

US00RE47894E

(19) **United States**
(12) **Reissued Patent**
Wang

(10) **Patent Number:** **US RE47,894 E**
(45) **Date of Reissued Patent:** ***Mar. 3, 2020**

(54) **METHOD AND SYSTEM FOR DYNAMIC INFORMATION EXCHANGE ON LOCATION AWARE MESH NETWORK DEVICES**

(71) Applicant: **III HOLDINGS 2, LLC**, Wilmington, DE (US)

(72) Inventor: **Ray Wang**, McLean, VA (US)

(73) Assignee: **III HOLDINGS 2, LLC**, Wilmington, DE (US)

(*) Notice: This patent is subject to a terminal disclaimer.

(21) Appl. No.: **14/693,299**

(22) Filed: **Apr. 22, 2015**

Related U.S. Patent Documents

Reissue of:

(64) Patent No.: **8,427,979**
Issued: **Apr. 23, 2013**
Appl. No.: **13/668,621**
Filed: **Nov. 5, 2012**

U.S. Applications:

(63) Continuation-in-part of application No. 12/884,521, filed on Sep. 17, 2010, now Pat. No. 8,305,935, which
(Continued)

(51) **Int. Cl.**
H04L 12/28 (2006.01)
H04B 1/707 (2011.01)
H04L 29/08 (2006.01)
H04L 29/06 (2006.01)
H04W 76/14 (2018.01)
H04W 4/029 (2018.01)
H04W 4/02 (2018.01)
H04W 84/18 (2009.01)

(52) **U.S. Cl.**
CPC **H04B 1/707** (2013.01); **H04L 63/08** (2013.01); **H04L 63/102** (2013.01); **H04L 67/306** (2013.01); **H04W 4/023** (2013.01); **H04W 4/029** (2018.02); **H04W 76/14** (2018.02); **H04L 63/0428** (2013.01); **H04L 67/12** (2013.01); **H04L 67/18** (2013.01); **H04W 84/18** (2013.01)

(58) **Field of Classification Search**
CPC ... H04W 64/00; H04W 64/003; H04W 4/023; H04W 4/021; H04W 4/04; H04L 41/12; H04L 45/02

See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

3,960,722 A 6/1976 Tomikawa
4,048,075 A 9/1977 Colvin

(Continued)

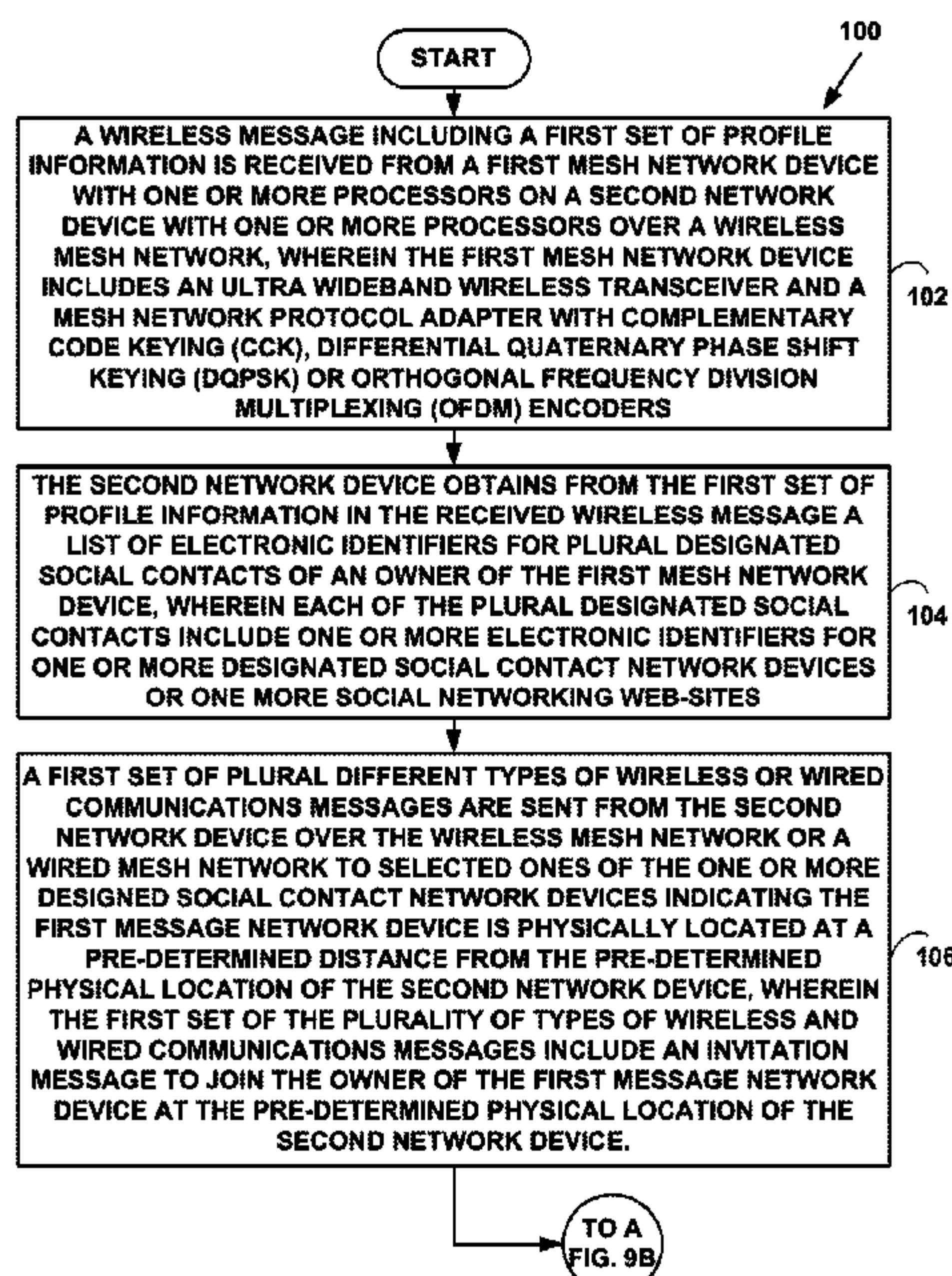
Primary Examiner — Charles R Craver

(74) *Attorney, Agent, or Firm* — McAndrews, Held & Malloy, Ltd.

(57) **ABSTRACT**

A method and system for dynamic information exchange on mesh network devices. Mobile location aware mesh network devices automatically exchange information with other mobile location aware devices that are located at a pre-determined distance of each other at a desired physical location. A server network device compares electronic profiles that include stated interests of the mobile location aware devices. The server network device also provides additional information to the mobile location aware mesh network devices based on stated interests in the electronic profiles of the mobile location aware network devices.

53 Claims, 19 Drawing Sheets



US RE47,894 E

Page 2

Related U.S. Application Data

is a continuation-in-part of application No. 11/880, 271, filed on Jul. 20, 2007, now Pat. No. 7,801,058.

(60) Provisional application No. 60/833,741, filed on Jul. 27, 2006.

(56) References Cited

U.S. PATENT DOCUMENTS

4,053,677	A	10/1977	Corao
4,119,096	A	10/1978	Drews
4,135,564	A	1/1979	Muller
4,142,950	A	3/1979	Creamer
4,158,275	A	6/1979	Moore
4,221,854	A	9/1980	Hammar
4,222,563	A	9/1980	Heflter
4,226,408	A	10/1980	Tomita
4,280,075	A	7/1981	Comby
4,286,362	A	9/1981	Hammar
4,342,884	A	8/1982	Ban
4,343,690	A	8/1982	de Nora
4,373,027	A	2/1983	Berneman
4,400,287	A	8/1983	Kimura
4,440,000	A	4/1984	Bacchus
4,455,187	A	6/1984	von Blucher
4,479,875	A	10/1984	Nelson
4,562,015	A	12/1985	Lefevre
4,564,539	A	1/1986	Tsuji
4,654,556	A	3/1987	Comby
4,693,986	A	9/1987	Vit
4,698,768	A	10/1987	Thuy
4,751,869	A	6/1988	Paynter
4,781,056	A	11/1988	Noel
4,788,088	A	11/1988	Kohl
4,837,798	A *	6/1989	Cohen G06Q 10/107 379/396
4,837,850	A	6/1989	Maisel
4,917,537	A	4/1990	Jacobson
4,940,972	A	7/1990	Mouchot
5,034,352	A	7/1991	Vit
5,042,463	A	8/1991	Lekholm
5,105,424	A	4/1992	Flaig
5,128,789	A	7/1992	Abramovitz
5,182,440	A	1/1993	Dufour
5,207,687	A	5/1993	Bernon
5,218,565	A	6/1993	Mou
5,236,027	A	8/1993	Lu
5,309,107	A	5/1994	Pausch
5,365,518	A	11/1994	Noser
5,396,359	A	3/1995	Abramovitz
5,447,776	A	9/1995	Disselbeck
5,448,389	A	9/1995	Peacock
5,477,888	A	12/1995	Mezzalira
5,512,828	A	4/1996	Pausch
5,530,575	A	6/1996	Acampora
5,545,318	A	8/1996	Richmond
5,550,805	A	8/1996	Takatori
5,571,080	A	11/1996	Jensen
5,571,352	A	11/1996	Disselbeck
5,581,187	A	12/1996	Pausch
5,592,610	A	1/1997	Chittor
5,606,666	A	2/1997	Grant
5,670,278	A	9/1997	Disselbeck
5,682,537	A	10/1997	Davies
5,689,647	A	11/1997	Miura
5,703,834	A	12/1997	Bonnefoy
5,802,054	A	9/1998	Bellenger
5,842,034	A	11/1998	Bolstad
5,884,017	A	3/1999	Fee
5,934,614	A	8/1999	Mueller
5,949,760	A	9/1999	Stevens
5,959,999	A	9/1999	An
5,963,546	A	10/1999	Shoji
6,038,044	A	3/2000	Fee
6,049,593	A	4/2000	Acampora
6,113,080	A	9/2000	Kazuma

6,143,029	A	11/2000	Rippstein
6,154,587	A	11/2000	Okayama
6,189,102	B1	2/2001	Beser
6,219,346	B1	4/2001	Maxemchuk
6,256,306	B1	7/2001	Bellenger
6,298,053	B1	10/2001	Flammer, III
6,314,163	B1	11/2001	Acampora
6,324,162	B1	11/2001	Chaudhuri
6,329,902	B1	12/2001	Lee
6,370,110	B1	4/2002	Eslambolchi
6,396,837	B1	5/2002	Wang
6,403,210	B1	6/2002	Stuivinga
6,460,128	B1	10/2002	Baxter
6,480,497	B1	11/2002	Flammer, III
6,549,513	B1	4/2003	Chao
6,618,611	B2	9/2003	Gebhardt
6,640,087	B2	10/2003	Reed et al.
6,654,379	B1	11/2003	Grover
6,711,166	B1	3/2004	Amir
6,735,393	B1	5/2004	Zouganeli
6,763,190	B2	7/2004	Agrawal
6,780,340	B2	8/2004	Conta
6,785,725	B1	8/2004	Ramanan
6,805,732	B1	10/2004	Billiotte
6,823,180	B2	11/2004	Reed
6,835,173	B2	12/2004	Couvillon, Jr.
6,848,006	B1	1/2005	Hermann
6,850,502	B1	2/2005	Kagan
6,853,641	B2	2/2005	Lindhorst-Ko
6,856,592	B2	2/2005	Grover
6,879,574	B2	4/2005	Naghian
6,904,364	B2	6/2005	Randazzo
6,909,903	B2	6/2005	Wang
6,912,204	B2	6/2005	Kossi
6,917,759	B2	7/2005	DeBoer
6,934,248	B1	8/2005	DeBoer
6,940,866	B1	9/2005	Miller
6,948,048	B2	9/2005	Baxter
6,965,575	B2	11/2005	Srikrishna
6,965,969	B2	11/2005	Burger
6,970,417	B1	11/2005	Doverspike
6,970,808	B2	11/2005	Abhulimen
6,999,441	B2	2/2006	Flammer, III
7,003,313	B2	2/2006	Garces
7,012,887	B2	3/2006	Zhu
7,027,388	B2	4/2006	Wen
7,031,293	B1	4/2006	Srikrishna
7,031,757	B2	4/2006	Schwengler
7,039,067	B2	5/2006	Feinberg
7,042,988	B2	5/2006	Juitt
7,043,250	B1	5/2006	DeMartino
7,050,819	B2	5/2006	Schwengler
7,053,853	B2	5/2006	Merenda
7,054,262	B2	5/2006	Gerstel
7,058,021	B2	6/2006	Srikrishna
7,068,873	B2	6/2006	Frankel
7,069,483	B2	6/2006	Gillies
7,088,676	B1	8/2006	Doverspike
7,088,920	B2	8/2006	Krishnaswamy
7,089,089	B2	8/2006	Cumming
7,106,261	B2	9/2006	Nagel
7,117,466	B2	10/2006	Kalafala
7,119,758	B2	10/2006	Louzir
7,123,589	B1	10/2006	Dawes
7,127,261	B2 *	10/2006	Van Erlach G06Q 30/0239 455/41.2
7,133,359	B2	11/2006	Weis
7,203,743	B2	4/2007	Shah-Heydari
7,215,658	B2	5/2007	Alastalo
7,215,926	B2	5/2007	Corbett
7,224,642	B1	5/2007	Tran
7,233,620	B2	6/2007	Brommer
7,239,238	B2	7/2007	Tester
7,239,850	B2	7/2007	Peikari
7,242,664	B2	7/2007	Einstein
7,245,216	B2	7/2007	Burkley
7,248,217	B2	7/2007	Mani
7,251,570	B2	7/2007	Hancock
7,257,106	B2	8/2007	Chen

(56)

References Cited

U.S. PATENT DOCUMENTS

7,257,250 B2	8/2007	Boier-Martin	2005/0141641 A1	6/2005	Tanaka et al.
7,260,059 B2	8/2007	Grover	2005/0190778 A1	9/2005	Ozluturk
7,262,694 B2	8/2007	Olsen	2005/0193357 A1	9/2005	Honary
7,263,379 B1	8/2007	Parkulo	2005/0243765 A1	11/2005	Schrader
7,269,347 B1	9/2007	Matricardi	2005/0246112 A1	11/2005	Abhulimen
7,271,736 B2	9/2007	Siegel	2005/0272430 A1	12/2005	Griebeling
7,274,869 B1	9/2007	Pan	2005/0281237 A1	12/2005	Heinonen
7,277,931 B1	10/2007	Booth	2006/0031659 A1	2/2006	Chow
7,280,755 B2	10/2007	Kang	2006/0095539 A1	5/2006	Renkis
7,282,944 B2	10/2007	Gunn	2006/0133332 A1	6/2006	Achanta
7,283,494 B2	10/2007	Hammel	2006/0133807 A1	6/2006	Jenkins
7,289,428 B2	10/2007	Chow	2006/0133817 A1	6/2006	Xie
7,289,923 B2	10/2007	Marovitz	2006/0154642 A1 *	7/2006	Scannell, Jr. 455/404.1
7,295,806 B2	11/2007	Corbett	2006/0159024 A1	7/2006	Hester
7,298,240 B2	11/2007	Lamar	2006/0182076 A1	8/2006	Wang
7,301,824 B1	11/2007	New	2006/0218225 A1	9/2006	Hee Voon
7,302,339 B2	11/2007	Gray	2006/0234631 A1 *	10/2006	Dieguez H04W 76/023 455/41.2
7,305,459 B2	12/2007	Klemba	2006/0262737 A1	11/2006	Livet
7,308,198 B1	12/2007	Chudak	2006/0268910 A1	11/2006	Kawahara
7,308,370 B2	12/2007	Mason, Jr. et al.	2007/0014573 A1	1/2007	Wei
7,310,515 B2 *	12/2007	Enderlein H04L 63/0407 455/414.1	2007/0066308 A1	3/2007	Andric
7,313,399 B2	12/2007	Rhee et al.	2007/0066874 A1	3/2007	Cook
7,522,058 B1 *	4/2009	Light G06Q 10/10 340/539.1	2007/0086361 A1	4/2007	Allan
7,586,888 B2	9/2009	Wang	2007/0090996 A1	4/2007	Wang
7,603,112 B2 *	10/2009	Huomo G06Q 20/382 455/3.06	2007/0091871 A1	4/2007	Taha
7,630,736 B2	12/2009	Wang	2007/0189249 A1	8/2007	Gurevich
7,801,058 B2 *	9/2010	Wang 370/254	2007/0195808 A1 *	8/2007	Ehrlich et al. 370/408
7,929,958 B2 *	4/2011	Van Erlach G06Q 30/0207 340/10.3	2007/0206521 A1	9/2007	Osaje
8,019,692 B2 *	9/2011	Rosen G06F 17/3087 705/319	2007/0206616 A1	9/2007	Orth
8,249,605 B2 *	8/2012	Niranjan H04L 12/66 370/254	2008/0002672 A1 *	1/2008	Lin H04L 12/66 370/352
8,295,851 B2 *	10/2012	Finnegan H04M 1/72513 455/411	2008/0025330 A1	1/2008	Wang
8,305,935 B2	11/2012	Wang	2008/0108308 A1 *	5/2008	Ullah G06Q 30/02 455/41.2
8,305,936 B2	11/2012	Wang	2009/0189739 A1	7/2009	Wang
9,300,925 B1 *	3/2016	Zhang H04N 7/181	2010/0280904 A1 *	11/2010	Ahuja G06Q 30/02 705/14.58
2002/0089712 A1	7/2002	Kang	2011/0019587 A1	1/2011	Wang
2002/0181427 A1	12/2002	Sparr et al.	2011/0208710 A1	8/2011	Lesavich
2003/0011839 A1	1/2003	Liang	2011/0210816 A1	9/2011	Wang
2004/0203387 A1 *	10/2004	Grannan G08C 17/00 455/41.2	2011/0225510 A1 *	9/2011	Lavrov G06Q 10/10 715/751
2004/0248601 A1	12/2004	Chang	2011/0235627 A1	9/2011	Wang
2005/0038876 A1	2/2005	Chaudhuri G06F 17/3087 709/219	2011/0299478 A1 *	12/2011	Clark H04L 67/30 370/329
2005/0048961 A1	3/2005	Ribaudo	2012/0016794 A1 *	1/2012	Orr G06Q 10/109 705/39
2005/0071714 A1	3/2005	Soga et al.	2012/0150960 A1 *	6/2012	Nalawade G06Q 30/02 709/204
2005/0074019 A1	4/2005	Handforth	2012/0278622 A1	11/2012	Lesavich
2005/0135286 A1	6/2005	Nurminen et al.	2014/0038526 A1 *	2/2014	Ennis H04W 4/005 455/41.2
			2015/0289100 A1 *	10/2015	Stringer, II H04W 4/023 455/456.3

