Address, the client device shall process the message with the SLK.

[0048] Using the systems and processes described herein, the UESI may send at least the following information to all Inter-PAN clients: Electricity price using the Publish Price Command in the Price Cluster and Energy usage using the Simple Metering Cluster server attributes.

[0049] Referring to **Figure 9**, the registration and subsequent communication processes and intervals pursuant to an exemplary embodiment wherein the UESI **10** is part of the utility meter as shown. In this example, target device (Inter-PAN devices) **15a** is not yet available to receive registration messages, target devices **15b** are available to receive registration messages (R) and target devices **15c** are registered and available to receive published price (P) and energy (E) application messages. The time (T) is indicated and an exemplary table of time intervals is also shown representing the interval between clusters of Registration messages.

[0050] In an alternative approach to support a registration, the UESI sends the registration messages on a single, e.g., channel X (or a few) channel(s) as compared to all, and the registering clients scan all or a subset of channels for registration messages sent to their own MAC addresses. Once a client finds such a registration message it retrieves the SLK and Channel mask, and the process proceeds as described. A benefit of this approach is that is can significantly reduce the traffic associated with registration messages (e.g., down to 1/16) that are periodically repeated. (See **Figure 7b**).

[0051] Further still, in another alternative embodiment, all communications (i.e., both registration and application messages) are supported on the same channel and the channel mask is not needed. When a UESI needs to change channels, the UESI starts using the new channel. The clients eventually time out when they stop receiving messages on the original channel and start scanning again, hunting for their registration messages. (See **Figure 7b**).

[0052] While descriptions above detail a process for distributing a single SLK, in an alternative embodiment, multiple SLKs could be used to extend to multiple groups of target devices to confidentially send different smart energy information to devices within a premise. For example, referring to **Figure 10**, two sets of target devices on a single HAN can be addressed individually and receive different sets of energy information by the UESI **10** in accordance with different SLKs and/or different PAN IDs. In this example, **SET 1** includes the refrigerator **15a** and thermostat **15b** and is established for energy data push from the UESI **10** using either SLK1 or PAN ID1, whereas **SET 2** includes the wash machine **15c** and server **15d** and is established for energy data push from the UESI **10** using either SLK2 or PAN ID2.

[0053] Referring to **Figure 1c**, an alternative embodiment to the one-way communication system describer with respect to the **Figure 1b** is shown. In **Figure 1b**, the UESI **10** provides

secure smart energy information to a registered target device **15**, indirectly via an intermediate energy information server IEIS **12** (e.g., a full function HAN device). The UESI **10** communicates with the IEIS **12** via a secure two-way HAN and provisions it to communicate with the target device **15** on its behalf. Using two-way secure Inter-PAN, the HAN device requests data from a meter by first contacting the meter via a beacon request. Once it locates the meter, it then requests data via an Inter-PAN message, which is then provided by the meter in response. The benefit of this architecture is that it provides extended coverage via the HAN, as Inter-PAN is limited to a single hop. The IEIS **12** thus extends the reach of the UESI **10** and provides a secure way of distributing smart energy information to one-way target devices.

[0054] The embodiments described to this point have generally been directed to one-way secure communications or combinations of one-way and two-way secure communications. **Figures 1d** and **1e** illustrate systems wherein secure two-way communications are implemented. More particularly, as shown in **Figure 1d**, a smart energy device **15**, e.g., IHD or meter, communicates wirelessly with a field tool using secure two-way Inter-PAN, e.g., ZigBee. In this configuration, the Field Tool **25** is able to ascertain information from the smart energy device **15** to determine the need for and initiate operation, maintenance and configuration interactions as needed.

[0055] Referring to **Figure 1e**, the underlying communications from Field Tool **25** to an UESI **10** are two-way secured Inter-PAN, but the data flow from the UESI **10** to the HAN device **15** is one-way. The field tool first establishes a secure two-way Inter-PAN connection with the UESI which serves as a proxy, and in turn establishes a secure connection with the Smart Energy device via standard ZigBee security procedures.

[0056] The ability to add a Field Tool in an ad hoc fashion using the processes described herein avoids the requirement that the Field Tool actually join the HAN in order to communicate with a target device. This process can be expanded to other ad hoc device such as smart phones which can use the processes to communicate with the target devices.

[0057] In accordance with the embodiments described above, there are both one-way and two-way processes for securing Inter-PAN communications. While these processes have underlying similarities, there are differences. The steps of the one-way process are generally outlined in **Figure 4a** which is described above. The steps of the two-way process are generally

outlined in **Figure 4b**. In both scenarios, there is an authentication phase followed by a phase where both parties arrive at an SLK, which is then used to encrypt communications during the authorized session, and is valid until it times out. More particularly, for two-way Inter-PAN, mutual authentication is achieved via the Certificate Based Key Exchange (CBKE) **S105** process as described in the SEP Document incorporated herein by reference**.** After mutual authentication and exchange of ephemeral data, both parties derive a shared link key **S110**, the server verifies the client's MAC address versus a trusted list **S115** and the SLK is used by both client and server to encrypt each message **S120.** A prior art CBKE flow is illustrated in **Figure 11**.

[0058] As shown in **Figures 1b-1e**, the secure Inter-PAN communications are utilized as part of a larger system. Referring to **Figure 12**, in a specific example, the UESI **10** is hosted on an existing meter **30** at a customer location which communicates with the HES **5** through the NAN. This infrastructure enables secure over-the-air remote registration and key management via the HES, as well as locally from the field using radio-enabled communications with the meter (e.g., via USB adapter connected to field operator laptop **20**). More specifically, the HES supports a Web Services API to accept Installation Codes and MAC Addresses, one pair for each target client's registration (multiple per meter). The Installation Codes and MAC Addresses are stored at the HES and configured in the meters which use these to on-the-fly calculate the individual Pre-configured Link Keys to encrypt Inter-PAN Registration messages and forward them to targets using their individual MAC Addresses. The HES allows for the generation, storage, and distribution of SLKs (generally one per meter, but multiple possible in accordance with **Figure 10**). Keys are distributed over-the-air via the NAN. Additionally, the field computer **20** also supports the capability to accept an entered Installation Code and MAC Address and write it to the meter. Such configurations are synchronized with the HES, when it is part of the deployment.

[0059] The present embodiments support as an application message, the Publish Price message in the SEP Documents incorporated herein by reference. **Table 10** is an exemplary application message format for Publish Price messages. Fields are listed in their order of transmission; the first field listed is transmitted first. All multi-bytes fields are encoded Least Significant Byte first (LSB).

Table 10

Fields name	Data type	Description and value
ZigBee APS Header		
APS frame control	1 byte	
Frame type	Bits 0 to 1	Inter-PAN (11)
Delivery Mode	Bits 2 to 3	Unicast (00)
Security	Bit 5	True (1)
ACK request	Bit 6	False (0)
Extended Header Present	Bit 7	False (0)
Cluster identifier	2 bytes	Price (0x0700)
Profile identifier	2 bytes	ZigBee Smart Energy (0x0109)
Auxiliary Header		
Security control		
Security level	Bits 0 to 2	ENC-MIC-32 (101)
Key identifier	Bits 3 to 4	A data key(00)
Extended nonce	Bit 5	(0)
Frame counter	4 bytes	
ZCL header		
Frame control	1 byte	
Frame type	Bits 0 to 1	Command is specific to a cluster (01)
Manufacturer specific	Bit 2	False(0)
Direction	Bit 3	From the server(1)
Disable default response	Bit 4	True(1)
Transaction sequence number	1 byte	Unique ID generated by the Inter-PAN server
Command identifier	1 byte	Identify (0x00)
ZCL payload		
Provider ID	Unsigned 32 bit Integer	
Rate Label	Octet String	
Issuer Event ID	Unsigned 32 bit Integer	
Current Time	UTC Time	
Unit of Measure	8 bits enumeration	
Currency	Unsigned 16 bit Integer	
	8 bit BitMap	
Price Trailing Digit		
Price Tier		
	8 bit BitMap	
Number of Price Tiers		
Register Tier		
Start Time	UTC Time	
Duration In Minutes	Unsigned 16 bit Integer	
Price	Unsigned 32 bit Integer	
Price Ratio	Unsigned 8 bit Integer	

Fields name	Data type	Description and value
Generation Price	Unsigned 32 bit Integer	
Generation Price Ratio	Unsigned 8 bit Integer	
Alternate Cost Delivered	Unsigned 32 bit Integer	
Alternate Cost Unit	8 bits enumeration	
• Alternate Cost Trailing Digit	8 bit BitMap	

[0060] The UESI supports time-of-use (TOU) rates and critical peak pricing events (CPP). It may receive information for Publish Price messages from the Utility HES, or possibly generate the messages using locally configured parameters. The UESI transmits price messages per the ZigBee Smart Energy Profile guidelines for the Publish Price Command when an update to the pricing information is available from the commodity (e.g., gas, electricity, water) provider. The UESI transmits price messages in pairs: the current price and then the next price. In the case of the Publish Price message related to the current price, the fields CURRENT TIME and START TIME are identical. In the case of the Publish Price message related to the next price, the field CURRENT TIME will be before the field START TIME. The UESI meter may have a real-time clock and use the UTC time shared across the AMI network to populate the field CURRENT TIME of the Publish Price message. The UTC time shared across the AMI network is provided by an NTP server via the HES. It is possible for HAN devices to approximately synchronize time with the UESI meter using the CURRENT TIME message field. The UESI transmits the price message as a broadcast addressed message on the IEEE 802.15.4 channels specified in the Channel Mask field (see **Figure 8**).

[0061] Since this UESI is based on a one-way model, there is a probability that a listening client may occasionally not successfully receive the price messages (since there is no mechanism to request retransmissions). Missing a Publish Price message update could potentially let a device use out of date price information for long periods of time. The UESI may therefore optionally transmit Publish Price messages periodically between changes in the price from when an update to the pricing information is available from the commodity provider. With this mechanism in place, a client that misses an update is able to re-synchronize, simply by listening to the subsequent periodic price message transmissions. As discussed above, in a specific implementation, the UESI supports a configurable time period parameter for price messages. The HES user interface allows the utility operator to modify the broadcast time period

parameter of the UESI meter, and then use the AMI network to send the update to the UESI meter. The default time period parameter may be predetermined, e.g., 10 minutes.