* cited by examiner

FIG. 1

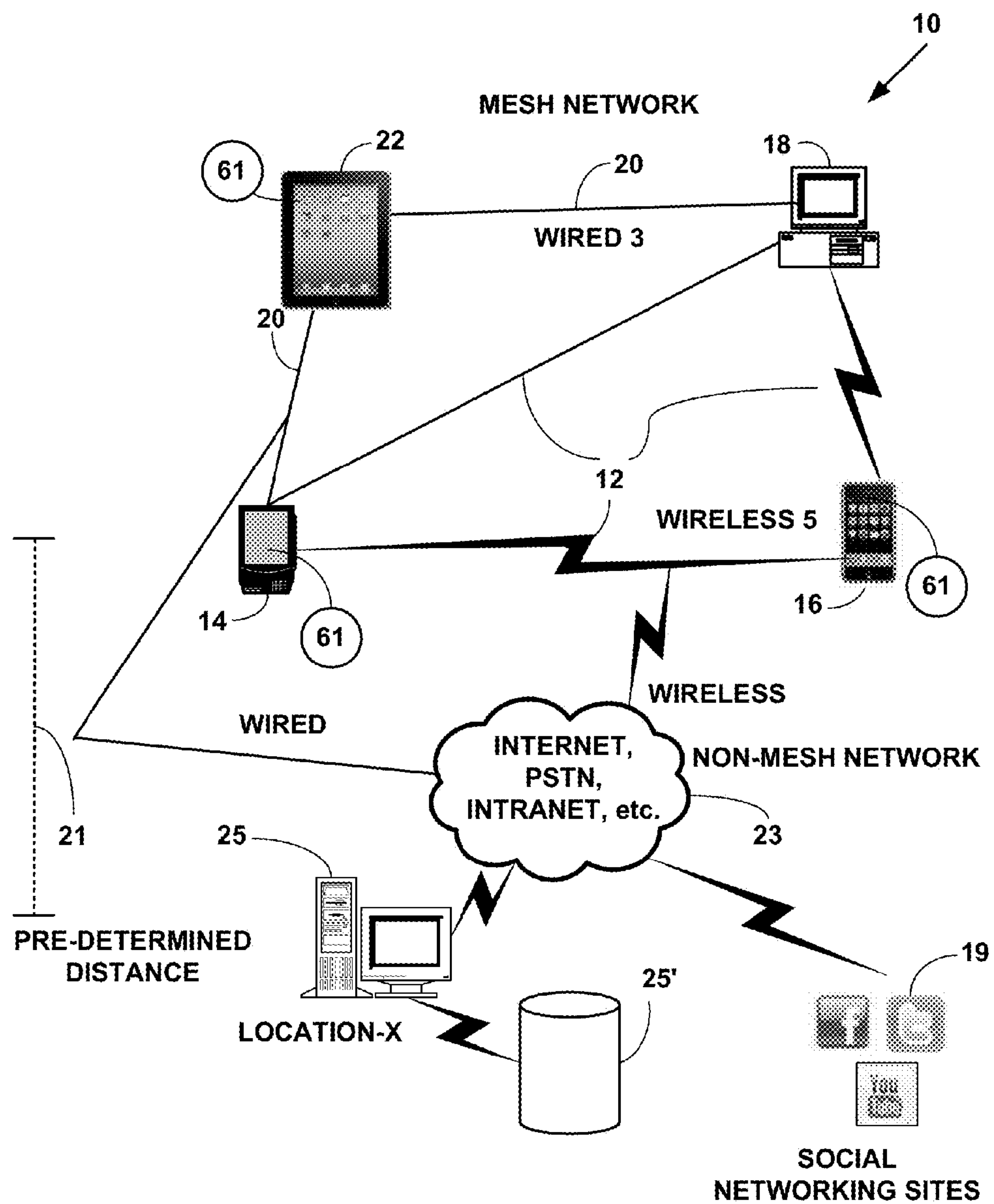


FIG. 2

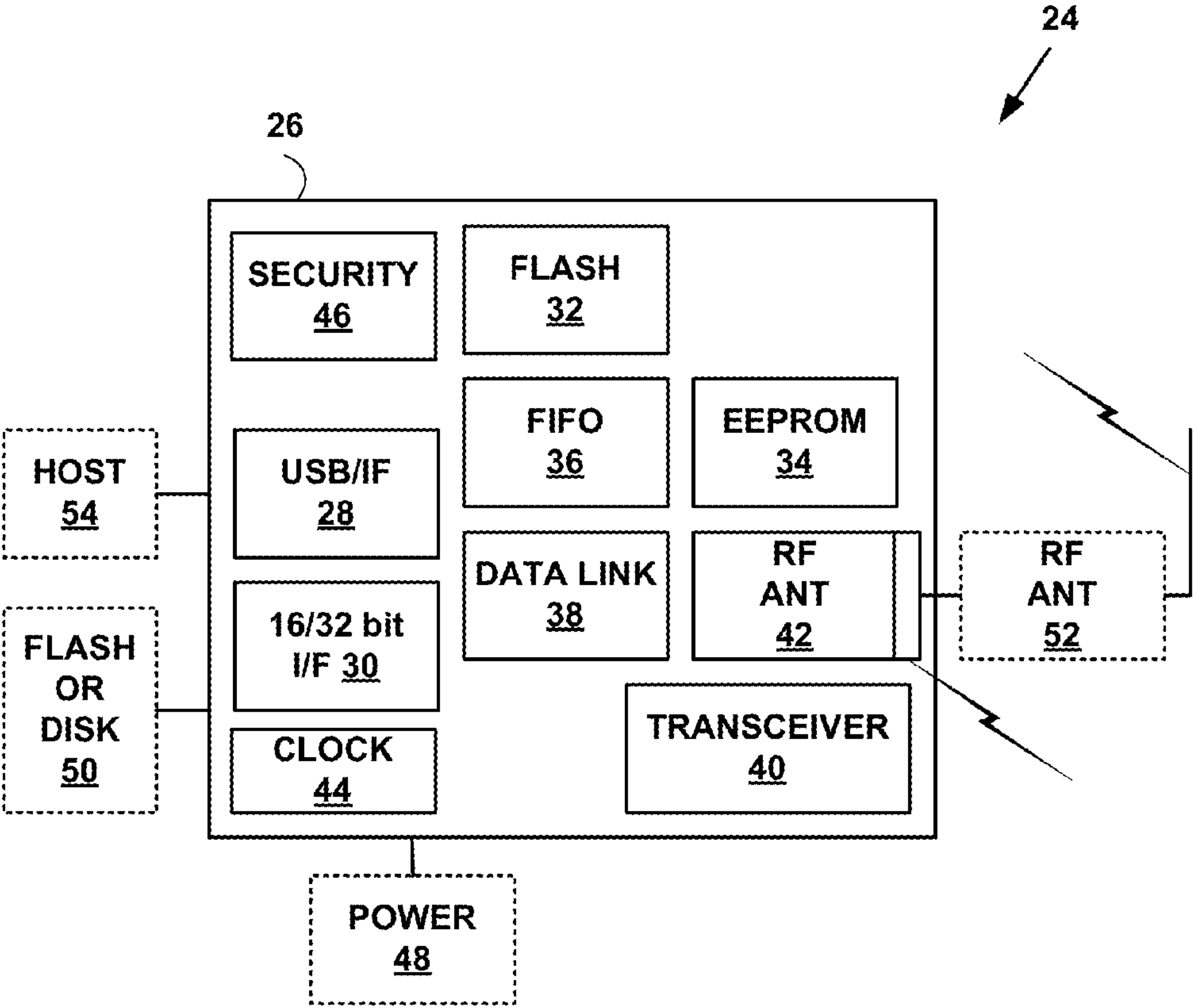


FIG. 3A

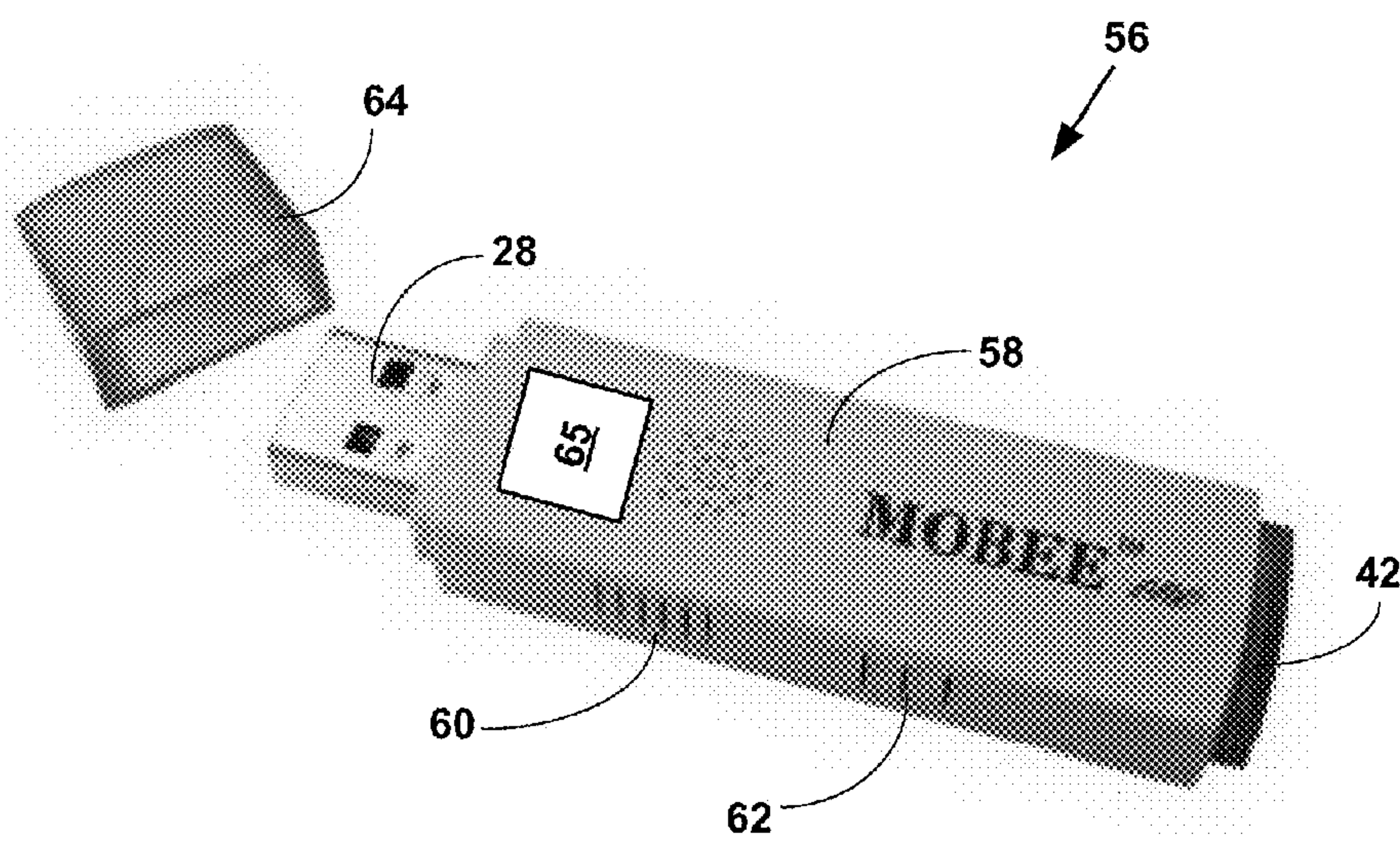


FIG. 3B

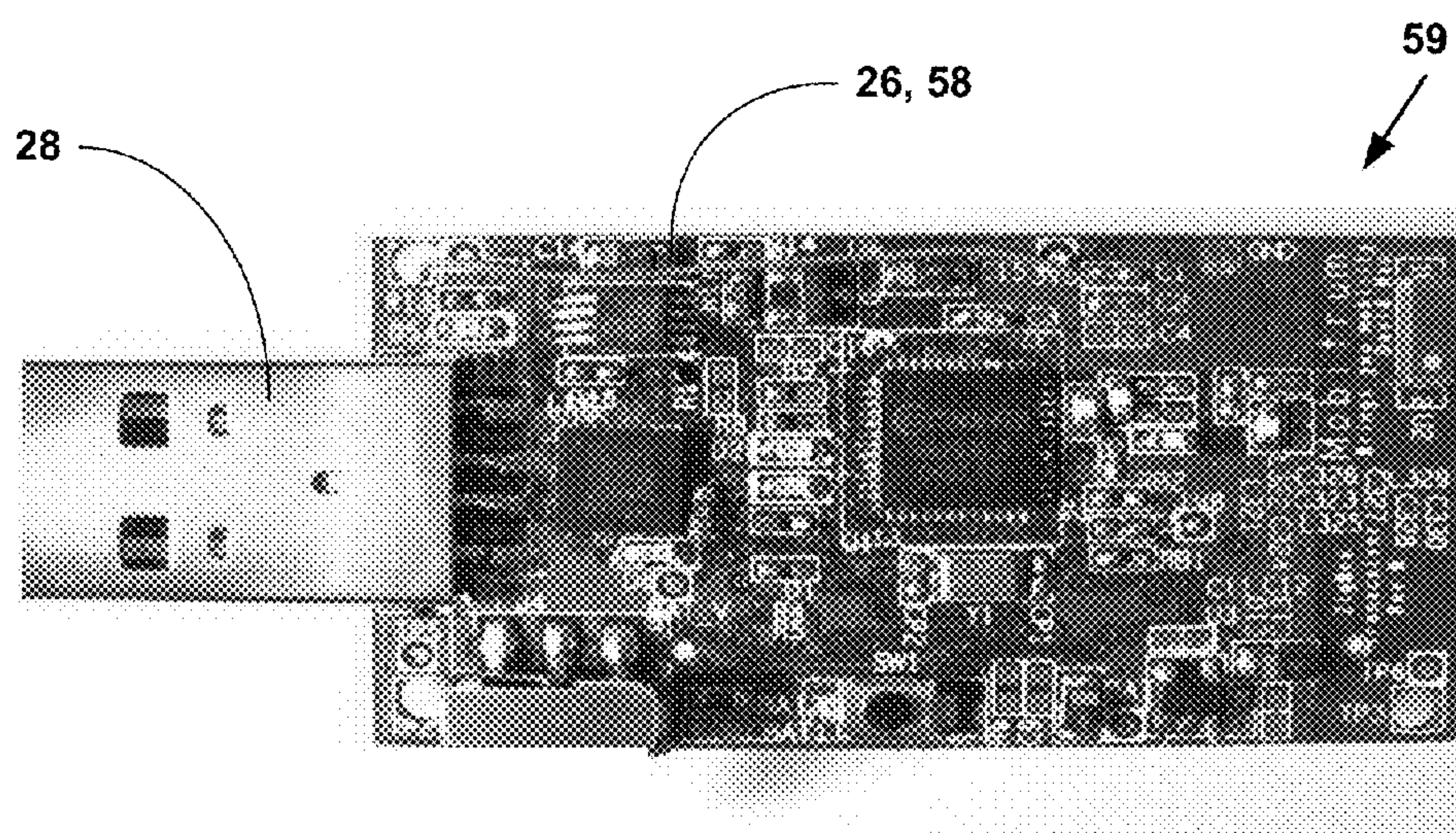


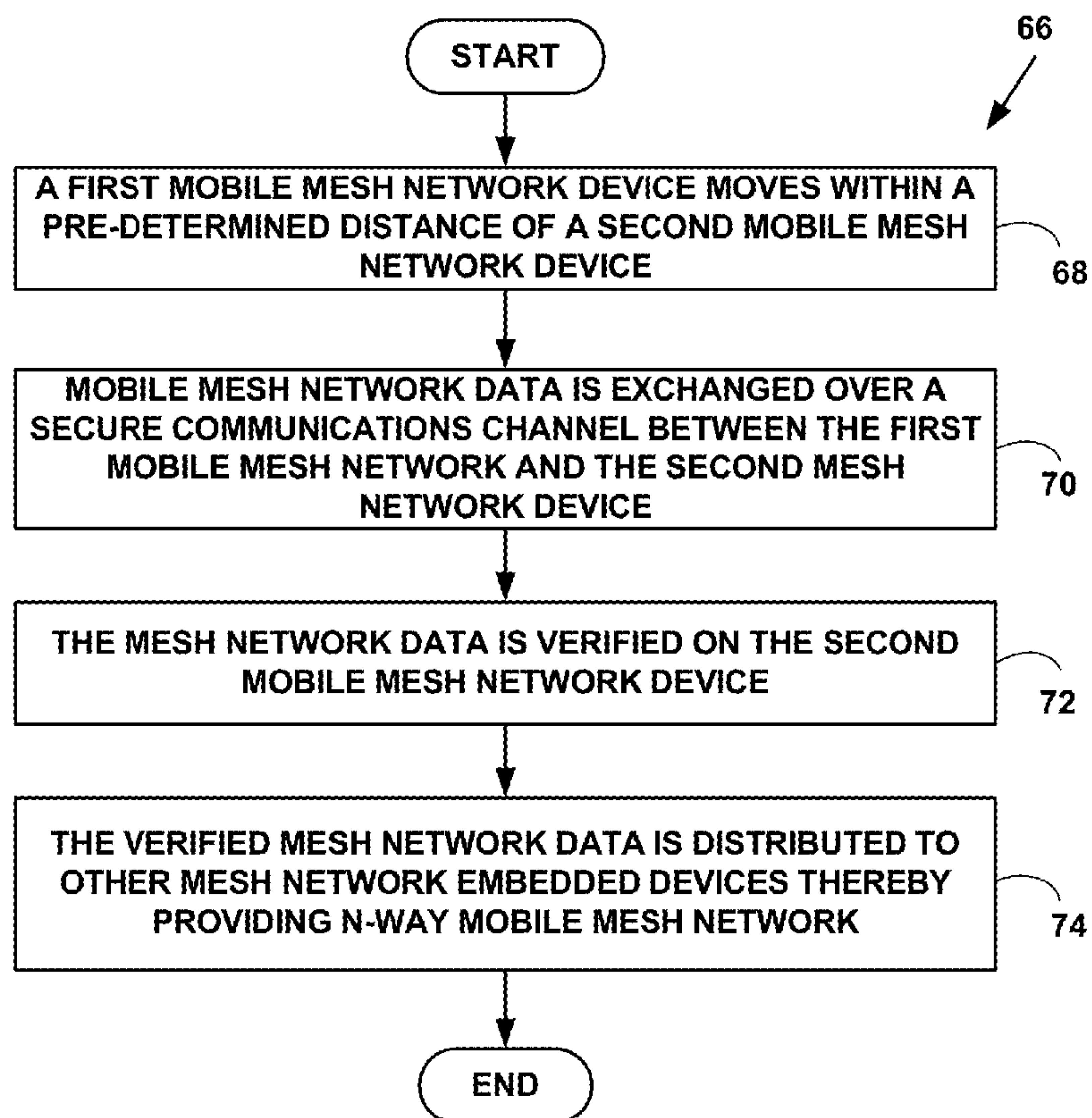
FIG. 4

FIG. 5

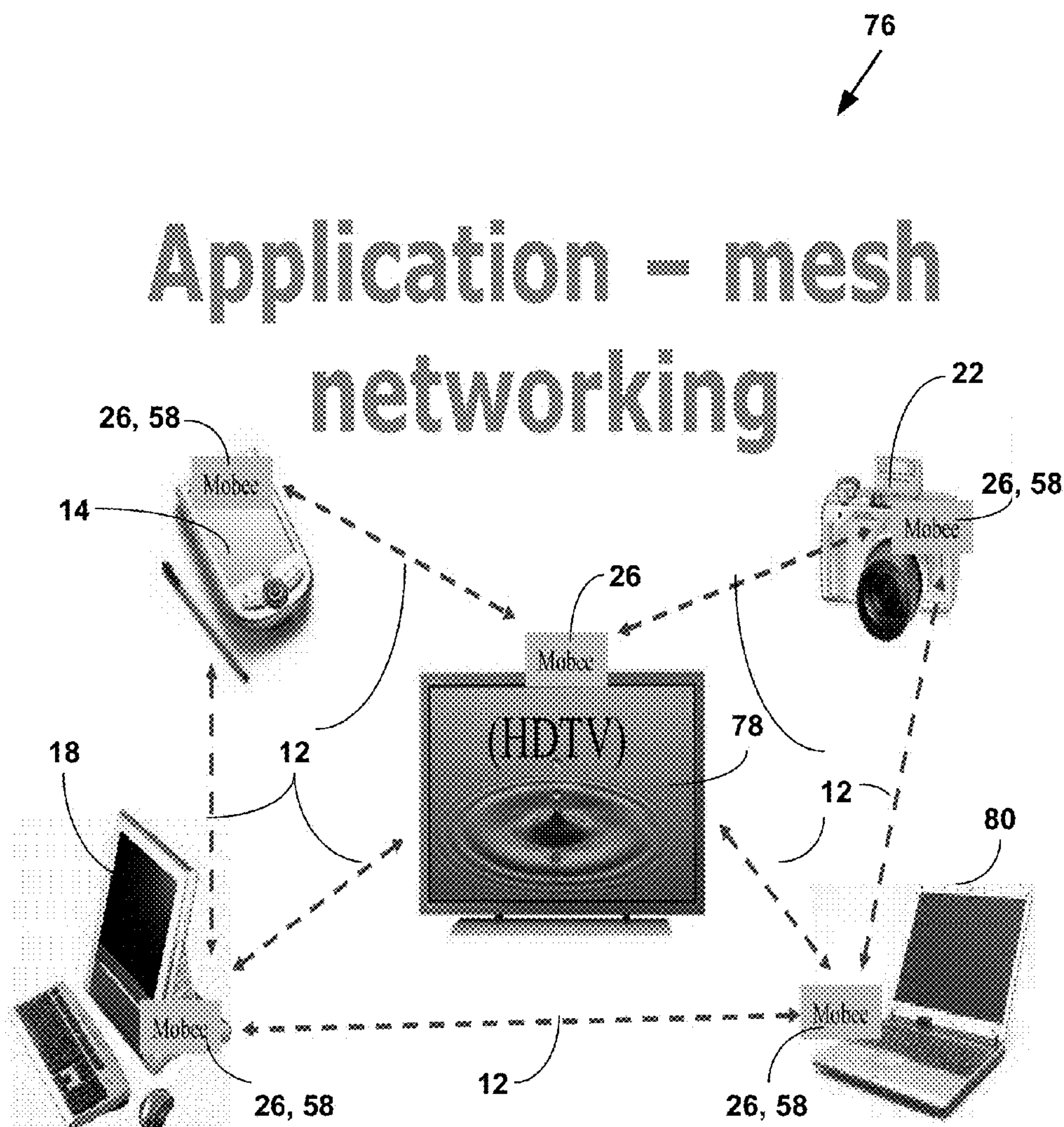


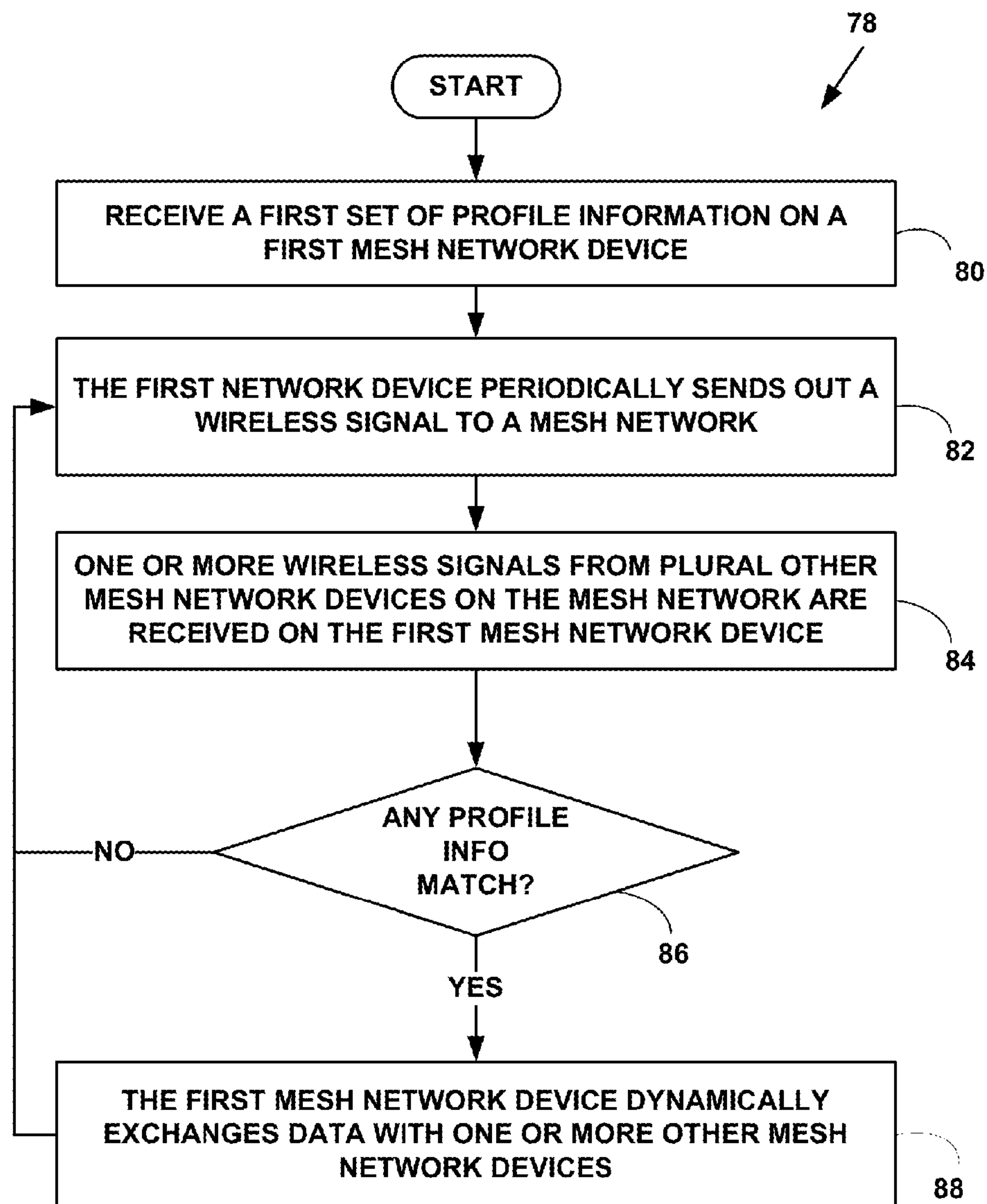
FIG. 6

FIG. 7

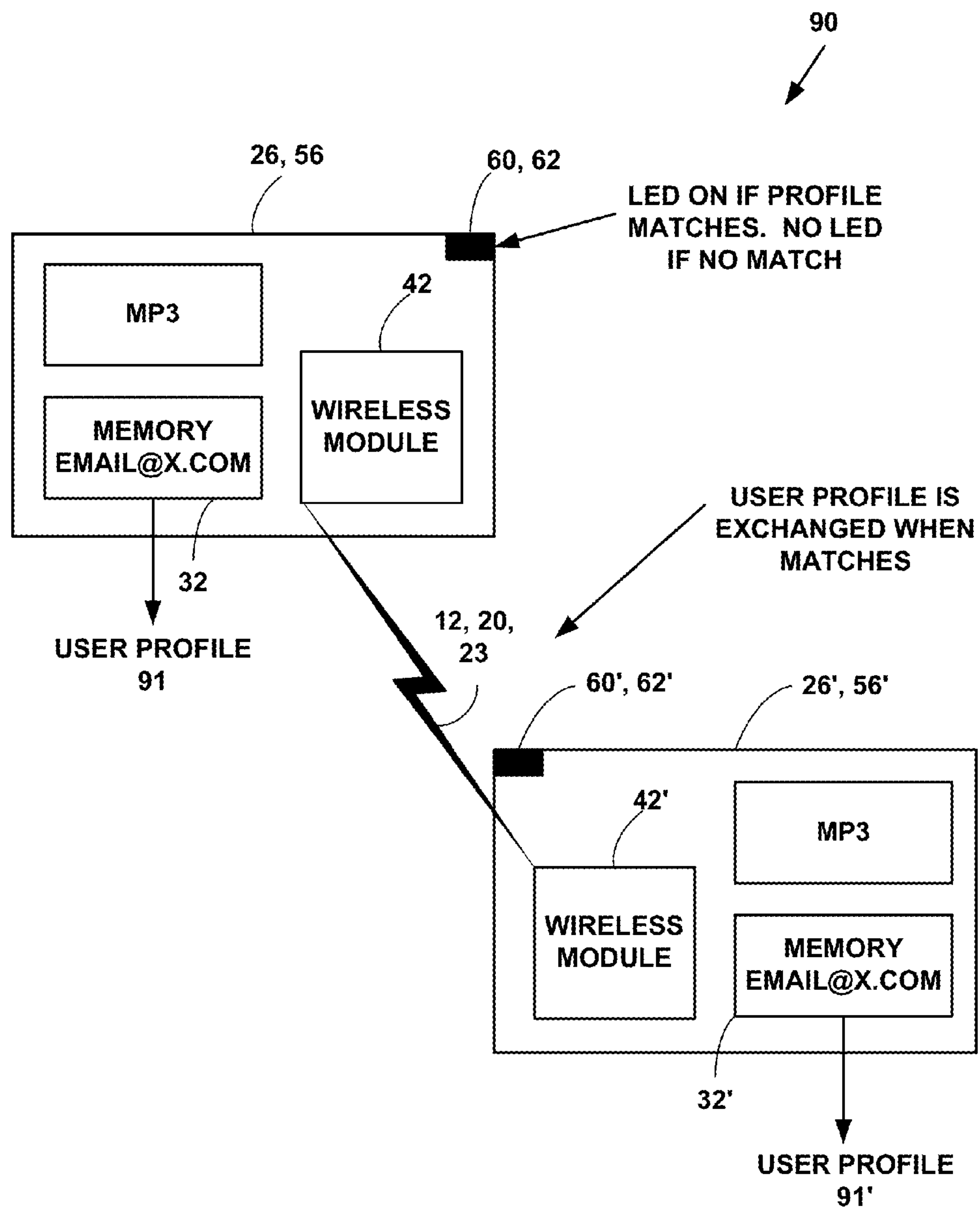


FIG. 8

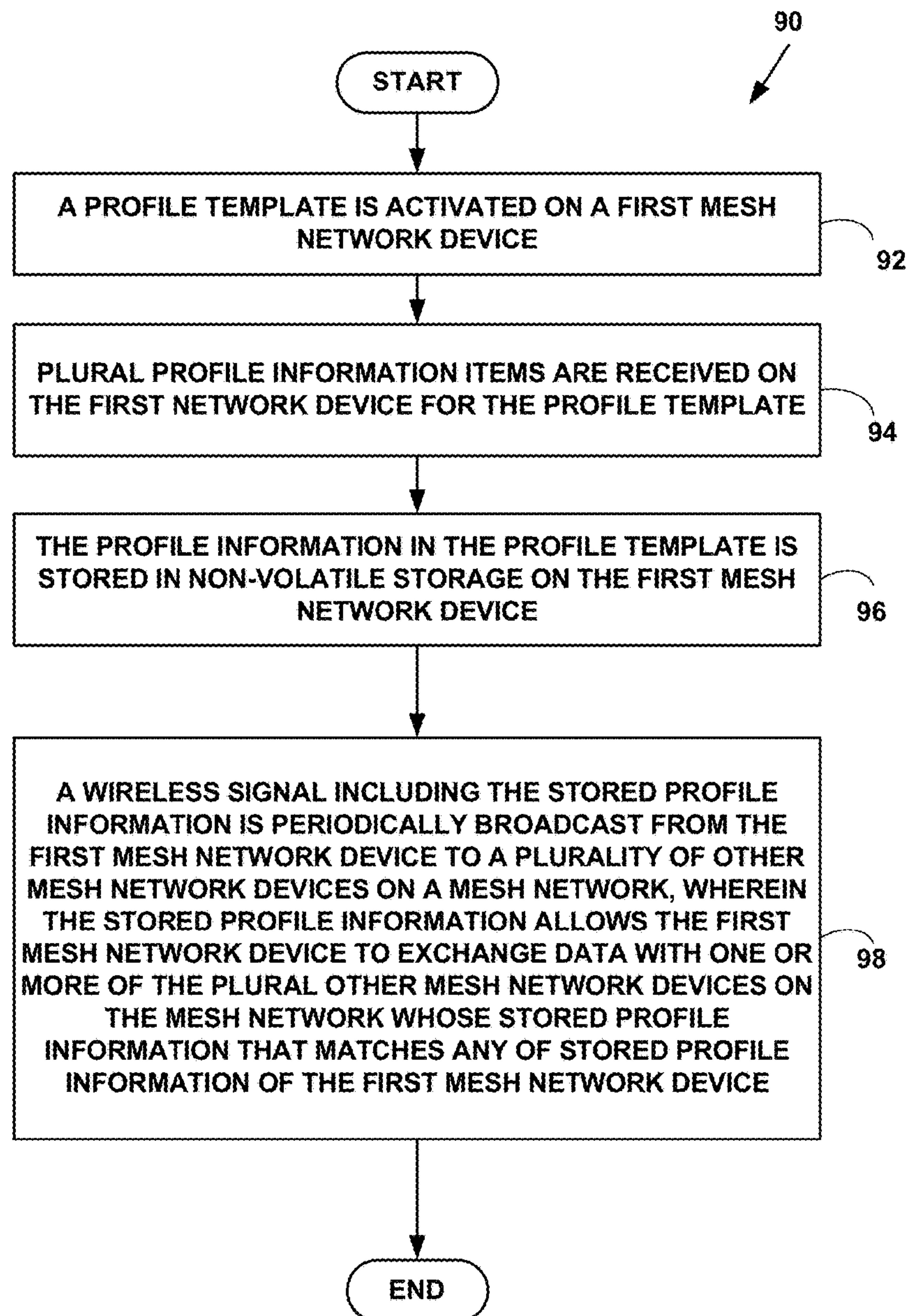


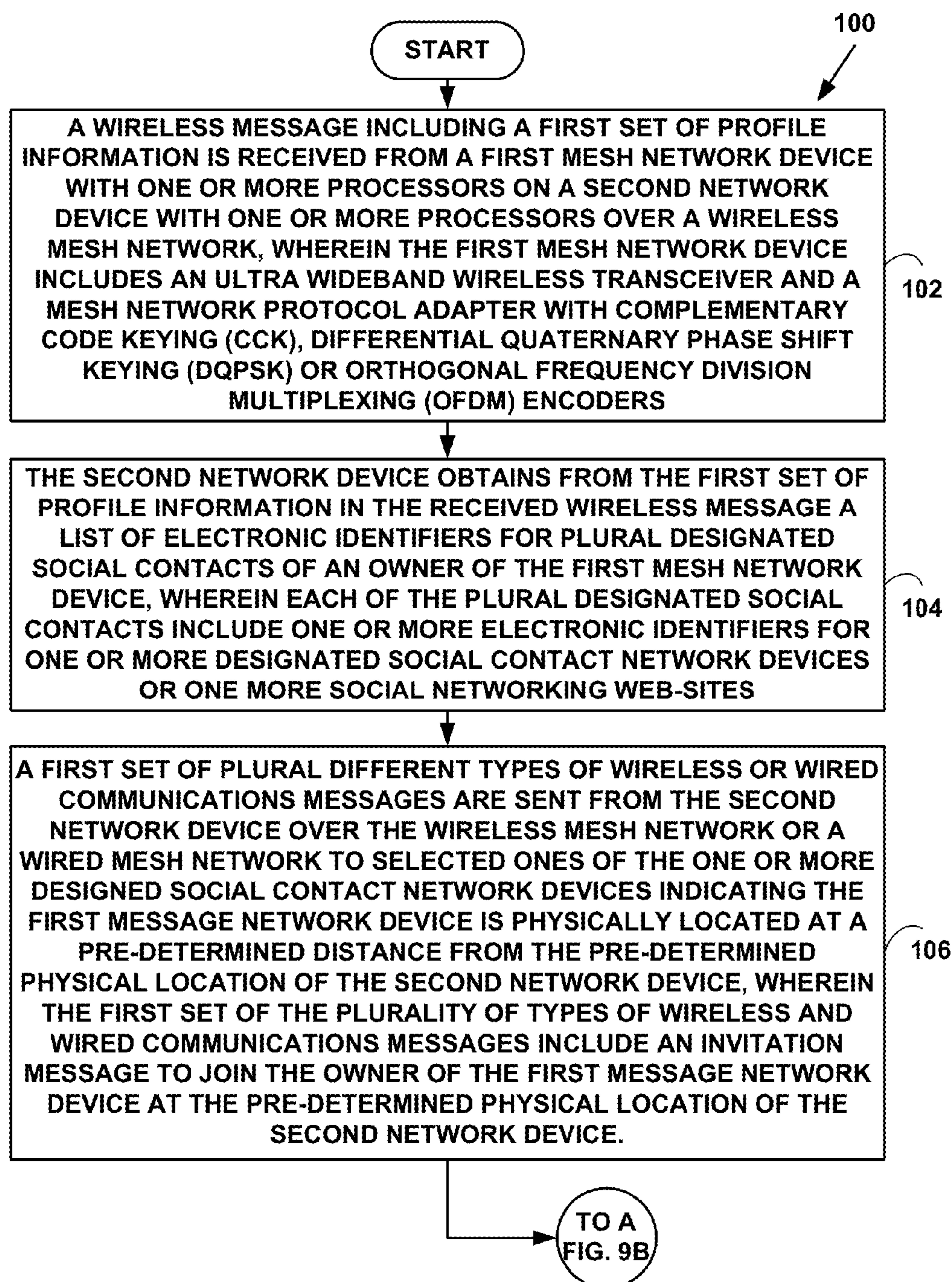
FIG. 9A

FIG. 9B

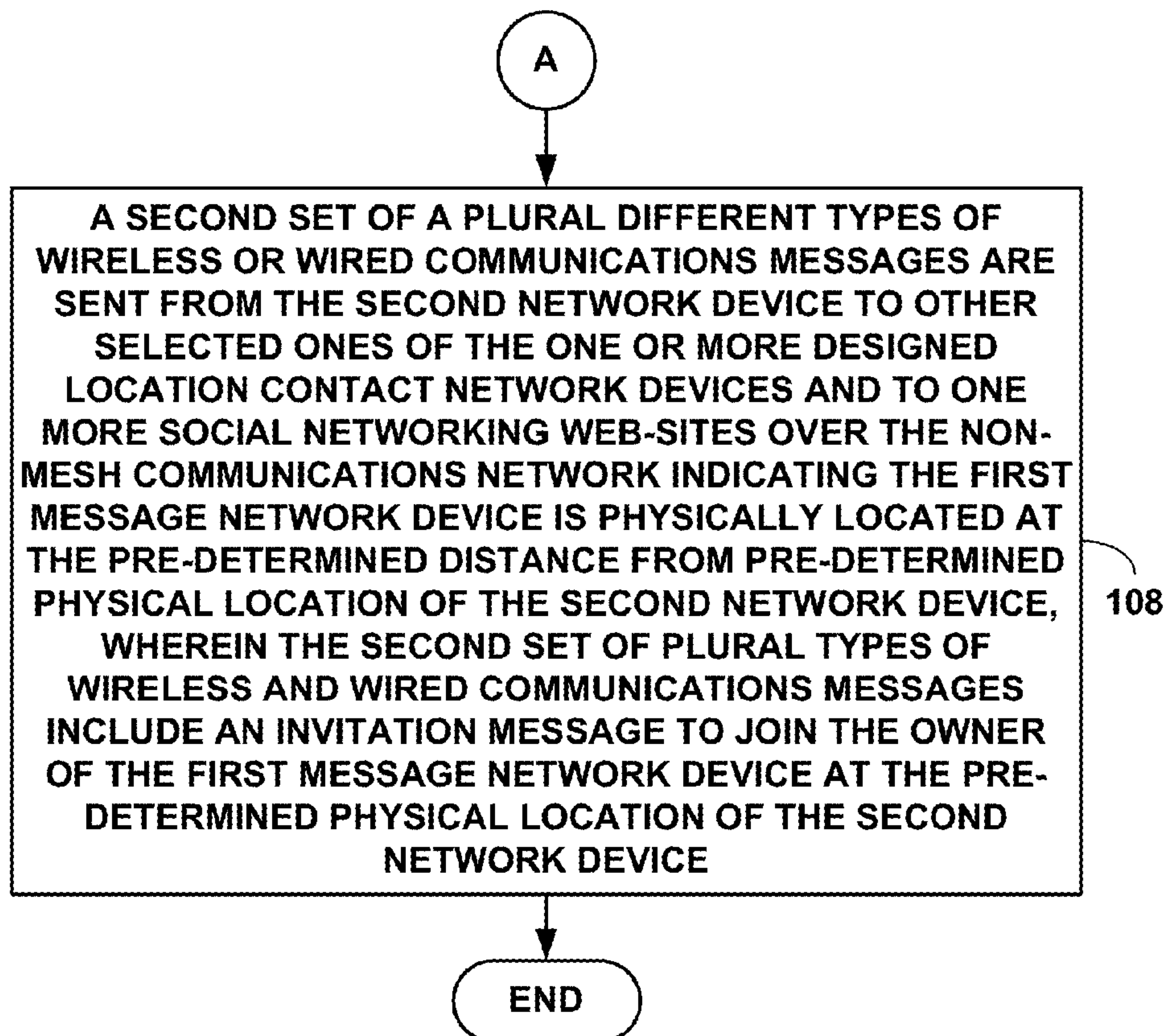


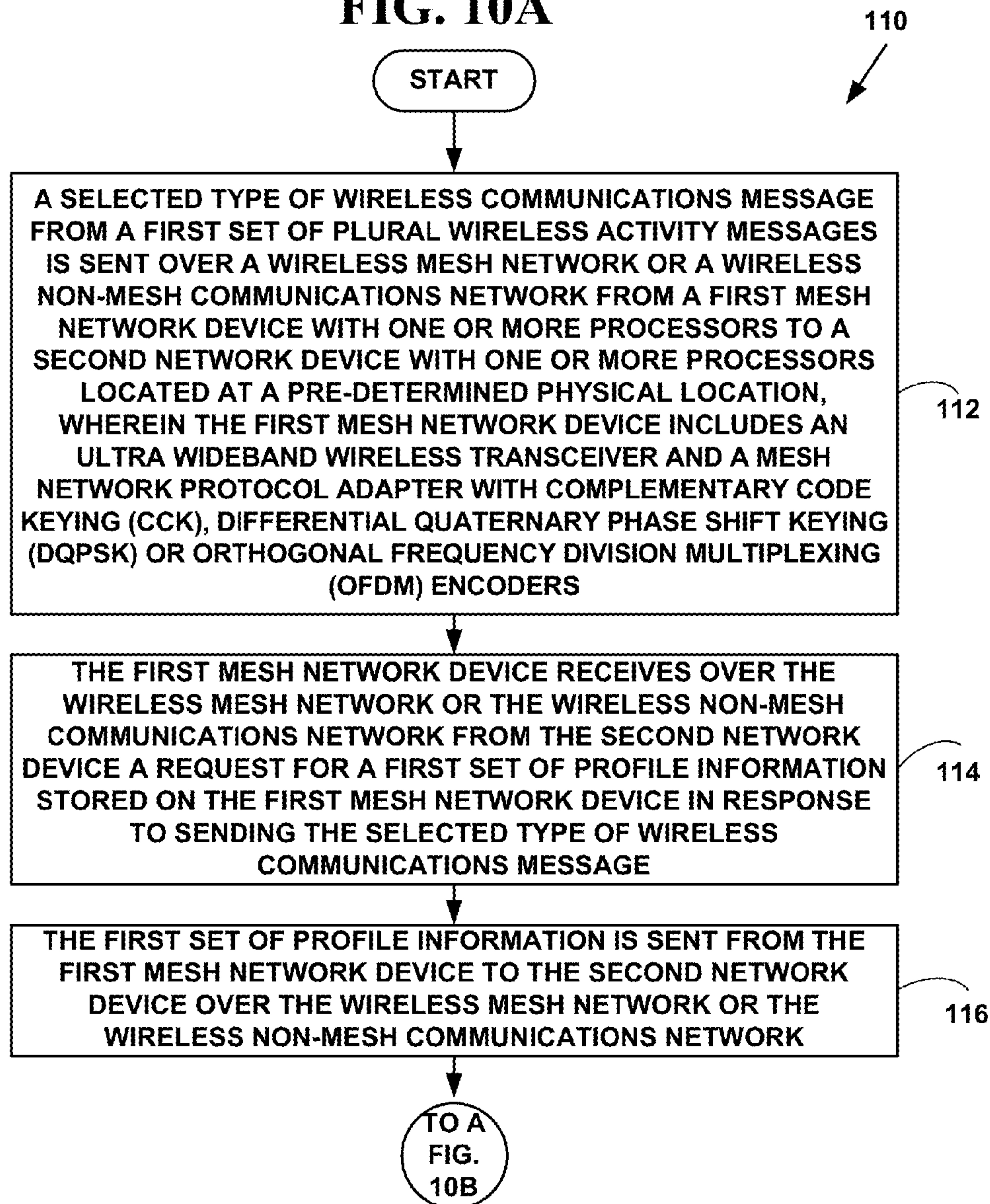
FIG. 10A

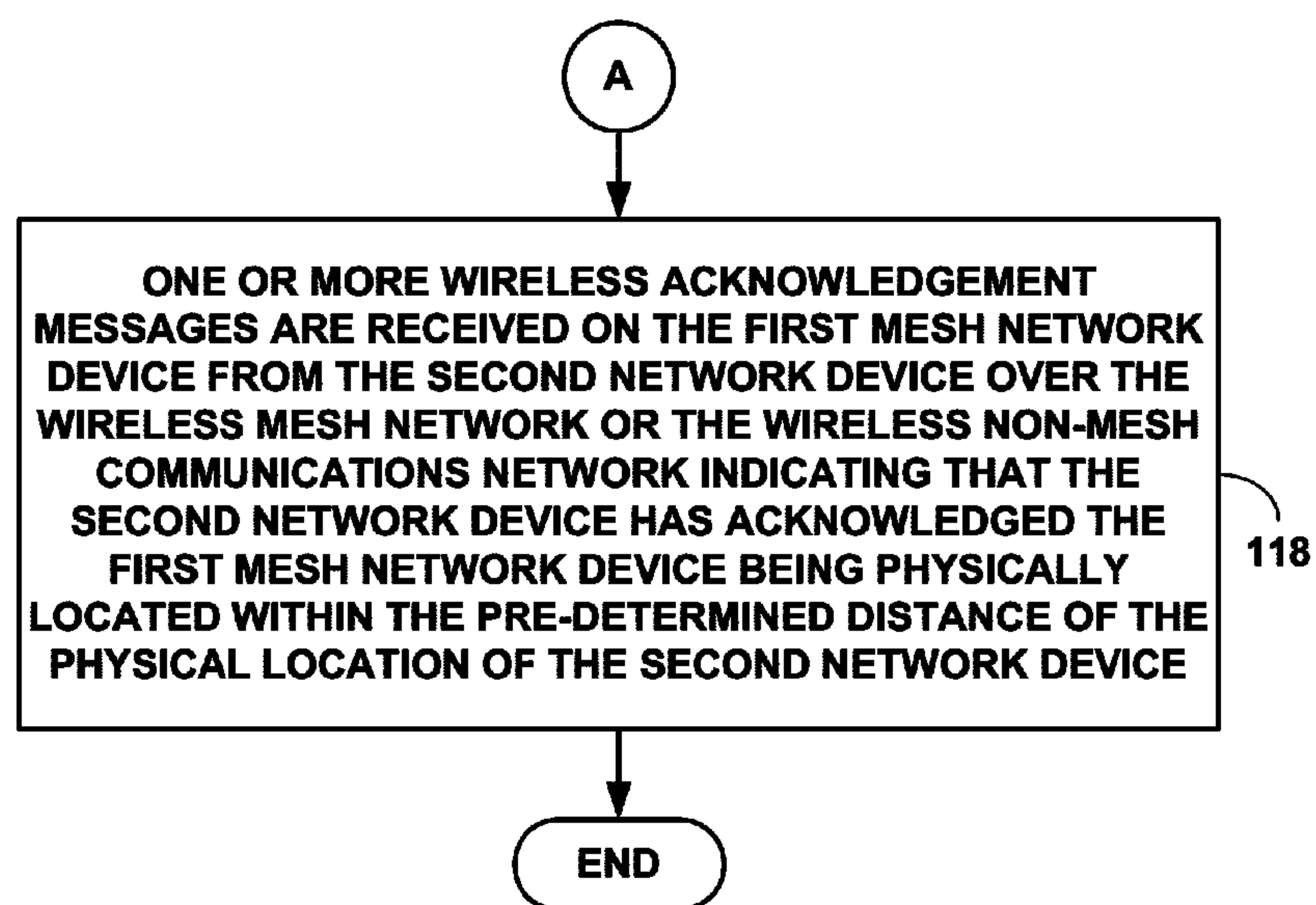
FIG. 10B

FIG. 11A

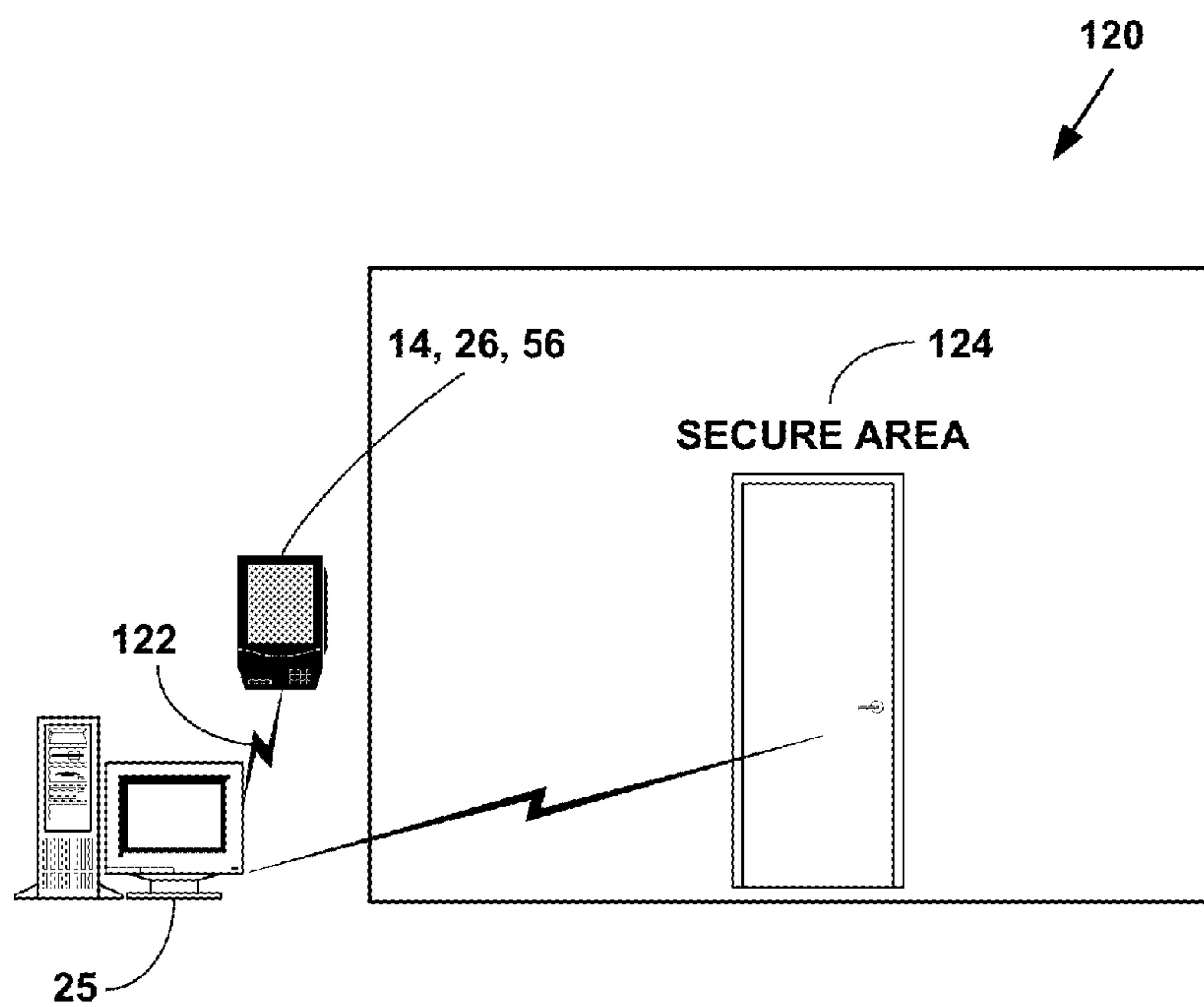


FIG. 11B

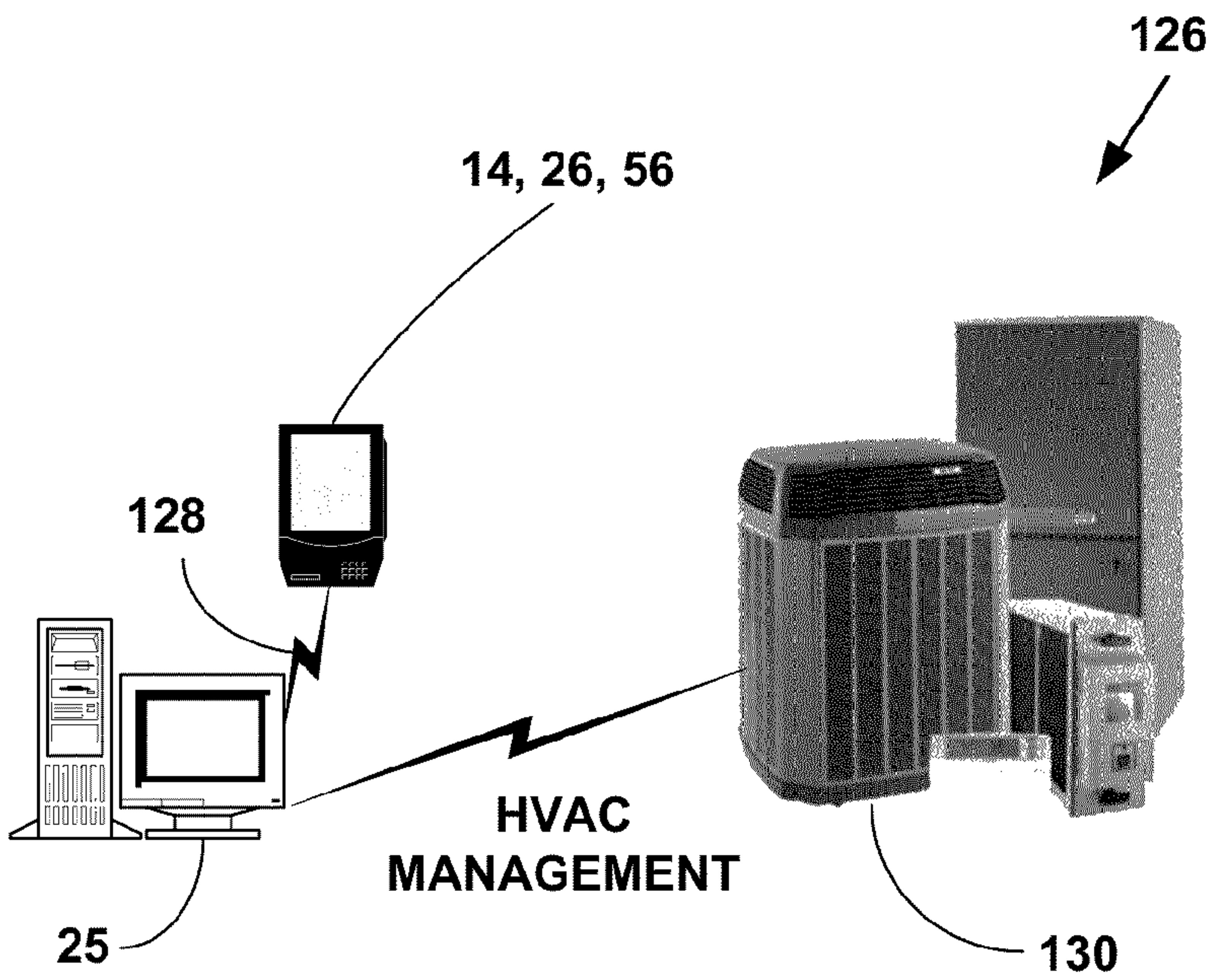


FIG. 11C

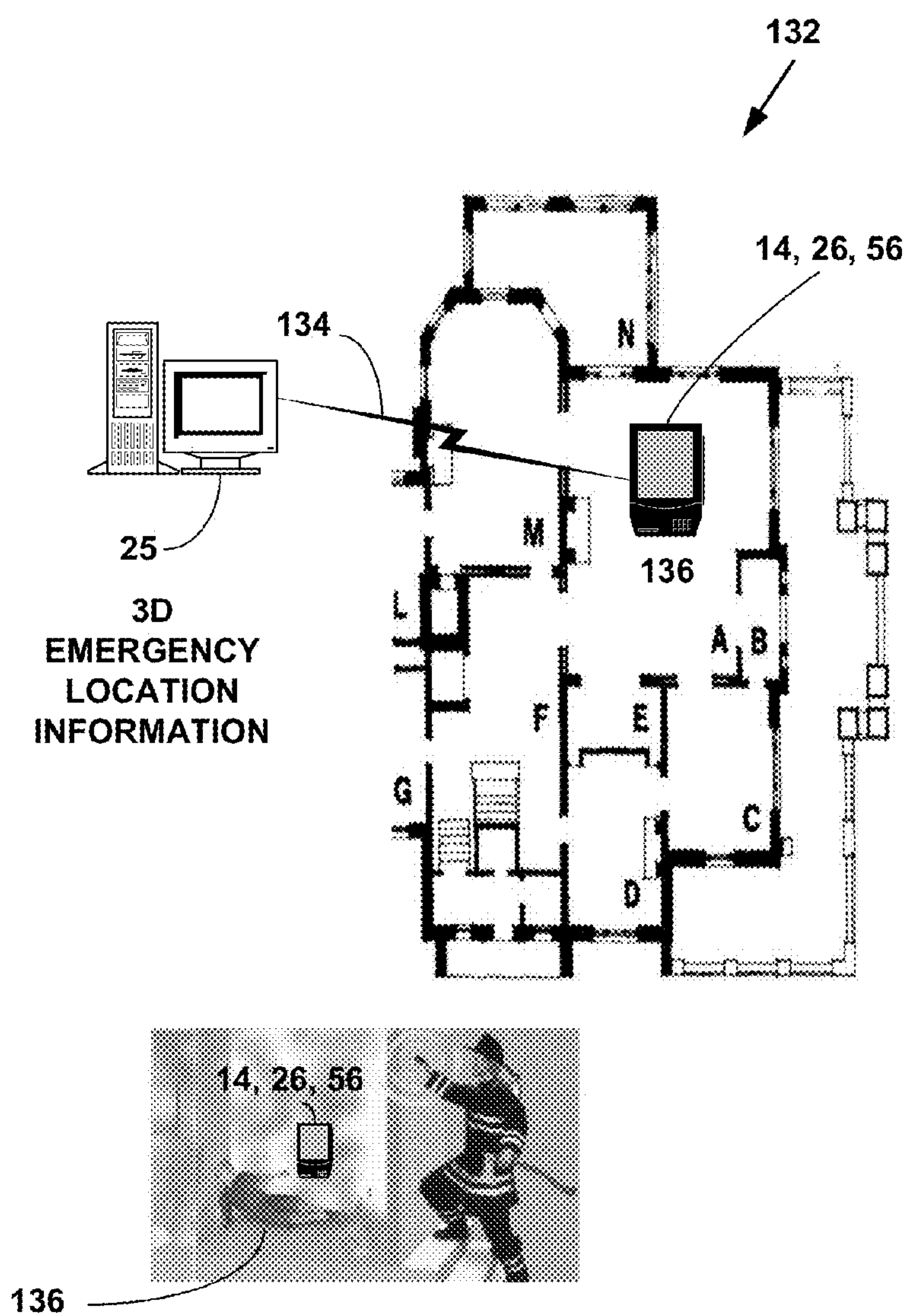


FIG. 12A

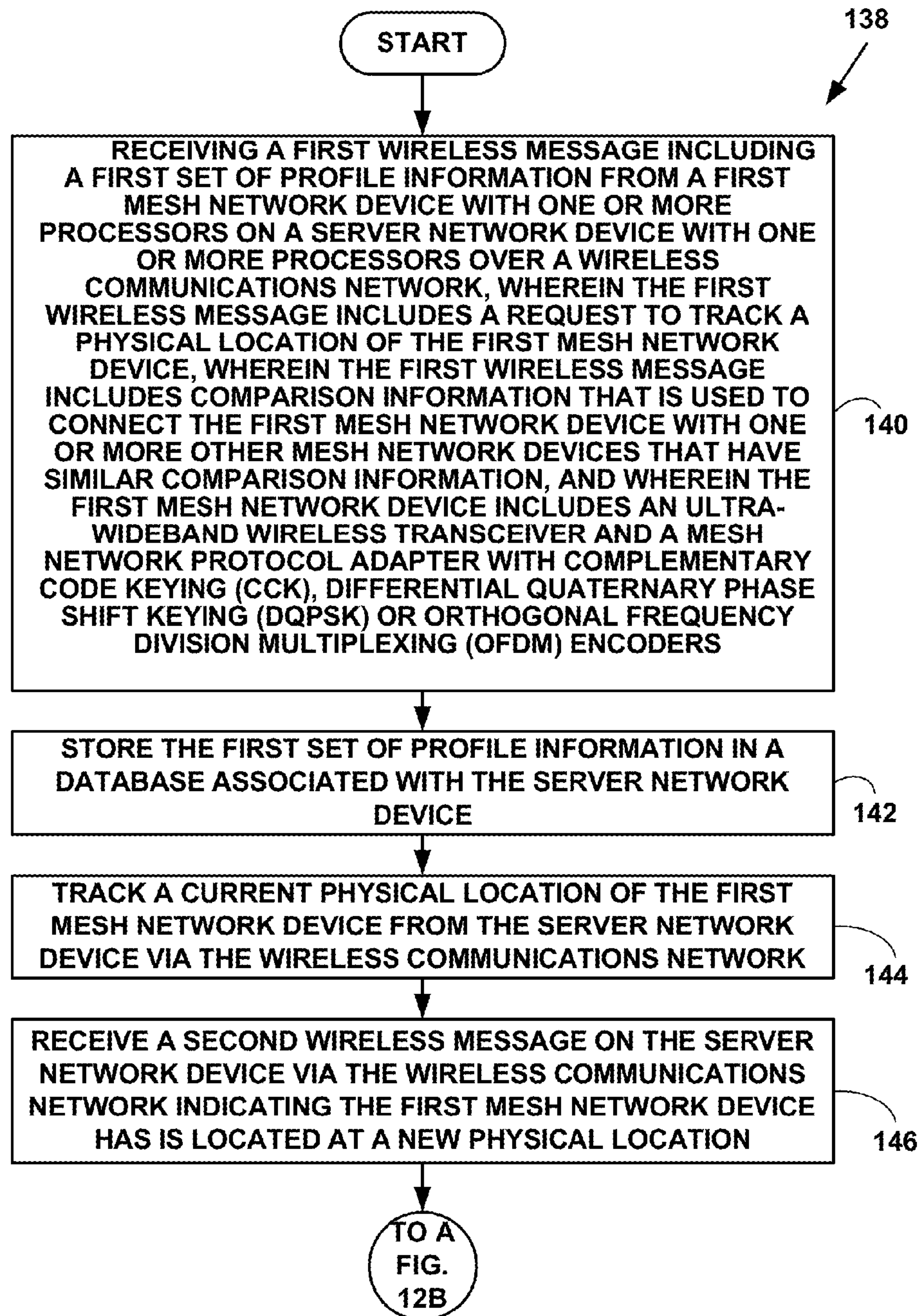


FIG. 12B

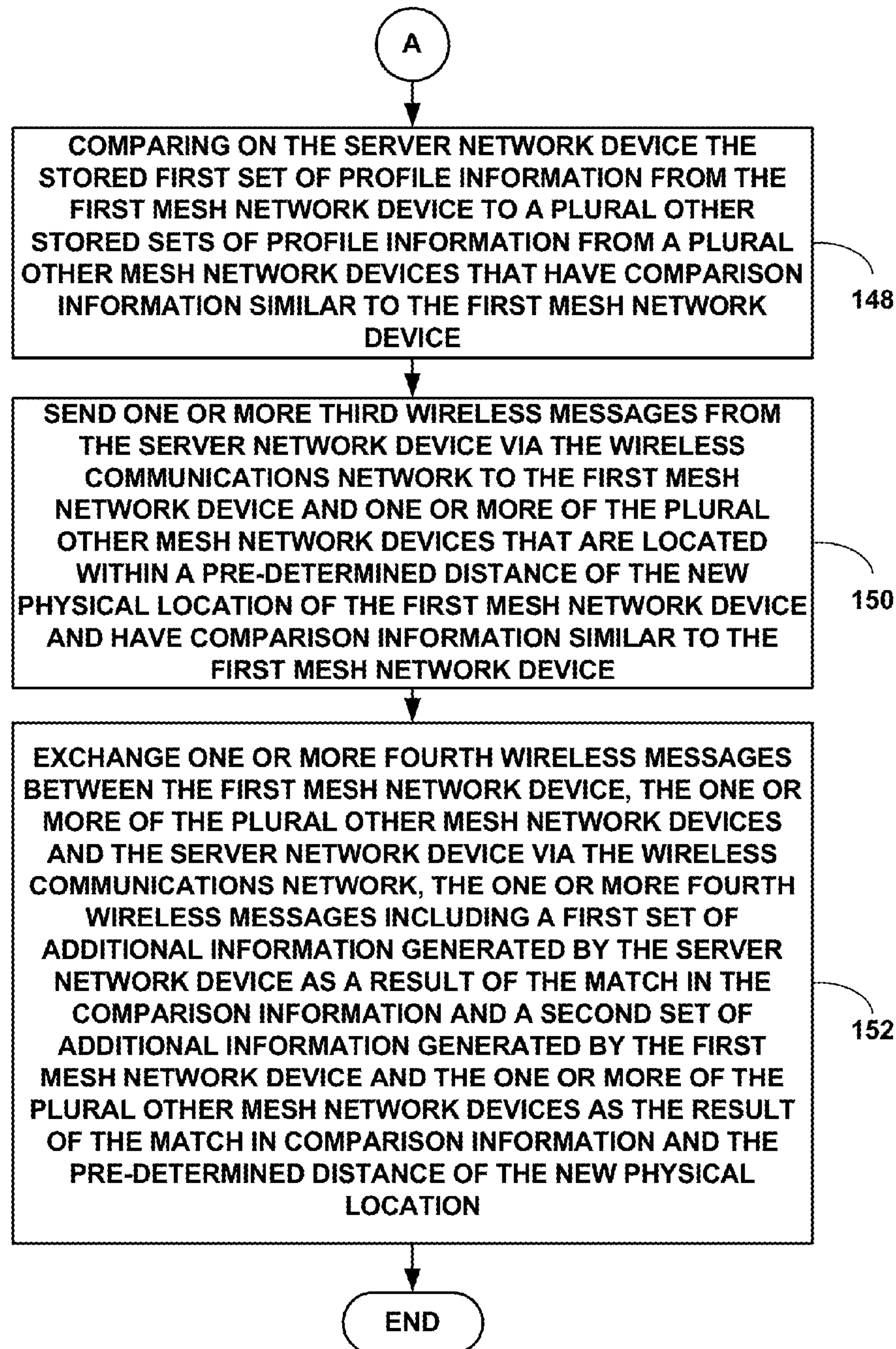


FIG. 13

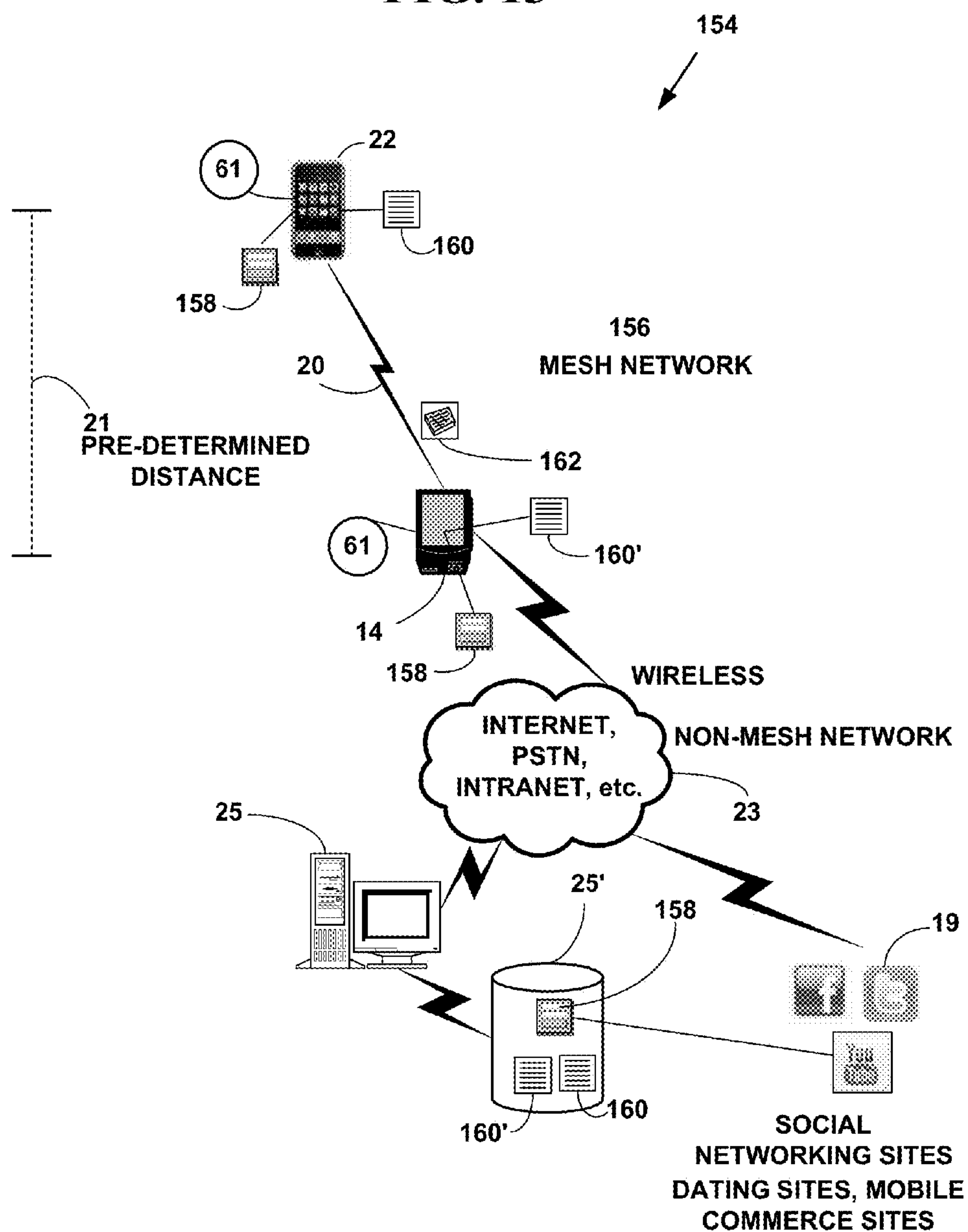
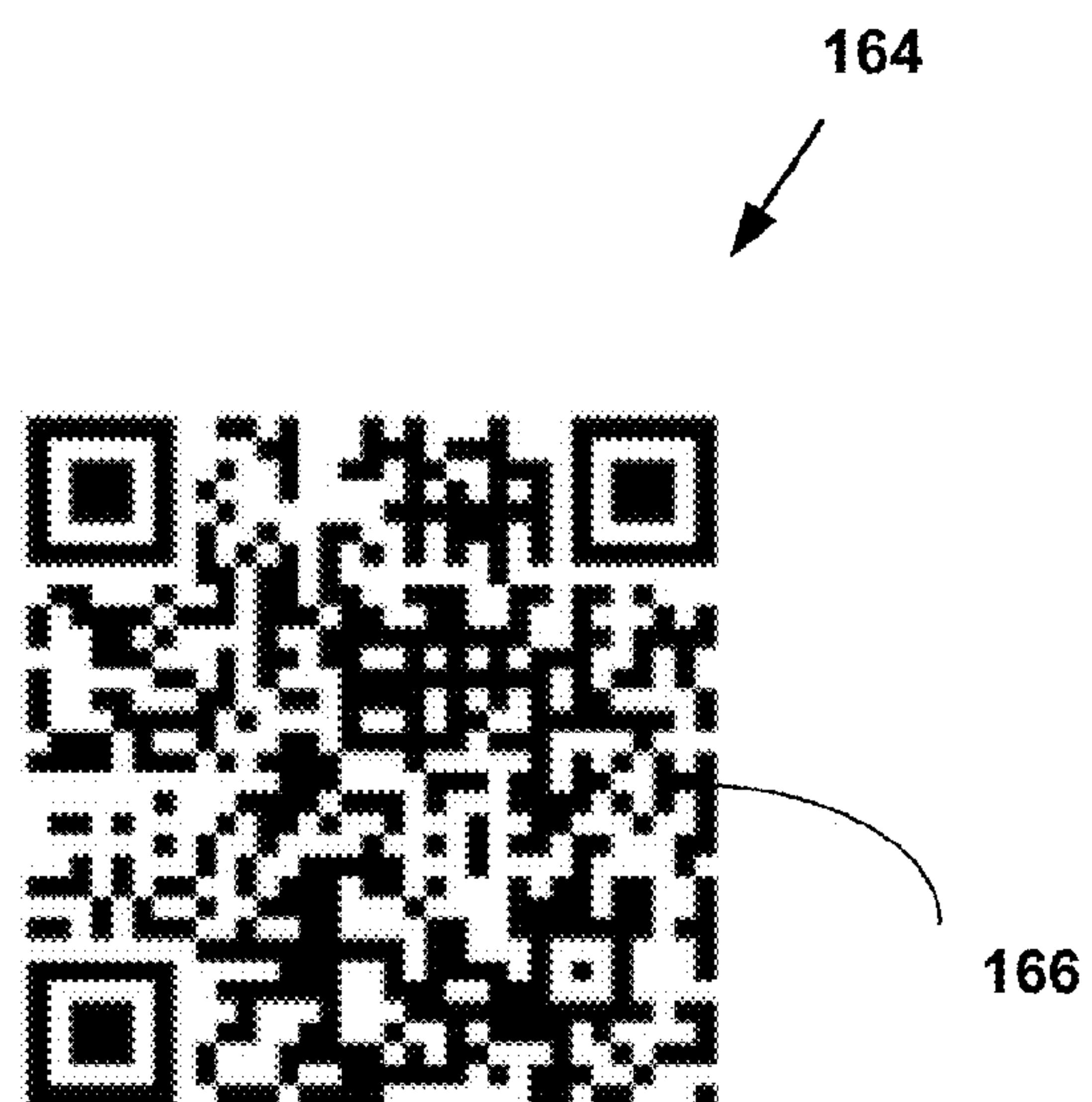


FIG. 14



QR Barcode

METHOD AND SYSTEM FOR DYNAMIC INFORMATION EXCHANGE ON LOCATION AWARE MESH NETWORK DEVICES

Matter enclosed in heavy brackets [] appears in the original patent but forms no part of this reissue specification; matter printed in italics indicates the additions made by reissue; a claim printed with strikethrough indicates that the claim was canceled, disclaimed, or held invalid by a prior post-patent action or proceeding.

CROSS REFERENCES TO RELATED APPLICATIONS

This application is a Continuation-In-Part (CIP) of Ser. No. 12/884,521, filed Sep. 17, 2010, that issued as U.S. Pat. No. 8,305,935, on Nov. 6, 2012, which is a CIP of U.S. utility patent application Ser. No. 11/880,271, filed Jul. 20, 2007, which issued as U.S. Pat. No. 7,801,058, on Sep. 21, 2010, utility patent application Ser. No. 11/880,271 claims priority to U.S. Provisional Patent Application 60/833,741, filed Jul. 27, 2006, the contents of all which are incorporated by reference.

FIELD OF THE INVENTION

This invention relates to mesh networks. More specifically, it relates to a method and system for dynamic information exchange on location aware mesh network devices.

BACKGROUND OF THE INVENTION

There are many types of computer and communications networks in existence. One variety of such networks is a mesh network.

A mesh network is a self-organizing network built from plural mesh network nodes that may spontaneously create an impromptu network, assemble the network themselves, dynamically adapt to device failure and degradation, manage movement of mesh network nodes, and react to changes in task and network requirements. The plural mesh network nodes are reconfigurable smart network nodes that are self-aware, self-reconfigurable and autonomous.

A mesh network is a network that employs one of two connection arrangements, "full mesh" topology or "partial mesh" topology. In the full mesh topology, each node is connected directly to each of the others. In the partial mesh topology, nodes are connected to only some, not all, of the other nodes.

There are a number of problems associated with wired and wireless mesh networks. One problem is that a number of independent mesh devices each make a local decision and then try to combine these decisions at a central point to generate a global decision. Routing, bandwidth, and power constraints determine the quality of the distributed detection and/or estimation decision. Another problem is that is often difficult to determine a load on a mesh network and what resources are required to determine a desired quality of service.

Another problem is that some mesh networks are mobile networks in which it is assumed at least some of the nodes of the network are mobile units that change position over time. The dynamic management of complex routing information is very difficult. Mobile sensor networks include plural client units in such as a personal digital/data assistant