[0062] The embodiments described herein assume that the HAN devices are able to manage Publish Price messages. In addition to requirements set forth in the SEP Document which is incorporated herein by reference, the embodiments require the HAN devices handle two instances of Publish Price messages. As described above, the first instance is related to current price and the second instance is related to next price. This approach gives more robustness to the system in the case the HAN device is missing a price update. In that case, the client must apply the next price at the appropriated time. Additionally, as described, the Publish Price message related to current price can be used to perform time synchronization, the HAN device needs to be able to handle the UTC to local time conversion.

[0063] The systems and processes described herein depict a mechanism for providing utility usage information. An exemplary message format for a meter cluster application message prepared by the UESI for an Inter-PAN device is illustrated in **Table 11**.

Table 11

Fields name	**Data type**	**Description and value**
ZigBee APS Header		
APS frame control	1 byte	
Frame type	Bits 0 to 1	Inter-PAN (11)
Delivery Mode	Bits 2 to 3	Unicast (00)
Security	Bit 5	True (1)
ACK request	Bit 6	False (0)
Extended Header Present	Bit 7	False (0)
Cluster identifier	2 bytes	Simple Metering (0x0702)
Profile identifier	2 bytes	ZigBee Smart Energy (0x0109)
Auxiliary Header		
Security control		
Security level	Bits 0 to 2	ENC-MIC-32 (101)
Key identifier	Bits 3 to 4	A data key(00)
Extended nonce	Bit 5	(0)
Frame counter	4 bytes	
ZCL header		
Frame control	1 byte	
Frame type	Bits 0 to 1	Command acts across the entire profile (00)

Fields name	Data type	Description and value
Manufacturer specific	Bit 2	False(0)
Direction	Bit 3	From the server(1)
Disable default response	Bit 4	True(1)
Transaction sequence number	1 byte	Unique ID generated by the Inter-PAN server
Command identifier	1 byte	Report attributes (0x0a)
ZCL payload		
CurrentSummationDelivered		
Attribute identifier	2 bytes	0x0000
Attribute data type	1 byte	Unsigned 48 bit Integer (0x25)
Attribute data	6 bytes	
InstantaneousDemand		
Attribute identifier	2 bytes	0x0400
Attribute data type	1 byte	Signed 24 bit Integer (0x2A)
Attribute data	3 bytes	
CurrentDayConsumptionDelivered		
Attribute identifier	2 bytes	0x0401
Attribute data type	1 byte	Unsigned 24 bit Integer (0x22)
Attribute data	3 bytes	
PreviousDayConsumptionDelivered		
Attribute identifier	2 bytes	0x0403
Attribute data type	1 byte	Unsigned 24 bit Integer (0x22)
Attribute data	3 bytes	
UnitofMeasure		
Attribute identifier	2 bytes	0x0300
Attribute data type	1 byte	8-bit Enumeration (0x30)
Attribute data	1 byte	
Multiplier		
Attribute identifier	2 bytes	0x0301
Attribute data type	1 byte	Unsigned 24 bit Integer (0x22)
Attribute data	3 bytes	
Divisor		
Attribute identifier	2 bytes	0x0302
Attribute data type	1 byte	Unsigned 24 bit Integer (0x22)
Attribute data	3 bytes	
SummationFormatting		

Fields name	Data type	Description and value
Attribute identifier	2 bytes	0x0303
Attribute data type	1 byte	8 bit BitMap (0x18)
Attribute data	1 byte	
DemandFormatting		
Attribute identifier	2 bytes	0x0304
Attribute data type	1 byte	8 bit BitMap (0x18)
Attribute data	1 byte	
HistoricalConsumptionFormatting		
Attribute identifier	2 bytes	0x0305
Attribute data type	1 byte	8 bit BitMap (0x18)
Attribute data	1 byte	

[0064] The UESI uses the local meter data to generate the energy usage message. The UESI follows the Simple Metering server cluster guidelines as set forth in the SEP Document which is incorporated herein by reference. The UESI periodically transmits the energy usage message. A UESI may support a configurable time period. Once the end of the time period is met, the UESI generates and transmits an energy usage message, e.g., every 60 seconds. The UESI transmits the energy usage message as a broadcast addressed message on the IEEE 802.15.4 channels specified in the Channel Mask field.

[0065] The systems and methods described herein support "silent" joining via a commissioning or pre-provisioned method. All data required to enter the network is already provided to the node, i.e., client device, so that no joining procedure itself is required. A client device thus creates its own network and joins it. The client can enter the commissioning & registering state by using the silent join mode with default network and security parameters, and join the network as a router device. By way of example, the relevant default values are shown in **Table 12** below:

Table 12

Parameter	Value	Comment
Startup Control	0x00	0x00 means that the node will 'silently join' with the commissioned settings
PAN ID	CRC16 of its own MAC Address	This value will be overwritten based on the PAN ID received in the Registration message

Channel	Randomly selected by the application	This value may be overwritten based on the Channel mask received in the Registration message
Pre-configured Link key	MMO Hash of the configured Installation Code	

[0066] The client then listens for a Registration message on the selected channel that is (1) sent to its own MAC address and default PAN ID, and (2) can be successfully processed with its own Pre-configured Link key. When it successfully decrypts this message, the client saves the server's MAC Address, and updates the PAN ID, channel mask, and Shared Link key, accordingly. At this point the client is capable of receiving and decrypting application messages.

[0067] Notice that if two clients end up on the same channel (with the same PAN ID), even though a PAN ID conflict is detected, it is not resolved because clients are not Coordinators and only the Coordinator (which is the Network Manager as well) can change the PAN ID of the network. (The client device will attempt to send a conflict report to the Coordinator, but because there is no Coordinator node nothing happens). Accordingly, multiple clients can co-exist on the same channel with the same PAN ID.

[0068] The embodiments described herein are intended to be exemplary. One skilled in the art will recognize variations thereof that are clearly with the scope of the embodiments described.

CLAIMS

1. A communications module for facilitating secure communications on a first network and a second network comprising:

a single transceiver for receiving and transmitting first network messages from and to the first network and at least transmitting second network messages to the second network;

at least a first processor connected to the single transceiver for processing one or more first network messages and second network messages;

the at least a first processor including first network logic for processing first network messages and second network logic for processing second network messages; and

the second network logic including instructions for securing second network messages such that decryption of the second network messages is limited to a particular receiving device on the second network.

2. The communications module of Claim 1, further comprising a second processor connected to the single transceiver, wherein the first network logic is included on the first processor and the second network logic is included on the second processor.

3. The communications module of Claim 1, wherein the second network logic includes instructions received by the single transceiver from one or more first network messages indicating a set of communication channels on which the single transceiver is to transmit the second network messages.

4. The communications module of Claim 3, wherein the instructions received by the single transceiver from one or more first network messages further include information that is unique to the particular receiving device.

5. The communications module of Claim 4, wherein the information that is unique to the particular receiving device is generated based on identification data from the particular receiving device that is transmitted and received by a head end system location outside of both the first network and the second network.

6. The communications module of Claim 5, wherein the second network messages include two types of messages, registration messages and application messages.

7. The communications module of Claim 6, wherein each registration message transmitted by the single transceiver on the second network is encrypted with a pre-configured key based on

the information that is unique to a particular receiving device and is unicast by the single transceiver on the set of communication channels.

8. The communications module of Claim 7, wherein when the particular receiving device decrypts a registration message, it reads a shared link key.

9. The communications module of Claim 8, wherein each application message transmitted by the single transceiver on the second network is encrypted with the shared link key and is broadcast by the single transceiver to a subset of the set of communication channels.

10. The communications module of Claim 1, wherein the first network is a wide area network and the second network is a home area network, the home area network being unique to a consumer.

11. A process for registering a device located on a home area network with a communications module to facilitate receipt at the device of messages from the communications module that originated outside of the home area network comprising:

receiving a device registration key that is unique to the device at a head end system that is not on the home area network;

receiving at the communications module the device registration key from the head end system;

transmitting by the communications module a registration message encrypted with a version of the device registration key on multiple communication channels;

listening by the device for registration messages on a particular communication channel within the multiple communication channels; and

upon receiving on the particular communication channel the registration message encrypted with the device's registration key, decrypting the registration message to retrieve a shared link key for decrypting application messages from the communications module.

12. The process of Claim 11, wherein the application messages contain at least one of utility consumption information that is specific to one or more consumers associated with the home area network, utility pricing information that is specific to one or more consumers associated with the home area network, and text messages from a utility provider to one or more consumers associated with the home area network.

13. The process of Claim 11, wherein the device registration key is an installation code that is physically and/or electronically associated with the device during manufacture thereof.

14. The process of Claim 13, wherein the version of the device registration key is an MMO hash of the installation code.

15. The process of Claim 11, wherein the communications module also receives MAC address information for the device from the head end system.

16. The process of Claim 11, wherein the communications module transmits the registration message encrypted with a version of the device registration key on multiple communication channels at predetermined time intervals.

17. The process of Claim 12, wherein the communications module transmits the application messages at predetermined time intervals.

18. A process for registering multiple devices located on a home area network with a communications module to facilitate receipt at the multiple devices of messages from the communications module that originated outside of the home area network comprising:

receiving a unique device registration key for each of the multiple devices at a head end system that is not on the home area network;

receiving at the communications module each of the unique device registration keys from the head end system;

transmitting by the communications module on multiple communication channels individual registration messages each encrypted with a version of one the multiple device registration keys;

listening by each of the multiple devices for registration messages on a particular communication channel within the multiple communication channels;

upon receiving on the particular communication channel the registration message encrypted with an individual of the multiple device's registration key, decrypting the registration message to retrieve one of a first or second shared link key for decrypting application messages encrypted with one of the first or second shared link keys from the communications module;

wherein each of the multiple devices on the home area network receives either the first or the second shared link key, but not both.