(PDA), mobile phone, or other mobile unit for airport lounges, shopping malls, offices, etc.

There have been attempts to solve some of the problems associated with mesh networks. For example, U.S. Pat. No. 6,785,725 entitled "Signaling address resolution in a communication network," that issued to Ramanan teaches "a network configuration and method provide communication setup between neighbor nodes in a communication network, without broadcasting this setup information over the network. A signaling bandwidth separated from the data communication channel bandwidth facilitates address resolution over a common transmission medium. The user is not required to know any physical address properties of the neighbor nodes. This reduces the complexity of the information that a network administrator is required to manage. This processing feeds into a complete address resolution table, which is employed for controlling network communication over the main data communication channel bandwidth. Typically, substantially continuous transmission and/or reception over the signaling bandwidth is useful not only to determine the neighbor node's active address upon startup, but also while the network is running, to detect if a signaling element has been exchanged or has changed activity. The address resolution is automatically updated to reflect a new configuration."

U.S. Published Patent Application No. 20050272430 entitled "Reconfigurable micro-mesh communication system," that was published by Griebeling teaches "wide area wireless networks with high network throughput and low provisioning and maintenance costs. The wireless networks comprise a distributed reconfigurable micro-mesh cluster having direct wireless link capability. Multiple channels operating at different frequencies can be used per direct wireless link. To further reduce the provisioning and maintenance costs, narrow beam antennas are used at the point of presence. To expand the wide area wireless networks into the home market, adjustable antennas are installed at homes."

U.S. Published Patent Application No. 20050243765 entitled "Mesh network and piconet work system and method" that was published by Schrader et al. teaches "a method of distributed control of a wireless mesh network without knowledge of global topology. The method includes: a station joining the network with any current member by propagating the join-request, or two meshes merging using the steps of: one mesh joining the other as a whole and then re-synchronizing its timing. The method further includes: first, each station periodically transmits a beacon; second, in response to a beacon being no longer detected, a station transmitting a bitmap of stations that it can still receive; third, each station responds by adding stations that it can receive with all of the bitmaps received from other members, and retransmitting the updated bitmap; fourth, after time for all stations to respond, all stations base current membership on the bitmap. The method further includes: determining sharable time slots that will not interfere with neighbors or other slot sharers, using and then releasing those slots."

U.S. Published Patent Application No. 20050190778 entitled "Multi-system mesh network," that was published by Ozluturk teaches "a transmission is simultaneously provided on multiple mesh networks. Retransmission between two nodes may be performed for the same communication along multiple networks in a mesh topography for the multiple networks. This permits communication to be effected in a mesh topography where one or all systems would not be able to provide a complete network connection within any given system."

3

U.S. Published Patent Application No. 20050074019 entitled “method and apparatus for providing mobile inter-mesh communication points in a multi-level wireless mesh network,” that was published by Handforth et al. teaches “a mobile backhaul inter-mesh communication point forms an interface between a wireless mesh network on a first level and a wireless mesh network on a second, higher bandwidth, level. The two wireless networks are differentiated, e.g., by causing the mesh networks to be formed using different spectra, protocols or coding, or antennae. The mobile intra-mesh communication point functions as an access point in the lower level mesh network and as a relay point in the upper level mesh network. Utilizing mobile inter-mesh communication points facilitates deployment of wireless network access points while enabling the location of access points to follow the concentration of network users. Mobile inter-mesh communication points may be deployed in personal vehicles such as cars, trucks, and motorcycles, public transportation vehicles such as busses, trains, and aircraft, emergency vehicles such as fire trucks and ambulances, and many other types of vehicles.”

However, none of these solutions solve all of the problems associated with mesh networks. Thus, it would be desirable to solve some of the problems associated with mesh networks.

SUMMARY OF THE INVENTION

In accordance with preferred embodiments of the present invention, some of the problems associated with sensor networks are overcome. A method and system for dynamic information exchange on location aware mesh network devices is provided

Mobile location aware mesh network devices automatically exchange information with other mobile location aware devices that are located at a pre-determined distance of each other at a desired physical location. A server network device compares electronic profiles that include stated interests of the mobile location aware devices. The server network device also provides additional information based on stated interests in the electronic profiles of the mobile location aware network devices.