19. The process of Claim 18, wherein the application messages contain at least one of utility consumption information that is specific to one or more consumers associated with the home area network, utility pricing information that is specific to one or more consumers associated

with the home area network, and text messages from a utility provider to one or more consumers associated with the home area network.

20. The process of Claim 18, wherein the unique device registration keys are installation codes that are physically and/or electronically associated with the devices during manufacture thereof.

21. The process of Claim 20, wherein the version of the device registration key is an MMO hash of the installation code.

22. The process of Claim 18, wherein the communications module also receives MAC address information for the each of the multiple devices from the head end system.

23. The process of Claim 18, wherein the communications module transmits the registration messages encrypted with a version of the unique device registration keys on multiple communication channels at predetermined time intervals.

24. The process of Claim 19, wherein the communications module transmits the application messages at predetermined time intervals.

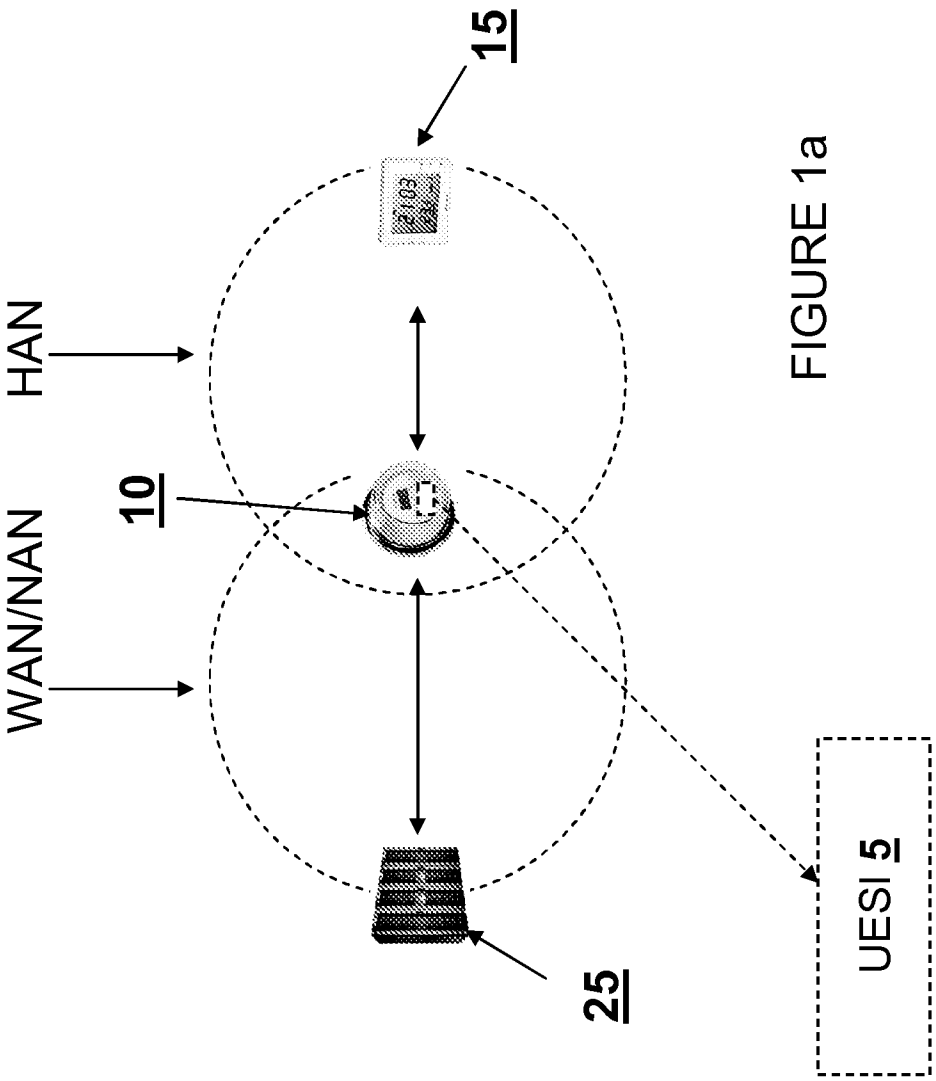


FIGURE 1a

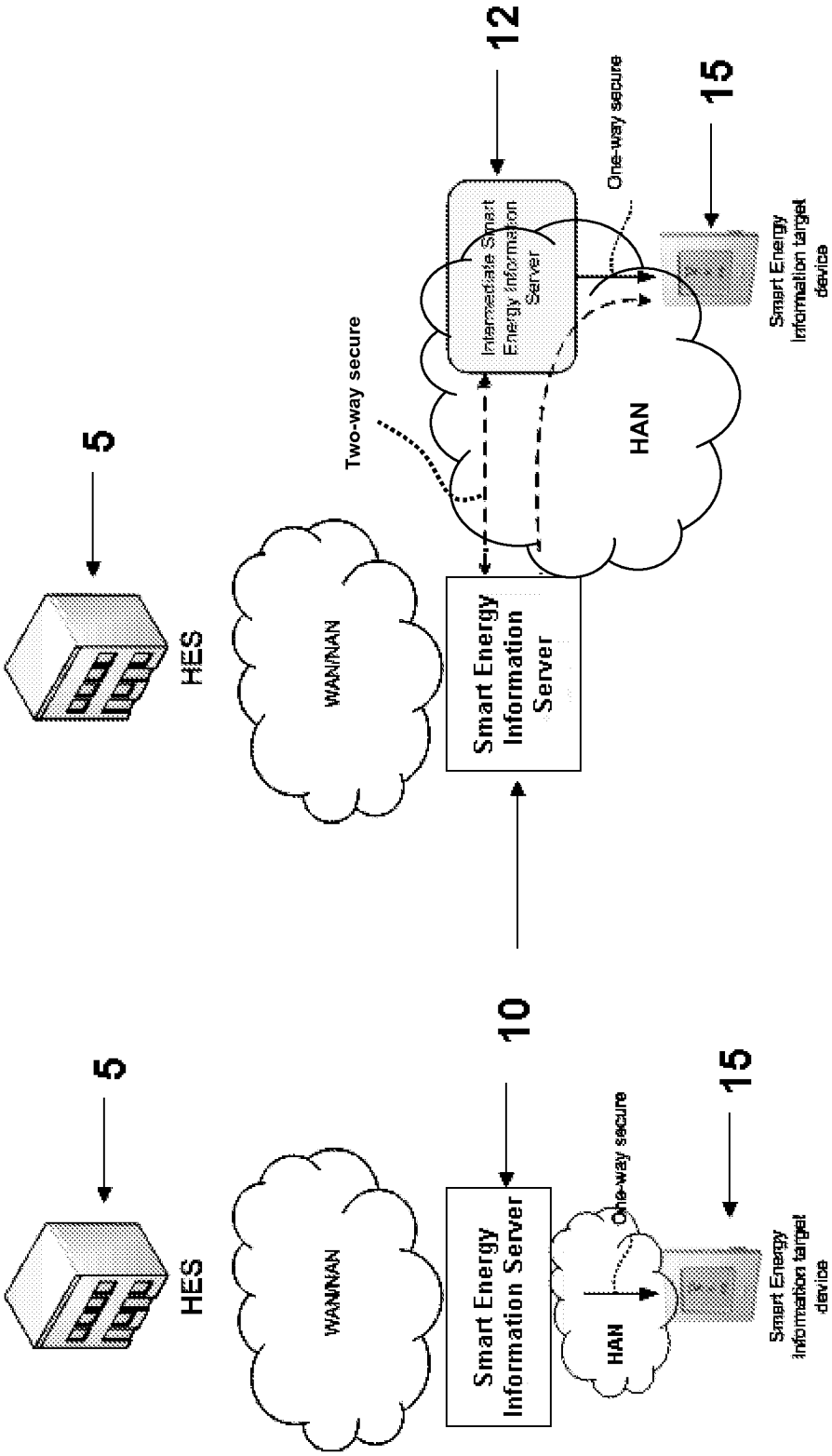


FIGURE 1b

FIGURE 1c

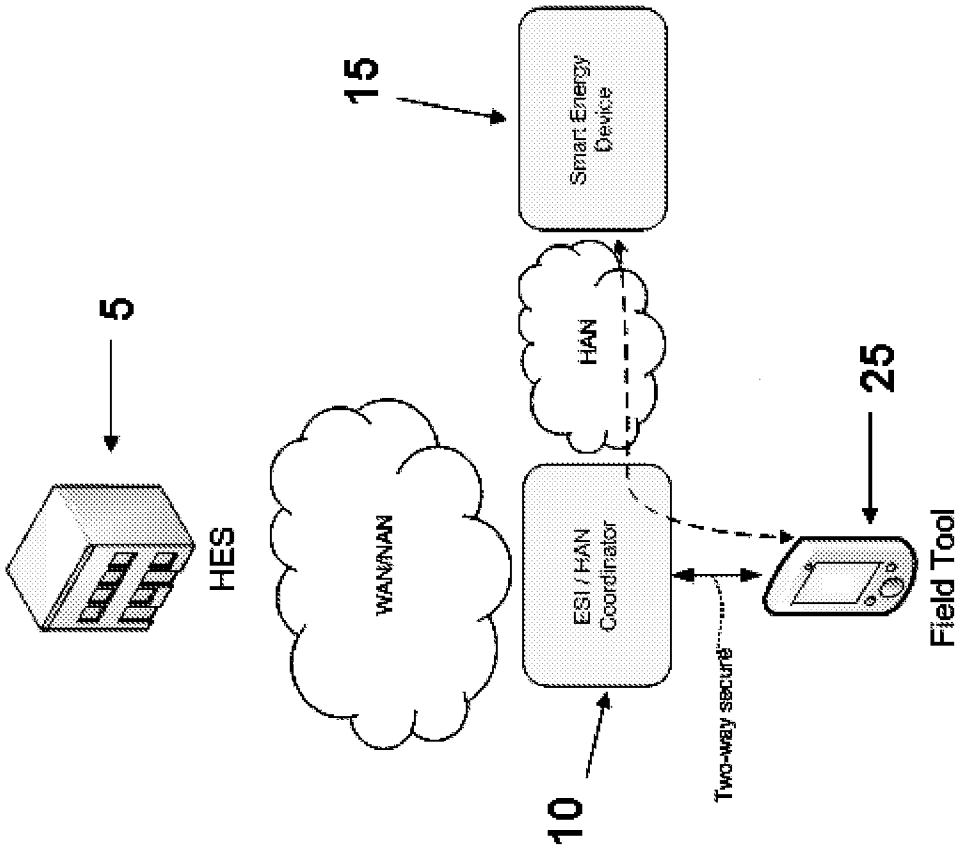


FIGURE 1e

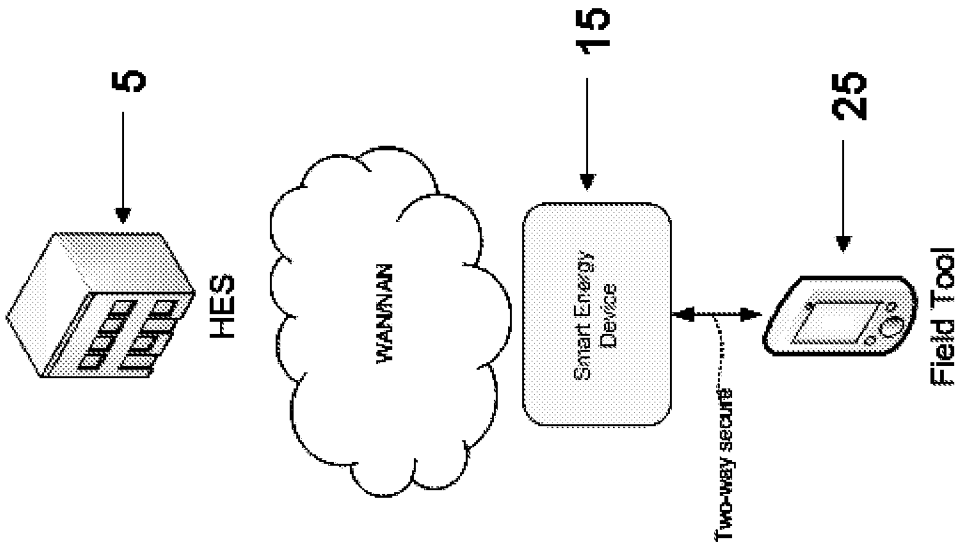


FIGURE 1d

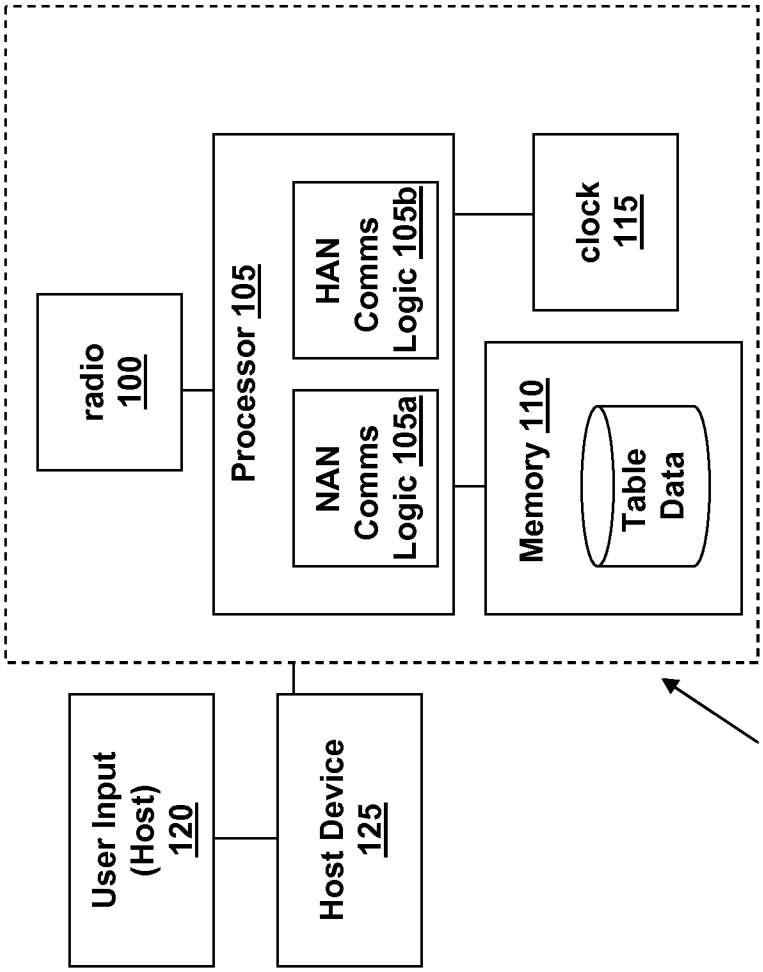

radio 100
Processor 105
HAN Comms Logic 105b
NAN Comms Logic 105a
clock 115
Memory 110
Table Data
User Input (Host) 120
Host Device 125
5

FIGURE 2a

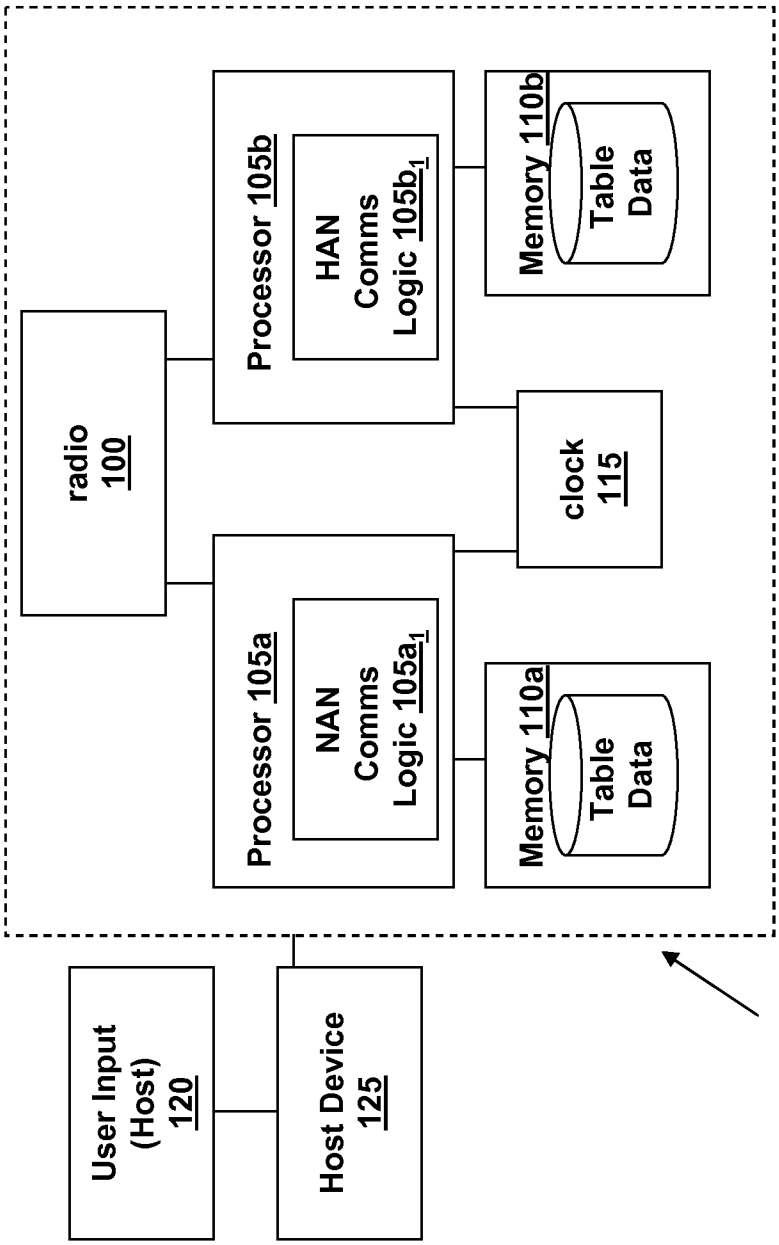

radio
100
Processor 105b
HAN
Comms
Logic 105b1
Memory 110b
Table
Data
clock
115
Processor 105a
NAN
Comms
Logic 105a1
Memory 110a
Table
Data
User Input
(Host)
120
Host Device
125
5

FIGURE 2b

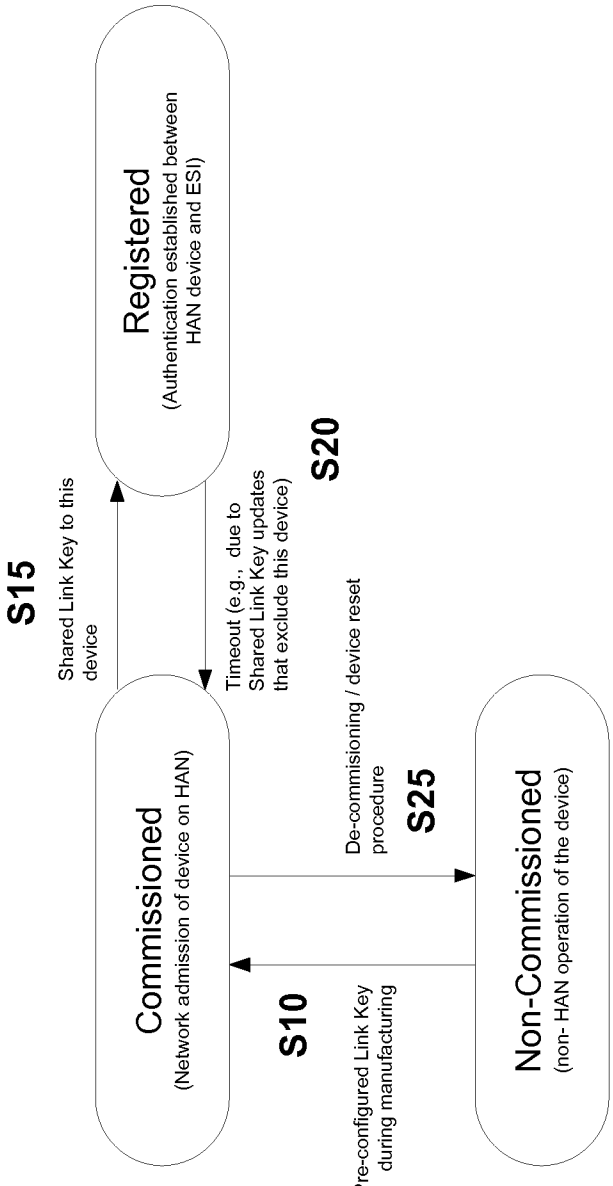

Registered
(Authentication established between HAN device and ESI)
S15
Shared Link Key to this device
Timeout (e.g., due to Shared Link Key updates that exclude this device)
S20
Commissioned
(Network admission of device on HAN)
De-commisioning / device reset procedure
S25
S10
Pre-configured Link Key during manufacturing
Non-Commissioned
(non- HAN operation of the device)