The foregoing and other features and advantages of preferred embodiments of the present invention will be more readily apparent from the following detailed description. The detailed description proceeds with references to the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

Preferred embodiments of the present invention are described with reference to the following drawings, wherein:

FIG. 1 is a block diagram of an exemplary mesh network;

FIG. 2 is a block diagram of an exemplary hardware architecture for an mesh network device;

FIG. 3A is a block diagram illustrating a specific exemplary implementation of the mesh network device of FIG. 2;

FIG. 3B is a block diagram illustrating a specific exemplary implementation of the mesh network device of FIG. 3A;

FIG. 4 is a flow diagram illustrating a method for mesh networking;

FIG. 5 is a block diagram illustrating an N-way mesh network formed using the mesh network device of FIG. 2; and

4

FIG. 6 is a flow diagram illustrating a method for dynamic information interchange for mesh network devices;

FIG. 7 is a block diagram illustrating a data flow for dynamic information interchange for mesh network devices;

FIG. 8 is a flow diagram illustrating a method for enabling dynamic information interchange for mesh network devices;

FIGS. 9A and 9B are a flow diagram illustrating a method for dynamic information interchange for location aware mesh network devices;

FIGS. 10A and 10B are a flow diagram illustrating a method for dynamic information interchange for location aware mesh network devices;

FIG. 11A is a block diagram illustrating a mesh activity message for entering a secure area;

FIG. 11B is a block diagram illustrating a mesh activity message for automatically and dynamically managing HVAC;

FIG. 11C is a block diagram illustrating a mesh activity message for providing 3D emergency location information;

FIGS. 12A and 12B are a flow diagram illustrating a method for dynamic information exchange for location aware network devices;

FIG. 13 is a block diagram illustrating a data flow for the method of FIG. 12; and

FIG. 14 is a block diagram illustrating display of an exemplary QR barcode.

DETAILED DESCRIPTION OF THE INVENTION

Exemplary Mesh Network System

Mesh networking is a type of networking wherein each node in the mesh network may act as an independent gateway/router/switch, regardless of whether it is connected to another communications network or not. It allows for continuous connections, disconnections and reconfigurations until a desired destination is reached. Mesh networks differ from other communications networks (e.g., the Internet, an intranet, the Public Switch Telephone Network (PSTN), a data network (e.g., Transmission Control Protocol (TCP)/Internet Protocol (IP), etc.) in that component parts can all connect to each other via multiple hops. Mesh networks are also considered as one type of ad hoc network. Mesh networks are self-healing: the network can still operate when one node breaks down or a connection goes bad. As a result, the network may typically be very reliable, as there is often more than one path between a source and a destination in the network.

One advantage of wireless mesh networks—as opposed to wired or fixed wireless non-mesh networks—is that they are truly wireless. Most traditional “wireless” access points still need to be wired to another non-mesh communications network to broadcast their wireless signal. For large wireless communications network wire cables need to be buried in ceilings and walls and throughout public areas. In a wireless mesh network, only one mesh node needs to be physically wired to a network connection like a DSL or cable modem. That one wired node then shares its Internet connection wirelessly with all other mesh nodes in its vicinity. Those mesh nodes then share the connection wirelessly with the nodes closest to them. The more nodes, the further the connection spreads, creating a wireless mesh “cloud of connectivity” that can serve a small area or a city of millions.

FIG. 1 is a block diagram of an exemplary mesh network 10. A mesh network is a short range local area network (LAN) that employs one of two connection arrangements,

5

“full mesh topology” or “partial mesh topology.” In the full mesh topology **12**, each node is a mesh network device **14**, **16**, **18** is connected directly to each of the other mesh network device. In the partial mesh topology **20** some mesh network devices **22** are connected to all the others, but some of the mesh network devices **22** are connected only to those other mesh network devices **18** with which they exchange the most data. The connections can be wired or wireless in a mesh network **12** or partial mesh **20** network topologies. A mesh network is reliable and offers redundancy. If one mesh node can no longer operate, all the rest can still communicate with each other, directly or through one or more intermediate nodes. Mesh networks work well when the nodes are located at scattered points that do not lie near a common line. The mesh network **12** and the partial mesh network **20** includes both wireless **3** and wired mesh networks **5** and wireless **3** and wired partial mesh networks **5**.

Some characteristics for mesh networks **12** or partial-mesh networks **20** include a network infrastructure that is decentralized, avoids a central point of failure and control, is cost effective and be maintained and expanded locally. A mesh network **12** or partial mesh network **20** includes many-to-many connections and is capable of dynamically updating and optimizing these connections. The mesh networks **12** or partial-mesh networks **20** include “mobile mesh networks” in which it is assumed that one or more of the mesh network devices dynamically change geographical location over time. Such mesh network devices may continuously change geographical location over time.

The mesh networks **12**, **20** may also include embedded mesh network devices that form an “embedded mesh network.” An embedded mesh network is typically a component of a larger more complex mesh network. Industrial machines, automobiles, medical equipment, cameras, household appliances, airplanes, vending machines, toys, etc. typically include embedded mesh networks. For example, an automobile may include a first embedded mesh network for anti-lock braking, a second for monitoring and maintaining oil pressure, etc. An embedded mesh network is designed to run on its own without intervention, responds to events (e.g., data collection, data transfer, etc.) in-real time and provides data to the larger more complex network.

The plural mesh network devices **14**, **16**, **18**, **22** include, but are not limited to, multimedia capable desktop and laptop computers, facsimile machines, mobile phones, non-mobile phones, tablet computers (e.g., IPAD by APPLE, etc.) Internet phones, Internet appliances, personal digital/data assistants (PDA), two-way pagers, digital cameras, cable television set-top boxes, digital televisions including high definition television (HDTV) and other types of network devices. The plural mesh network devices **14**, **16**, **18**, **22** also include embedded mesh network devices.

The plural mesh network devices **14**, **16**, **18**, **22** may also include mesh network tags and/or sensors and/or biometrics. A mesh network sensor is a device that receives and responds to a signal or stimulus. For example a mesh network sensor may be used to measure a physical quantity such as temperature, pressure, sound, etc. and convert it into an electronic signal (e.g., digital data, digital signal, etc.). A mesh network sensor may also measure an electrical quantity (e.g., a radio signal, Radio Frequency IDentification signal (RFID) signal, etc.) and convert it into another electronic signal.

As is known in the art, an “RFID tag” is an object that can be applied to or incorporated into a product, animal, or person for the purpose of identification and/or tracking using RF signals.

6

As is known in the art, an “RFID sensor” is a device that measures a physical quantity and converts it into an RF signal which can be read by an observer or by an instrument (e.g., RFID controller/RFID portal server network device, etc.)

As is known in the art, a “biometric” is method for uniquely recognizing humans or non-human entities based upon one or more intrinsic physical or behavioral traits. Thus, an RFID biometric tag is an object that can be applied to or incorporated on or into a human or animal for the purpose of identification.

The plural mesh network devices **14**, **16**, **18**, **22** may be used for unique identity identification via voice, biometrics, supply chain management, medical, for Data, Information and Knowledge (DIaK) sensors and sensor tracking extended services such as those used as part of capabilities offered by Integrated Systems Health Management (ISHM) and for other applications.

The architecture plural mesh network devices **14**, **16**, **18**, **22** brings a rich set of state-of-the-art capabilities to support ISHM systems for sensing, processing, control, and distribution. Such devices enable a mesh network, a mesh sensor network or other sensor network to significantly to increase capabilities for improved identification and tracking, data sharing, information dissemination, online data processing, automated feature extraction, data fusion, and parallel and distributed computing functions.

In one embodiment, the mesh network sensor is a simple device that includes an electrical circuit and a wired or wireless transceiver. In another embodiment, the mesh network sensor is a complex device (e.g., computer, PDA, mobile phone, etc.) including additional sensor functionality.

The plural network devices **14**, **16**, **18**, **22** include one or more of a wired interface and/or a wireless interface used to connect to a mesh network **12** or partial mesh network **20** to provide voice, video and data communications.

The plural network devices **14**, **16**, **18**, **22** include one or more of a wired interface and/or a wireless interface used to connect to non-mesh communications network **23** to provide voice, video and data communications such as the Internet, an intranet, the Public Switch Telephone Network (PSTN), etc. The non-mesh network communications network **23** has a non-mesh architecture based on the Open System Interconnection (OSI) model, Internet Protocol suite model, or other conventional non-mesh networking models.

The non-mesh communications network **23** may include one or more gateways, routers, bridges or switches As is known in the art, a gateway connects computer networks using different network protocols and/or operating at different transmission capacities. A router receives transmitted messages and forwards them to their correct destinations over the most efficient available route. A bridge is a device that connects networks using the same communications protocols so that information can be passed from one network device to another. A switch is a device that connects communications paths for voice, video and data streams.

The non-mesh communications network **23** may include one or more server network devices **25** (one of which is illustrated) and one or more web-sites accessible by users to send and receive information. The one or more servers **25**, may also include one or more associated databases **25'** for storing electronic information.

Preferred embodiments of the present invention include mesh network devices, non-mesh network devices and wired and wireless interfaces that are compliant with all or part of standards proposed by the Institute of Electrical and Elec-

tronic Engineers (IEEE), International Telecommunications Union-Telecommunication Standardization Sector (ITU), European Telecommunications Standards Institute (ETSI), Internet Engineering Task Force (IETF), U.S. National Institute of Security Technology (NIST), American National Standard Institute (ANSI), Wireless Application Protocol (WAP) Forum, Bluetooth Forum, or the ADSL Forum. However, network devices based on other standards could also be used.

An operating environment for devices and interfaces of the present invention include a processing system with one or more high speed Central Processing Unit(s) (CPU) or other processors and a memory. In accordance with the practices of persons skilled in the art of computer programming, the present invention is described below with reference to acts and symbolic representations of operations or instructions that are performed by the processing system, unless indicated otherwise. Such acts and operations or instructions are referred to as being "computer-executed," "CPU executed" or "processor executed."

It will be appreciated that acts and symbolically represented operations or instructions include the manipulation of electrical signals by the CPU. An electrical system represents data bits which cause a resulting transformation or reduction of the electrical signals, and the maintenance of data bits at memory locations in a memory system to thereby reconfigure or otherwise alter the CPU's operation, as well as other processing of signals. The memory locations where data bits are maintained are physical locations that have particular electrical, magnetic, optical, or organic properties corresponding to the data bits.

The data bits may also be maintained on a computer readable medium including magnetic disks, optical disks, organic memory, and any other volatile (e.g., Random Access Memory (RAM)) or non-volatile (e.g., Read-Only Memory (ROM)) mass storage system readable by the CPU. The computer readable medium includes cooperating or interconnected computer readable medium, which exist exclusively on the processing system or be distributed among multiple interconnected processing systems that may be local or remote to the processing system.

As is known in the art, the Open Systems Interconnection (OSI) reference model is a layered architecture that standardizes levels of service and types of interaction for computers exchanging information through a communications network. The OSI reference model separates network device-to-network device communications into seven protocol layers, or levels, each building—and relying—upon the standards contained in the levels below it. The OSI reference model includes from lowest-to-highest, a physical, data-link, network, transport, session, presentation and application layer. The lowest of the seven layers deals solely with hardware links; the highest deals with software interactions at the application-program level.

In one embodiment of the present invention, the wired and wireless interfaces include wired and wireless interfaces and corresponding networking protocols for wired connections to the non-mesh communications network 23 including, a Public Switched Telephone Network (PSTN) or a cable television network (CATV) including HDTV that connect the network devices 14, 16, 18, 22 via one or more twisted pairs of copper wires, digital subscriber lines (e.g. DSL, ADSL, VDSL, etc.) coaxial cable, fiber optic cable, other connection media or other wired connection interfaces. The PSTN is any public switched telephone network provided by AT&T, GTE, Sprint, MCI, SBC, Verizon and others.

The non-mesh communications network 23 may also include a paging and wireless messaging network, a wireless cellular telephone network, a Packet Cellular Network (PCN), Global System for Mobile Communications, (GSM), Generic Packet Radio Services (GPRS), network/Personal Communications Services network (PCS), a Cellular Digital Packet Data (CDPD), Wireless Application Protocol (WAP), Digital Audio Broadcasting (DAB) network, Transmission Control Protocol (TCP)/User Datagram Protocol (UDP)/Internet Protocol (IP) network, Voice over IP (VoIP network or other types of network.

The wireless cellular telephone network includes, but is not limited to Code Division Multiple Access (CDMA), Time Division Multiple Access (TDMA), or other wireless technologies.

As is known in the art, PCS networks include network that cover a range of wireless, digital communications technologies and services, including cordless phones, mobile phones, voice mail, paging, faxing, mobile personal digital/data assistants (PDAs), etc. PCS devices are typically divided into narrowband and broadband categories.

Narrowband devices, which operates in the 900 MHz band of frequencies, typically provide paging, data messaging, faxing, and one- and two-way electronic messaging capabilities. Broadband devices, which operate in the 1850 MHz to 1990 MHz range typically provide two-way voice, data, and video communications. Other wireless technologies such as GSM, CDMA and TDMA are typically included in the PCS category.

As is known in the art, GSM is another type of digital wireless technology widely used throughout Europe, in Australia, India, Africa, Asia, and the Middle East. GSM is gaining popularity in the United States. GSM is a wireless platform based on TDMA to digitize data. GSM includes not only telephony and Short Message Services (SMS) but also voice mail, call forwarding, fax, caller ID, Internet access, and e-mail.

As is known in the art, SMS is type of communications service that enables a user to allow private message communications with another user. GSM typically operates at three frequency ranges: 900 MHz (GSM 900) in Europe, Asia and most of the rest of the world; 1800 MHz (GSM 1800 or DCS 1800 or DCS) in a few European countries; and 1900 MHz (GSM 1900 also called PCS 1900 or PCS) in the United States. GSM also operates in a dual-band mode including 900/1800 Mhz and a tri-band mode include 900/1800/1900 Mhz.

As is known in the art, GPRS is a standard for wireless communications, which runs at speeds up to 150 kilo-bits-per-second ("kbit/s"). GPRS, which supports a wide range of bandwidths is an efficient use of limited bandwidth and is particularly suited for sending and receiving small bursts of data such as e-mail and Web browsing, as well as large volumes of data.

As is known in the art, CDPD is a wireless standard providing two-way, 19.2-Kbps or higher packet data transmission over existing cellular telephone channels. As is known in the art, a Packet Cellular Network (PCN) includes various types of packetized cellular data.

In one embodiment, of the invention, the wireless interfaces include WPAN wireless personal area network (WPAN) interfaces. As is known in the art, a WPAN is a personal area network for interconnecting devices centered around an individual person's devices in which the connections are wireless. A WPAN interconnects all the ordinary computing and communicating devices that a person has on

their desk (e.g. computer, etc.) or carry with them (e.g., PDA, mobile phone, two-way pager, etc.)

Typically, a wireless personal area network uses some technology that permits communication only within about 10 meters. One such technology is "Bluetooth." Another such technology is "Zigbee."

A key concept in WPAN technology is known as "plugging in." In the ideal scenario, when any two WPAN-equipped devices come into close proximity (within several meters of each other) or within a few kilometers of a central server (not illustrated), they can communicate via wireless communications as if connected by a cable. WPAN devices can also lock out other devices selectively, preventing needless interference or unauthorized access to secure information.

In one embodiment of the present invention, the wireless interfaces include but are not limited to, an IEEE 802.11a, 802.11b, 802.11g, 802.11n, 802.15.4 (ZigBee), 802.16a, 802.16g, "Wireless Fidelity" (WiFi), "Worldwide Interoperability for Microwave Access" (WiMAX), ETSI High Performance Radio Metropolitan Area Network (HIPERMAN) "RF Home," or other types of wireless interfaces. However, the present invention is not limited to such wireless interface and other types of wireless interfaces can also be used.

In another embodiment of the present invention, the wireless mesh network device **14**, **16**, **18**, **22** includes a wireless sensor device that comprises an integral or separate Bluetooth and/or infra data association (IrDA) module for wireless Bluetooth or wireless infrared communications.

As is known in the art, an 802.11b is a short-range wireless network standard. The IEEE 802.11b standard defines wireless interfaces that provide up to 11 Mbps wireless data transmission to and from wireless devices over short ranges. 802.11a is an extension of the 802.11b and can deliver speeds up to 54M bps. 802.11g deliver speeds on par with 802.11a. However, other 802.11xx interfaces can also be used and the present invention is not limited to the 802.11 protocols defined. The IEEE 802.11a, 802.11b and 802.11g standards are incorporated herein by reference.

As is known in the art, WiFi is a type of 802.11xx interface, whether 802.11b, 802.11a, dual-band, etc. WiFi devices include an RF interfaces such as 2.4 GHz for 802.11b or 802.11g and 5 GHz for 802.11a.