FIGURE 3

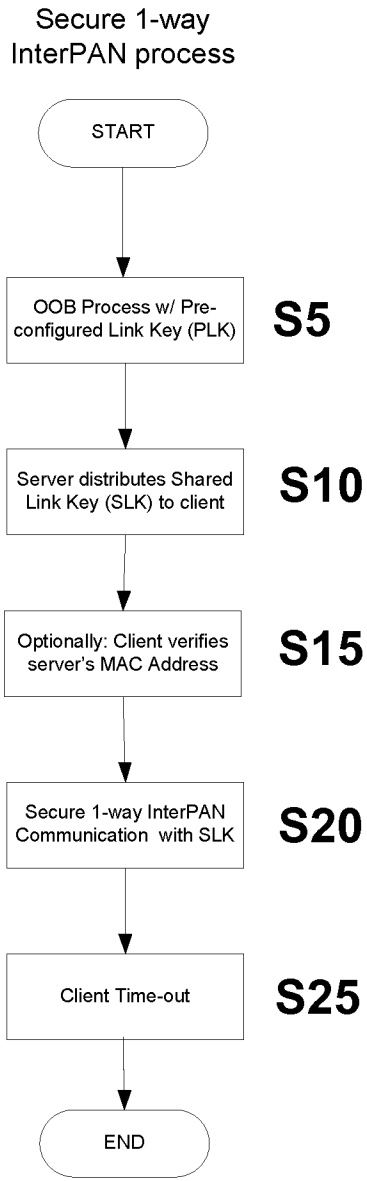


FIGURE 4a

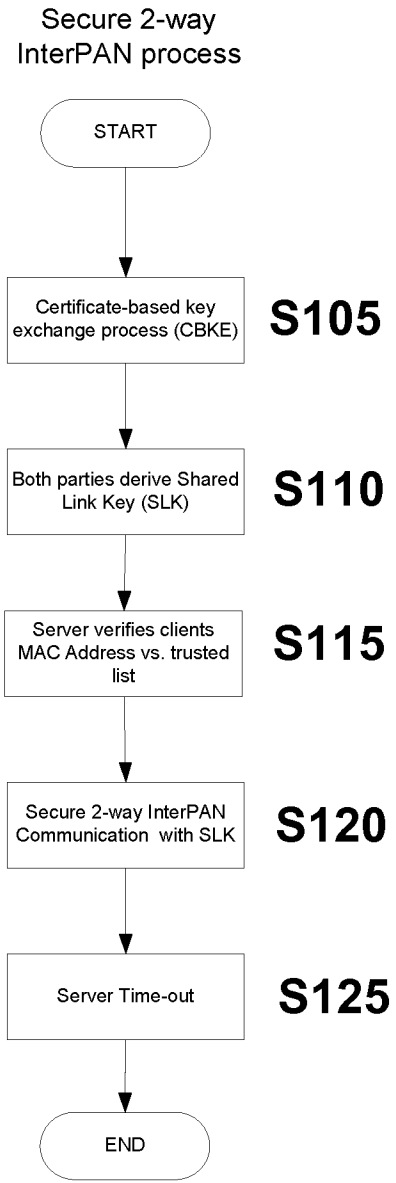


FIGURE 4b

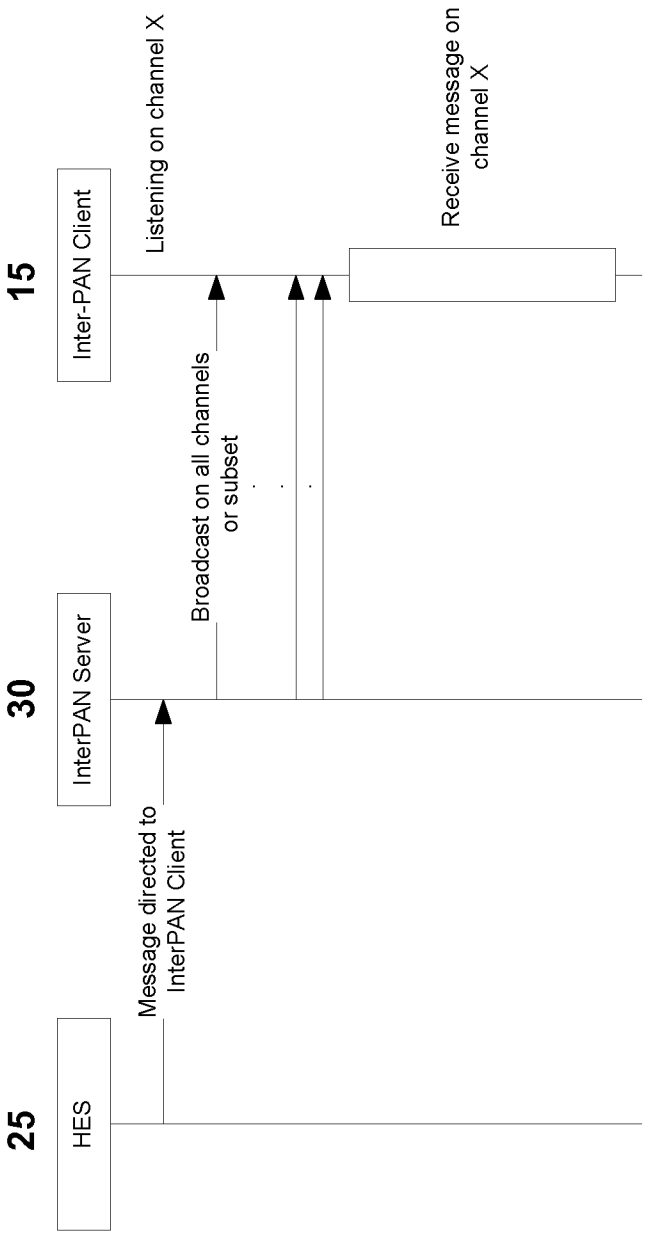

25
HES
30
InterPAN Server
15
Inter-PAN Client
Message directed to InterPAN Client
Broadcast on all channels or subset
Listening on channel X
Receive message on channel X

FIGURE 5

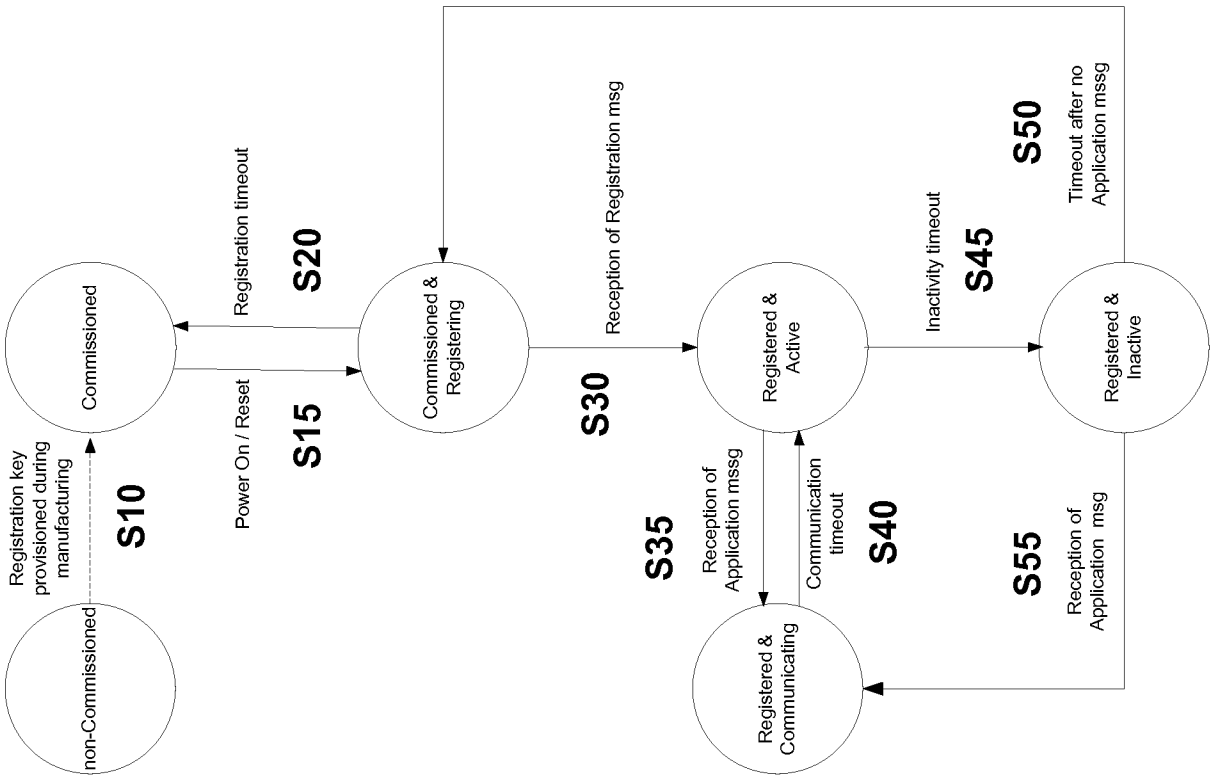

non-Commissioned
Registration key provisioned during manufacturing
S10
Commissioned
Power On / Reset
S15
Registration timeout
S20
Commissioned & Registering
Reception of Registration msg
S30
Registered & Active
Reception of Application mssg
S35
Registered & Communicating
Communication timeout
S40
Inactivity timeout
S45
Registered & Inactive
Timeout after no Application mssg
S50
Reception of Application msg
S55

FIGURE 6

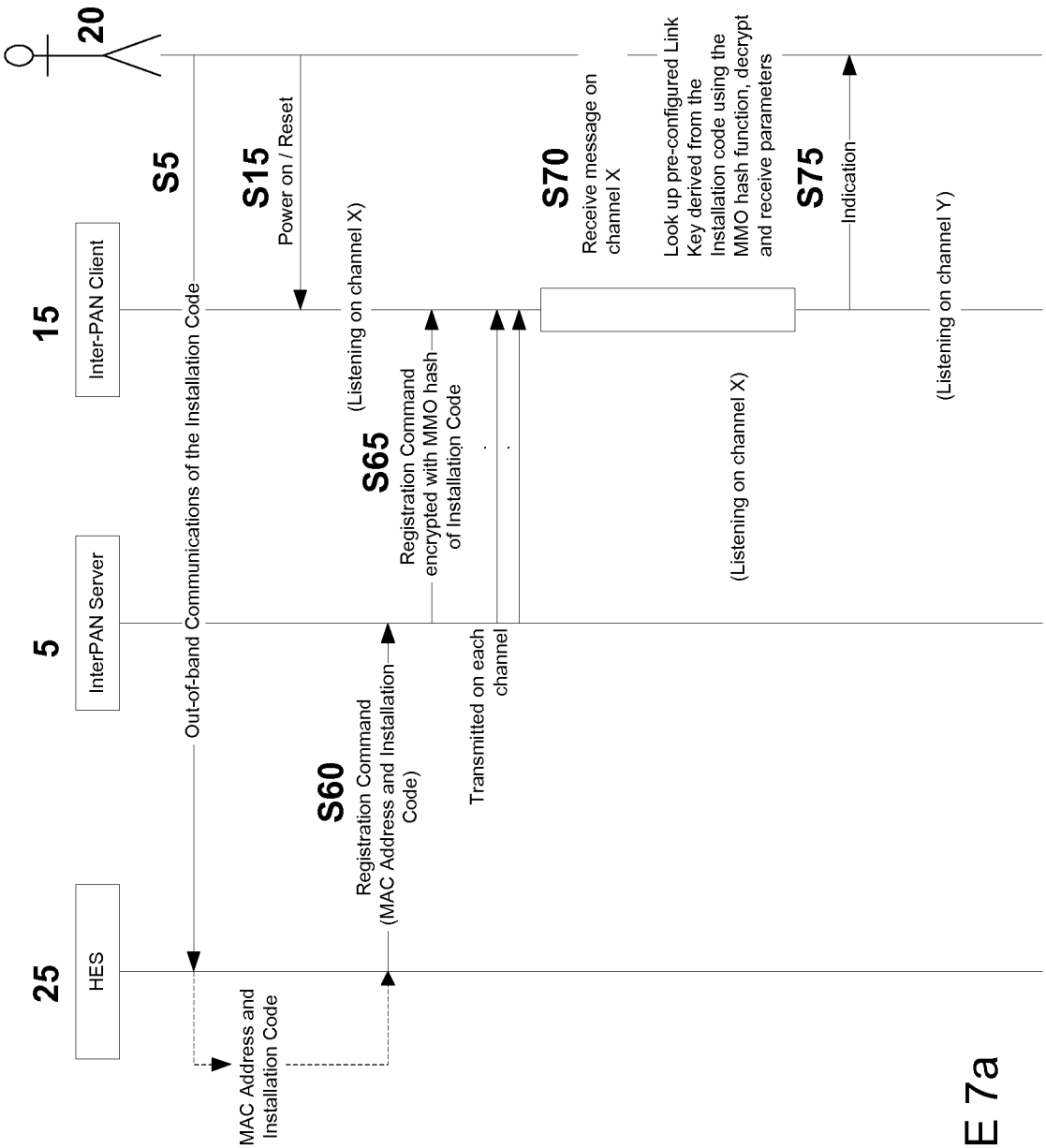

25
HES
5
InterPAN Server
15
Inter-PAN Client
20
S5
Out-of-band Communications of the Installation Code
S15
Power on / Reset
(Listening on channel X)
S60
Registration Command
(MAC Address and Installation Code)
S65
Registration Command
encrypted with MMO hash
of Installation Code
Transmitted on each channel
S70
Receive message on channel X
Look up pre-configured Link Key derived from the Installation code using the MMO hash function, decrypt and receive parameters
(Listening on channel X)
S75
Indication
(Listening on channel Y)
MAC Address and Installation Code

FIGURE 7a

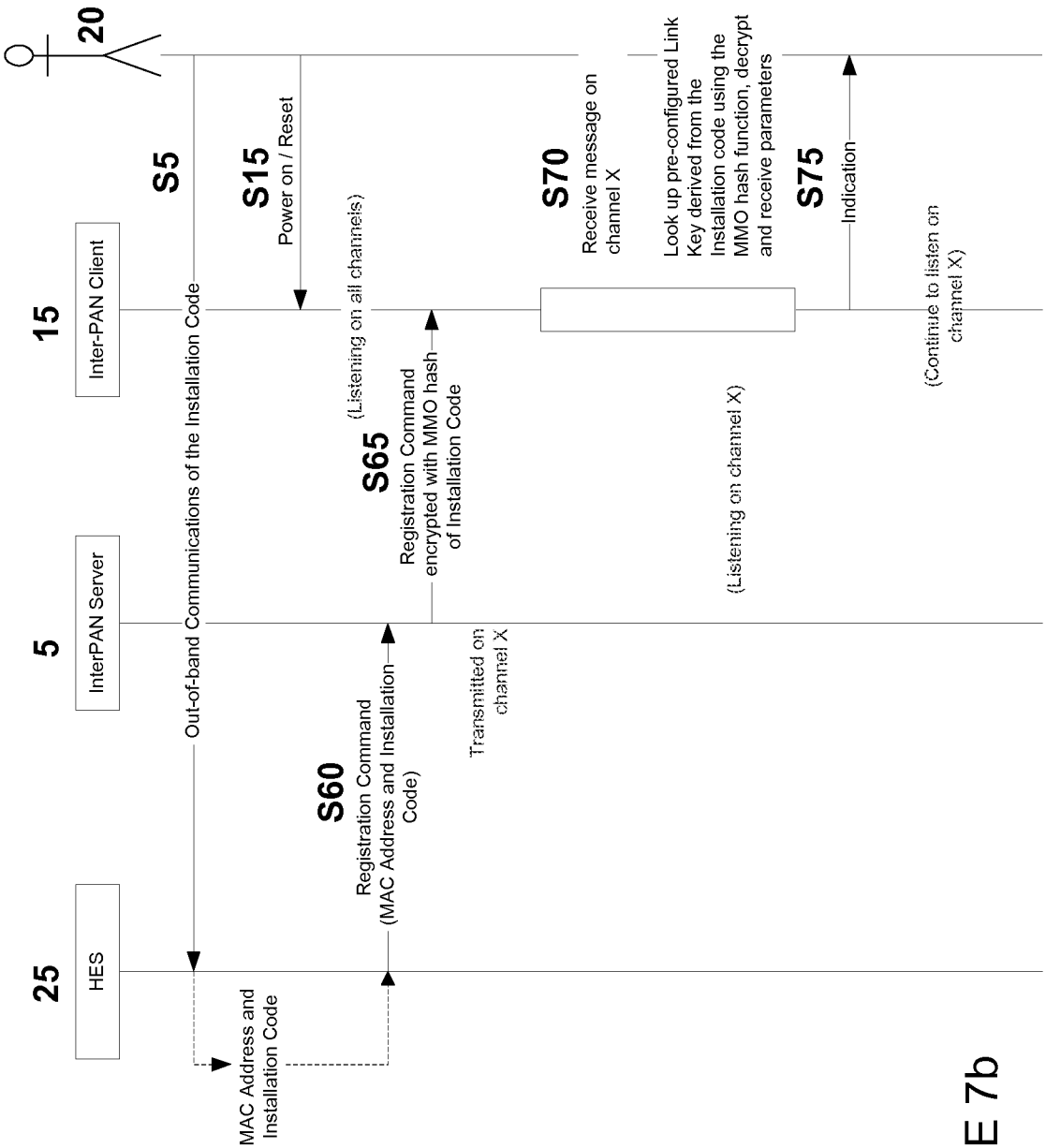

25
HES
5
InterPAN Server
15
Inter-PAN Client
20
Out-of-band Communications of the Installation Code
S5
S15
Power on / Reset
(Listening on all channels)
S60
Registration Command
(MAC Address and Installation Code)
S65
Registration Command
encrypted with MMO hash
of Installation Code
Transmitted on channel X
S70
Receive message on channel X
Look up pre-configured Link Key derived from the Installation code using the MMO hash function, decrypt and receive parameters
(Listening on channel X)
S75
Indication
(Continue to listen on channel X)
MAC Address and Installation Code

FIGURE 7b

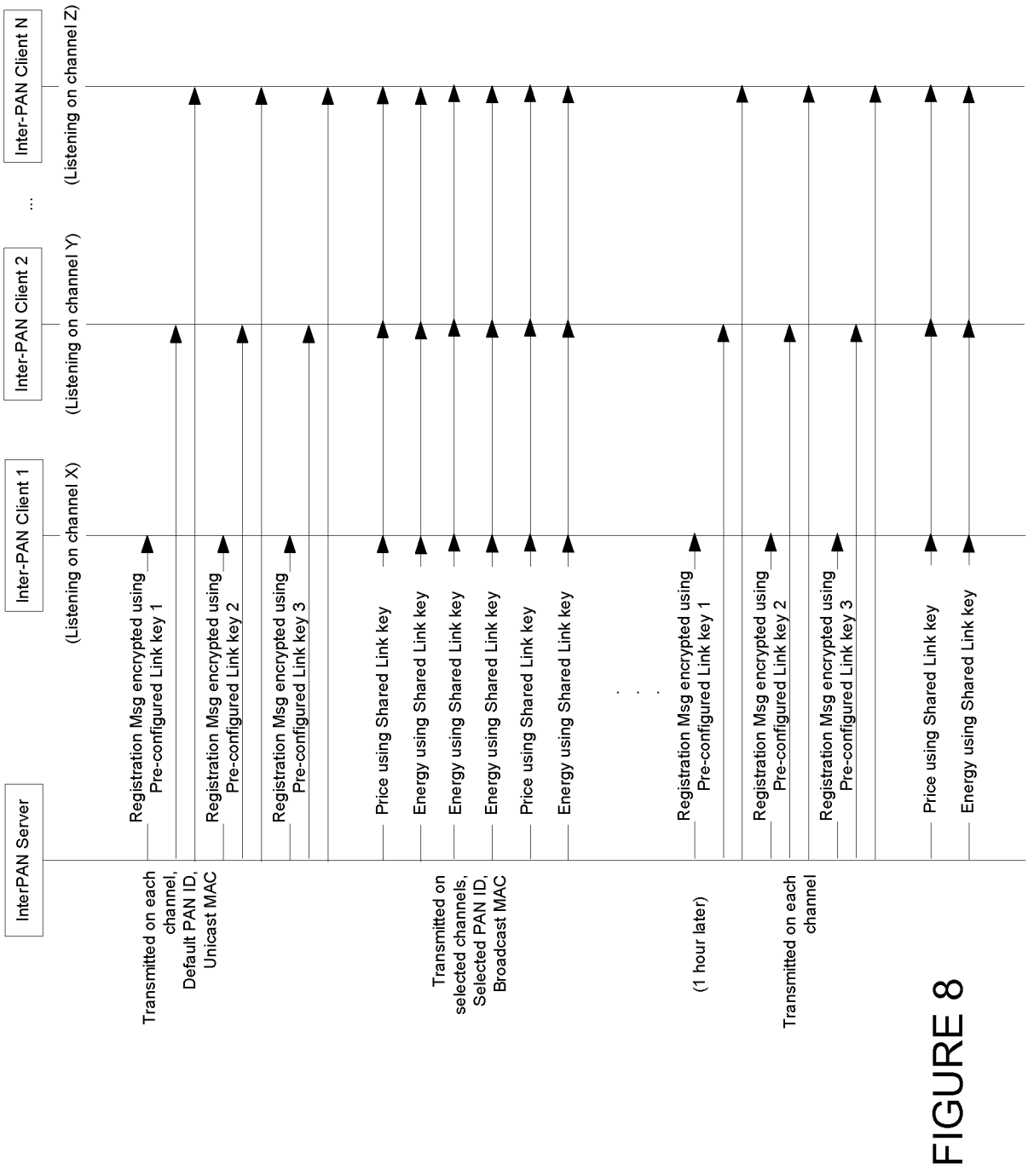
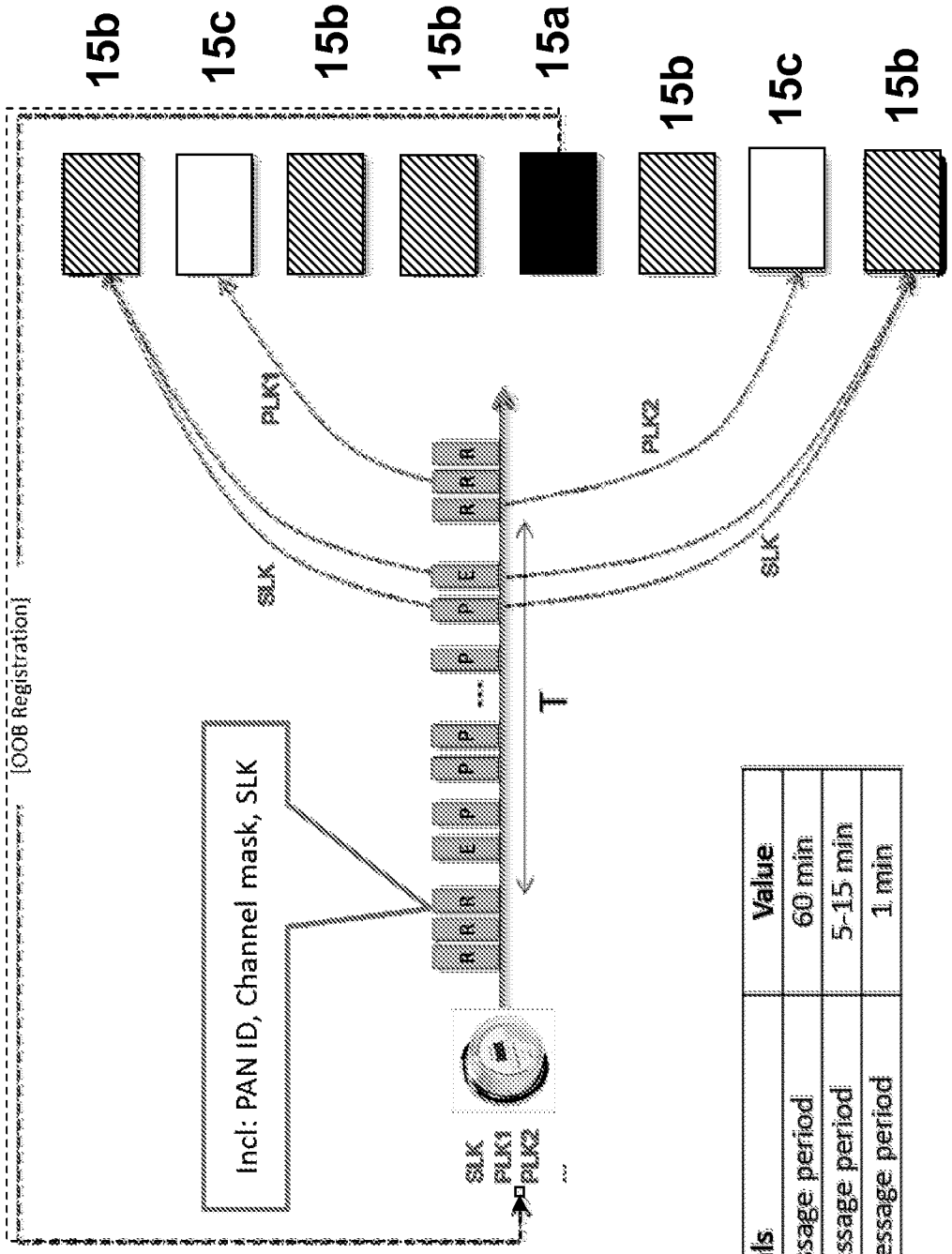

5
InterPAN Server
15a
Inter-PAN Client 1
(Listening on channel X)
15b
Inter-PAN Client 2
(Listening on channel Y)
...
15n
Inter-PAN Client N
(Listening on channel Z)
Transmitted on each channel, Default PAN ID, Unicast MAC
Registration Msg encrypted using Pre-configured Link key 1
Registration Msg encrypted using Pre-configured Link key 2
Registration Msg encrypted using Pre-configured Link key 3
Transmitted on selected channels, Selected PAN ID, Broadcast MAC
Price using Shared Link key
Energy using Shared Link key
Energy using Shared Link key
Energy using Shared Link key
Price using Shared Link key
Energy using Shared Link key
(1 hour later)
Registration Msg encrypted using Pre-configured Link key 1
Transmitted on each channel
Registration Msg encrypted using Pre-configured Link key 2
Registration Msg encrypted using Pre-configured Link key 3
Price using Shared Link key
Energy using Shared Link key

FIGURE 8

FIGURE 9



Example Intervals	Value
Registration message period	60 min
Publish Price message period	5-15 min
Energy Usage message period	1 min

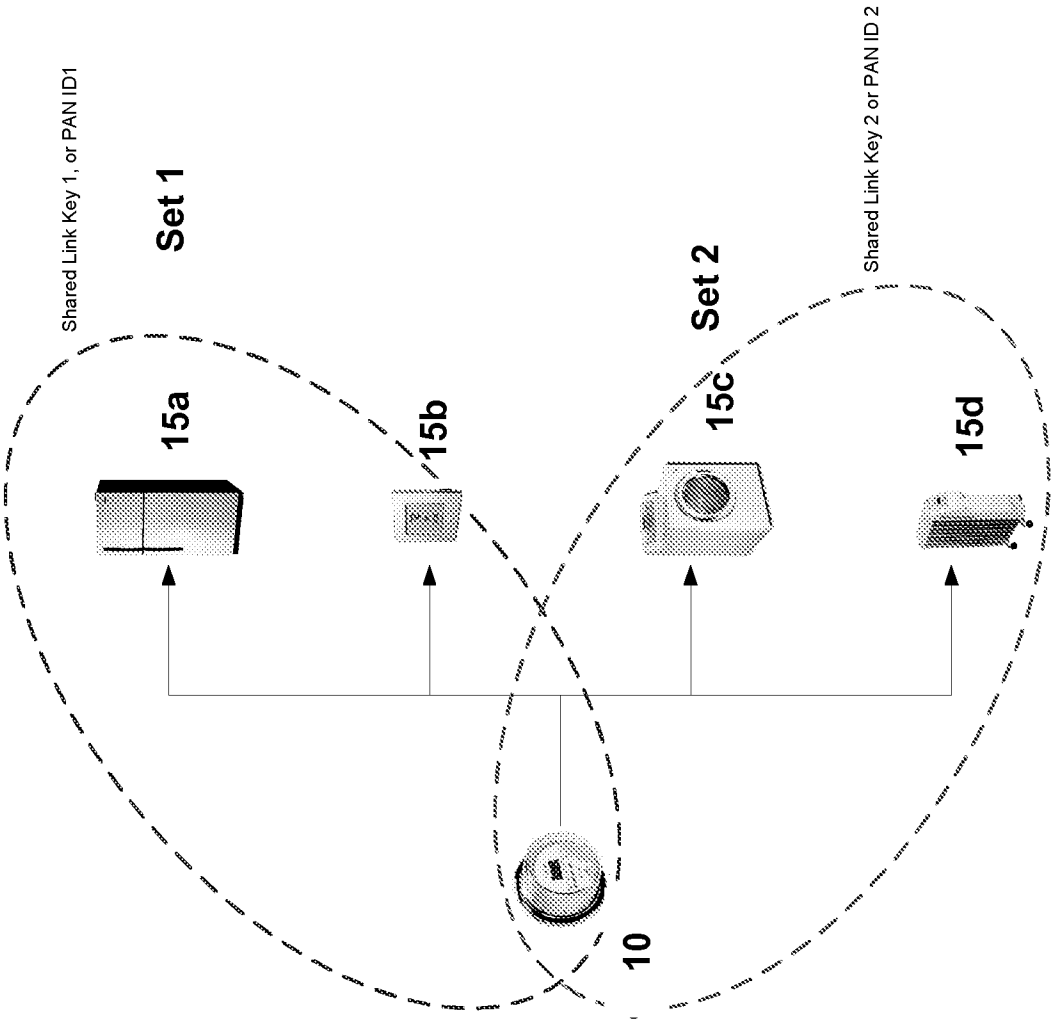

Shared Link Key 1, or PAN ID1
Set 1
15a
15b
Shared Link Key 2 or PAN ID 2
Set 2
15c
15d
10

FIGURE 10

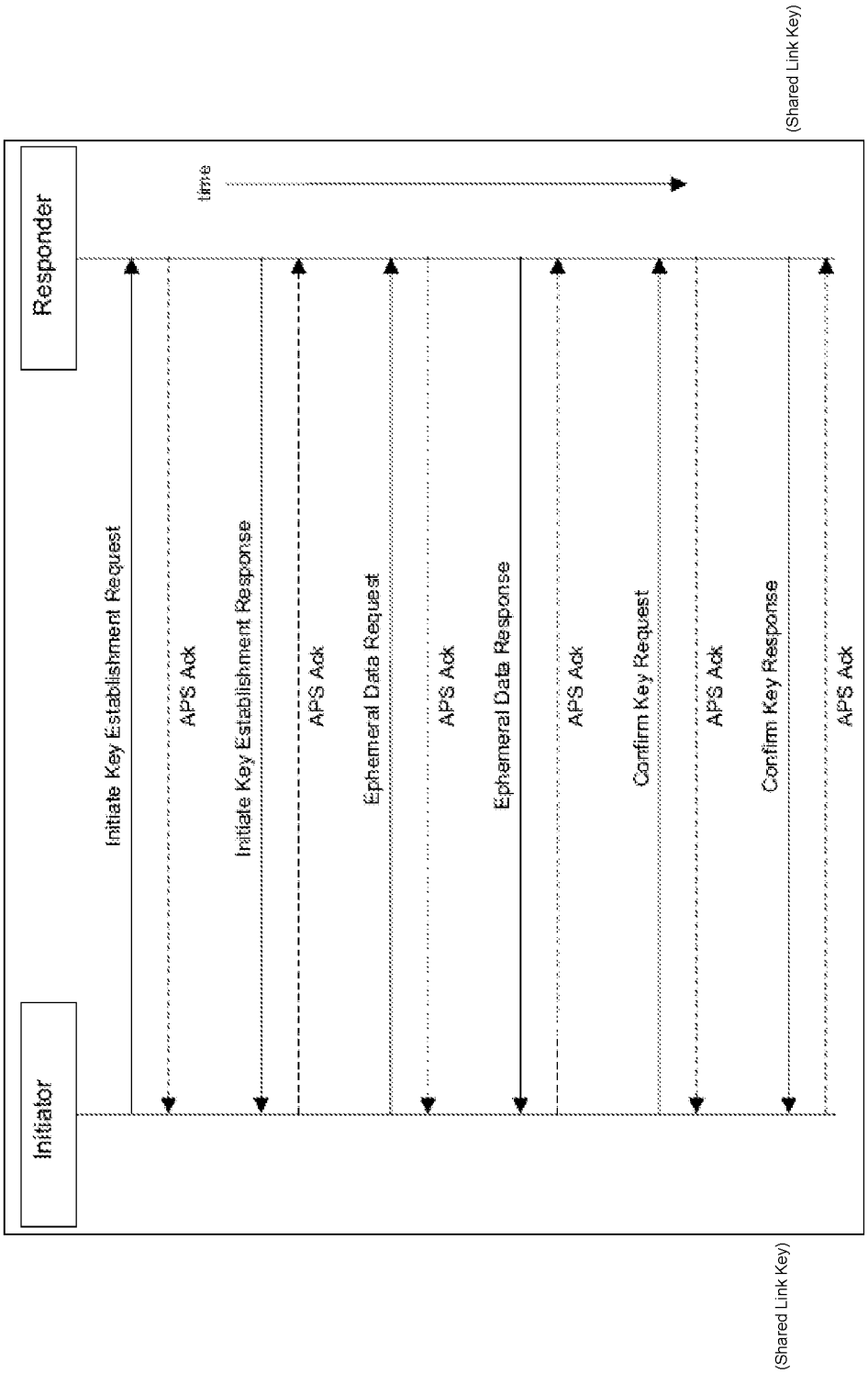


FIGURE 11
Prior Art

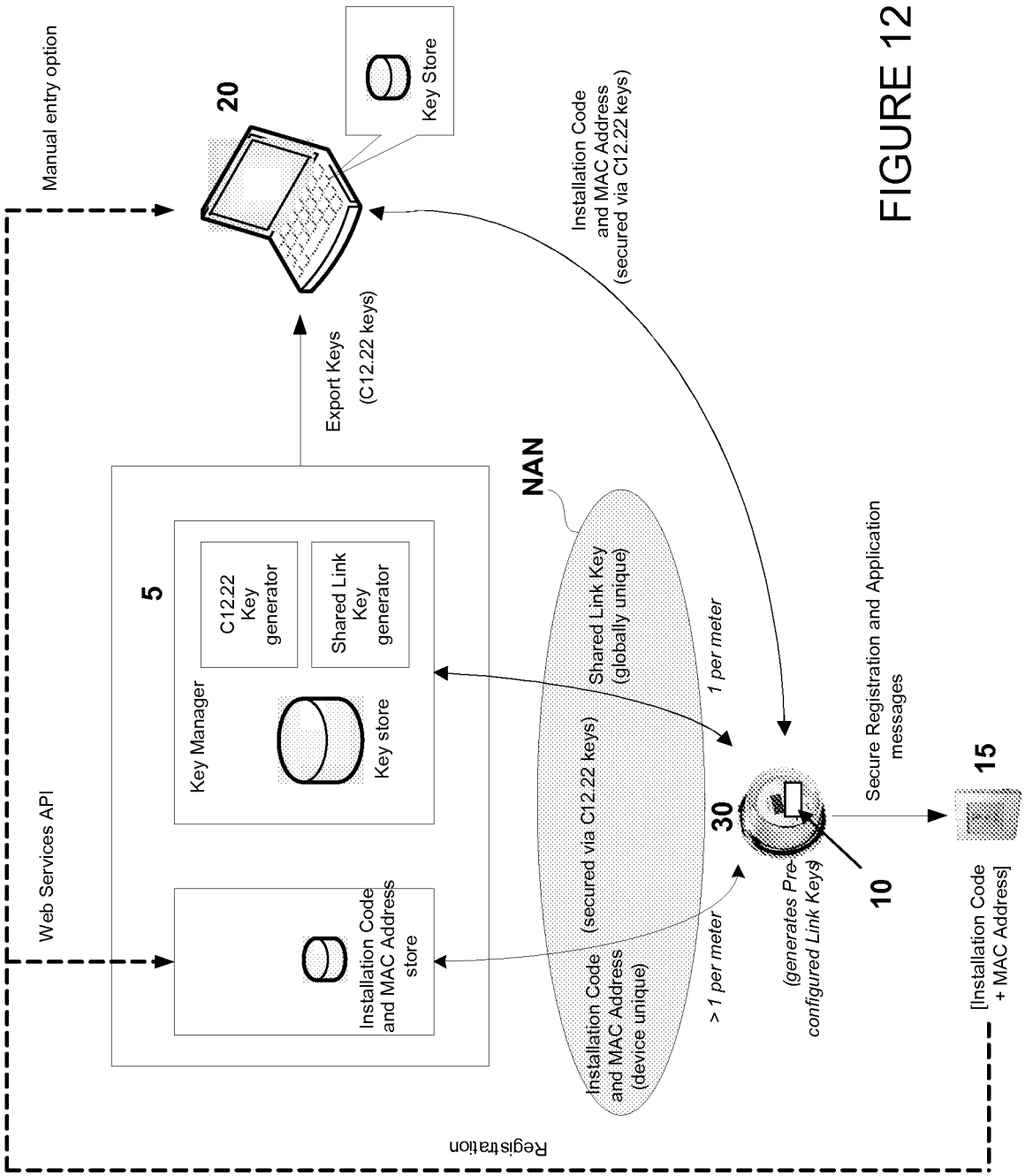

Manual entry option
20
Key Store
Installation Code
and MAC Address
(secured via C12.22 keys)
Export Keys
(C12.22 keys)
NAN
5
Key Manager
C12.22
Key
generator
Shared Link
Key
generator
Key store
Shared Link Key
(globally unique)
1 per meter
Web Services API
Installation Code
and MAC Address
store
(secured via C12.22 keys)
Installation Code
and MAC Address
(device unique)
> 1 per meter
30
(generates Pre-configured Link Keys)
10
Secure Registration and Application messages
15
[Installation Code
+ MAC Address]
Registration

FIGURE 12