As is known in the art, 802.15.4 (Zigbee) is low data rate network standard used for mesh network devices such as sensors, interactive toys, smart badges, remote controls, and home automation. The 802.15.4 standard provides data rates of 250 kbps, 40 kbps, and 20 kbps., two addressing modes; 16-bit short and 64-bit IEEE addressing, support for critical latency devices, such as joysticks, Carrier Sense Multiple Access/Collision Avoidance, (CSMA-CA) channel access, automatic network establishment by a coordinator, fully handshaked protocol for transfer reliability, power management to ensure low power consumption for multi-month to multi-year battery usage and up to 16 channels in the 2.4 GHz Industrial, Scientific and Medical (ISM) band (Worldwide), 10 channels in the 915 MHz (US) and one channel in the 868 MHz band (Europe). The IEEE 802.15.4-2003 standard is incorporated herein by reference.

As is known in the art, WiMAX is an industry trade organization formed by leading communications component and equipment companies to promote and certify compatibility and interoperability of broadband wireless access equipment that conforms to the IEEE 802.16XX and ETSI HIPERMAN. HIPERMAN is the European standard for metropolitan area networks (MAN).

The IEEE The 802.16a and 802.16g standards are wireless MAN technology standard that provides a wireless alternative to cable, DSL and T1/E1 for last mile broadband access. It is also used as complimentary technology to connect IEEE 802.11XX hot spots to the Internet.

The IEEE 802.16a standard for 2-11 GHz is a wireless MAN technology that provides broadband wireless connectivity to fixed, portable and nomadic devices. It provides up to 50-kilometers of service area range, allows users to get broadband connectivity without needing direct line of sight with the base station, and provides total data rates of up to 280 Mbps per base station, which is enough bandwidth to simultaneously support hundreds of businesses with T1/E1 -type connectivity and thousands of homes with DSL-type connectivity with a single base station. The IEEE 802.16g provides up to 100 Mbps.

The IEEE 802.16e standard is an extension to the approved IEEE 802.16/16a/16g standard. The purpose of 802.16e is to add limited mobility to the current standard which is designed for fixed operation.

The ESTI HIPERMAN standard is an interoperable broadband fixed wireless access standard for systems operating at radio frequencies between 2 GHz and 11 GHz.

The IEEE 802.16a, 802.16e and 802.16g standards are incorporated herein by reference. WiMAX can be used to provide a WLP.

The ETSI HIPERMAN standards TR 101 031, TR 101 475, TR 101 493-1 through TR 101 493-3, TR 101 761-1 through TR 101 761-4, TR 101 762, TR 101 763-1 through TR 101 763-3 and TR 101 957 are incorporated herein by reference. ETSI HIPERMAN can be used to provide a WLP.

As is known in the art, Bluetooth is a short-range radio frequency technology aimed at simplifying communications among network devices and between network devices. Bluetooth wireless technology supports both short-range point-to-point and point-to-multipoint connections. The Bluetooth Specification, GL 11r02, March 2005, prepared by the Bluetooth SIG, Inc. is incorporated herein by reference.

As is known in the art, IP is an addressing protocol designed to route traffic within a network or between networks. For more information on IP see IETF RFC-791 incorporated herein by reference.

TCP provides a connection-oriented, end-to-end reliable protocol designed to fit into a layered hierarchy of protocols that support multi-network applications. For more information on TCP see RFC-793, incorporated herein by reference.

UDP provides a connectionless mode of communications with datagrams in an interconnected set of networks. For more information on UDP see IETF RFC-768 incorporated herein by reference.

As is known in the art, VoIP is a set of facilities for managing the delivery of voice information using IP packets. In general, VoIP is used to send voice information in digital form in discrete data packets (i.e., IP packets) over data networks rather than using traditional circuit-switched protocols used on the PSTN. VoIP is used on both wireless and wired data networks.

VoIP typically comprises several applications (e.g., Session Initiation Protocol (SIP), Service Location Protocol (SLP), H.323, H.324, Domain Name System (DNS), Authentication Authorization and Accounting (AAA), codecs (G.7xx), etc.) that convert a voice signal into a stream of packets (e.g., IP packets) on a packet network and back again. VoIP allows voice signals to travel over a stream of data packets over a communications network.

Security and Encryption

Devices and interfaces (e.g., security interface 46) of the present invention include plural security and/or encryption methods for secure communications. Wireless Encryption Protocol (WEP) (also called Wired Equivalent Privacy) is a security protocol for WiLANs defined in the IEEE 802.11b standard. WEP is cryptographic privacy algorithm, based on the Rivest Cipher 4 (RC4) encryption engine, used to provide confidentiality for 802.11b wireless data.

As is known in the art, RC4 is cipher designed by RSA Data Security, Inc. of Bedford, Mass., which can accept encryption keys of arbitrary length, and is essentially a pseudo random number generator with an output of the generator being XORed with a data stream to produce encrypted data.

One problem with WEP is that it is used at the two lowest layers of the OSI model, the physical layer and the data link layer, therefore, it does not offer end-to-end security. One another problem with WEP is that its encryption keys are static rather than dynamic. To update WEP encryption keys, an individual has to manually update a WEP key. WEP also typically uses 40-bit static keys for encryption and thus provides "weak encryption," making a WEP device a target of hackers.

The IEEE 802.11 Working Group is working on a security upgrade for the 802.11 standard called "802.11i." This supplemental draft standard is intended to improve WiLAN security. It describes the encrypted transmission of data between systems 802.11X WiLANs. It also defines new encryption key protocols including the Temporal Key Integrity Protocol (TKIP). The IEEE 802.11i draft standard, version 4, completed Jun. 6, 2003, is incorporated herein by reference.

The 802.11i is based on 802.1x port-based authentication for user and device authentication. The 802.11i standard includes two main developments: Wireless or Wi-Fi Protected Access (WPA) and Robust Security Network (RSN).

WPA uses the same RC4 underlying encryption algorithm as WEP. However, WPA uses TKIP to improve security of keys used with WEP. WPA keys are derived and rotated more often than WEP keys and thus provide additional security. WPA also adds a message-integrity-check function to prevent packet forgeries.

RSN uses dynamic negotiation of authentication and selectable encryption algorithms between wireless access points and wireless devices. The authentication schemes proposed in the draft standard include Extensible Authentication Protocol (EAP). One proposed encryption algorithm is an Advanced Encryption Standard (AES) encryption algorithm.

Dynamic negotiation of authentication and encryption algorithms lets RSN evolve with the state of the art in security, adding algorithms to address new threats and continuing to provide the security necessary to protect information that WiLANs carry.

The NIST developed a new encryption standard, the Advanced Encryption Standard (AES) to keep government information secure. AES is intended to be a stronger, more efficient successor to Triple Data Encryption Standard (3DES).

As is known in the art, DES is a popular symmetric-key encryption method developed in 1975 and standardized by ANSI in 1981 as ANSI X.3.92, the contents of which are incorporated herein by reference. As is known in the art, 3DES is the encrypt-decrypt-encrypt (EDE) mode of the DES cipher algorithm. 3DES is defined in the ANSI standard, ANSI X9.52-1998, the contents of which are incorpo-

rated herein by reference. DES modes of operation are used in conjunction with the NIST Federal Information Processing Standard (FIPS) for data encryption (FIPS 46-3, October 1999), the contents of which are incorporated herein by reference.

The NIST approved a FIPS for the AES, FIPS-197. This standard specified "Rijndael" encryption as a FIPS-approved symmetric encryption algorithm that may be used by U.S. Government organizations (and others) to protect sensitive information. The NIST FIPS-197 standard (AES FIPS PUB 197, November 2001) is incorporated herein by reference.

The NIST approved a FIPS for U.S. Federal Government requirements for information technology products for sensitive but unclassified (SBU) communications. The NIST FIPS Security Requirements for Cryptographic Modules (FIPS PUB 140-2, May 2001) is incorporated herein by reference.

As is known in the art, RSA is a public key encryption system which can be used both for encrypting messages and making digital signatures. The letters RSA stand for the names of the inventors: Rivest, Shamir and Adleman. For more information on RSA, see U.S. Pat. No. 4,405,829, now expired, incorporated herein by reference.

As is known in the art, "hashing" is the transformation of a string of characters into a usually shorter fixed-length value or key that represents the original string. Hashing is used to index and retrieve items in a database because it is faster to find the item using the shorter hashed key than to find it using the original value. It is also used in many encryption algorithms.

Secure Hash Algorithm (SHA), is used for computing a secure condensed representation of a data message or a data file. When a message of any length $< 2^{64}$ bits is input, the SHA-1 produces a 160-bit output called a "message digest." The message digest can then be input to other security techniques such as encryption, a Digital Signature Algorithm (DSA) and others which generates or verifies a security mechanism for the message. SHA-512 outputs a 512-bit message digest. The Secure Hash Standard, FIPS PUB 180-1, Apr. 17, 1995, is incorporated herein by reference.

Message Digest-5 (MD-5) takes as input a message of arbitrary length and produces as output a 128-bit "message digest" of the input. The MD5 algorithm is intended for digital signature applications, where a large file must be "compressed" in a secure manner before being encrypted with a private (secret) key under a public-key cryptosystem such as RSA. The IETF RFC-1321, entitled "The MD5 Message-Digest Algorithm" is incorporated here by reference.

As is known in the art, providing a way to check the integrity of information transmitted over or stored in an unreliable medium such as a wireless network is a prime necessity in the world of open computing and communications. Mechanisms that provide such integrity check based on a secret key are called "message authentication codes" (MACS). Typically, message authentication codes are used between two parties that share a secret key in order to validate information transmitted between these parties.

Keyed Hashing for Message Authentication Codes (HMAC), is a mechanism for message authentication using cryptographic hash functions. HMAC is used with any iterative cryptographic hash function, e.g., MD5, SHA-1, SHA-512, etc. in combination with a secret shared key. The cryptographic strength of HMAC depends on the properties of the underlying hash function. The IETF RFC-2101,

entitled "HMAC: Keyed-Hashing for Message Authentication" is incorporated here by reference.

As is known in the art, an Electronic Code Book (ECB) is a mode of operation for a "block cipher," with the characteristic that each possible block of plaintext has a defined corresponding cipher text value and vice versa. In other words, the same plaintext value will always result in the same cipher text value. Electronic Code Book is used when a volume of plaintext is separated into several blocks of data, each of which is then encrypted independently of other blocks. The Electronic Code Book has the ability to support a separate encryption key for each block type.

As is known in the art, Diffie and Hellman (DH) describe several different group methods for two parties to agree upon a shared secret in such a way that the secret will be unavailable to eavesdroppers. This secret is then converted into various types of cryptographic keys. A large number of the variants of the DH method exist including ANSI X9.42. The IETF RFC-2631, entitled "Diffie-Hellman Key Agreement Method" is incorporated here by reference.

However, the present invention is not limited to the security or encryption techniques described and other security or encryption techniques can also be used.

As is known in the art, the HyperText Transport Protocol (HTTP) Secure (HTTPS), is a standard for encrypted communications on the World Wide Web. HTTPS is actually just HTTP over a Secure Sockets Layer (SSL). For more information on HTTP, see IETF RFC-2616 incorporated herein by reference.

As is known in the art, the SSL protocol is a protocol layer which may be placed between a reliable connection-oriented network layer protocol (e.g. TCP/IP) and the application protocol layer (e.g. HTTP). SSL provides for secure communication between a source and destination by allowing mutual authentication, the use of digital signatures for integrity, and encryption for privacy.

The SSL protocol is designed to support a range of choices for specific security methods used for cryptography, message digests, and digital signatures. The security method are negotiated between the source and destination at the start of establishing a protocol session. The SSL 2.0 protocol specification, by Kipp E. B. Hickman, 1995 is incorporated herein by reference.

As is known in the art, Transport Layer Security (TLS) provides communications privacy over the Internet. The protocol allows client/server applications to communicate over a transport layer (e.g., TCP) in a way that is designed to prevent eavesdropping, tampering, or message forgery. For more information on TLS see IETF RFC-2246, incorporated herein by reference.

In one embodiment, the security functionality includes Cisco Compatible EXtensions (CCX). CCX includes security specifications for makers of 802.11xx wireless LAN chips for ensuring compliance with Cisco's proprietary wireless security LAN protocols. As is known in the art, Cisco Systems, Inc. of San Jose, Calif. is supplier of networking hardware and software, including router and security products.

Exemplary Mesh Network Device

FIG. 2 is a block diagram illustrating an exemplary mesh network device architecture 24. The architecture 24 includes, but is not limited to, a mesh network device 26 comprising a universal serial bus (USB) interface (I/F) 28, a selectable communications bit-interface (e.g., 16/32 bit) 30, a flash memory 32, an erasable electronically programmable read only memory (EEPROM) 34, a first-in-first-out (FIFO) buffer 36, a data-link chip 38 (e.g., Medium Access

Control (MAC) chip, etc.), a baseband and/or ultra wideband transceiver (e.g., Zigbee, Bluetooth, WiFi, WiMax, etc.) 40, a wireless Radio Frequency (RF) antenna 42, a clock 44, and a security interface 46.

The EEPROM 34 may include one or more software modules used for networking (e.g., TCP/IP/UDP, etc.), security or for other purposes. In one embodiment, the security interface 46 is not a separate hardware interface but includes one more software modules included in the EEPROM 34 or in the flash memory 32.

As is known in the art, a "baseband" transceiver is a transceiver in which information is carried in digital form in one or more channels on a transmission medium. A baseband includes any frequency band on which information is superimposed, whether or not a frequency band is multiplexed and on which digital information can be sent on sub-bands.

In one embodiment, the mesh network device 26 further comprises an external power source 48 (e.g., via USB, etc.), an external flash memory or external disk drive 50, an external wireless radio frequency (RF) front end 52 (e.g., a wireless RF antenna, etc.) and an external host network device 54 (e.g., computer, PDA, mobile phone, etc.). The external flash or disk drive 50 includes, but is not limited to, a removable device such as a Compact Flash (CF), Secure Digital Card (SD), Memory Stick (MS), Micro Drive, MultiMediaCard (MMC) xD-Picture Card (xD), SmartMedia (SM) card or other removable device. However, the present invention is not limited to this embodiment and more, fewer or other components can also be used to practice the invention.

In one embodiment, the mesh network device 26 includes Complementary Code Keying (CCK). As is known in the art, CCK is a modulation scheme used with wireless networks (WLANs) that employ the IEEE 802.11b specification. A complementary code includes a pair of finite bit sequences of equal length, such that a number of pairs of identical elements (e.g., one or zero) with any given separation in one sequence are equal to a number of pairs of unlike elements having the same separation in the other sequence.

In one embodiment, the mesh network device 26 includes differential quadrature phase shift keying (DQPSK). DQPSK modulates using differential quaternary phase shift keying. DQPSK transmits only differences between values of a phase of a sin wave, rather than a full absolute value. DQPSK makes use of two carrier signals, separated by 90-degrees. The output is a baseband representation of the modulated signal.

In one embodiment, the mesh network device 26 includes differential binary phase shift keying (DBPSK). DBPSK modulates using the differential binary phase shift keying. DBPSK maps phase differences of θ and $\pi+\theta$, respectively, to outputs of zero and one, respectively, where θ is a phase rotation parameter. The output is a baseband representation of the modulated signal.

In one embodiment, the mesh network device 26 includes Orthogonal frequency division multiplexing (OFDM). OFDM is also called discrete multi-tone modulation (DMT) and is a transmission technique based upon the idea of frequency-division multiplexing (FDM) where multiple signals are sent out at different frequencies. OFDM uses a composite of narrow channel bands to enhance its performance in high frequency bands (such as 5.x GHz) in urban and rural applications where building clutter and foliage can negatively impact the propagation of radio waves for wireless devices.

15

In one embodiment, the mesh network device **26** includes Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA). CSMA/CA is a data-link layer protocol used in the data-link chip **38** for carrier transmission in 802.11xx networks. CSMA/CA acts to prevent collisions before they happen.

In one embodiment, the mesh network device **26** is an internal device to a mesh network device **[12,] 14, 16, 18, 22**. In another embodiment, the mesh network device an external portable removable device as illustrated in FIG. **3**. However, the present invention is not limited to such an embodiment and other embodiments can be used to practice the invention.

FIG. **3** is a block diagram illustrating an outer view **56** of a specific exemplary implementation **58** of the mesh network device **26** of FIG. **2**.

FIG. **3B** is a block diagram illustrating an inner view **59** specific exemplary implementation **58** of the mesh network device of FIG. **3A**. Mesh network device **26** can be used as an embedded component in other electronic devices (e.g., mobile phone, PDA, smart phone, etc.) with or without the USB interface component **28**.

In one embodiment, the mesh network device **58** further comprises a first light emitting diode (LED) **60** indicating when the mesh network device is connected to a mesh network or partial mesh network and a second LED **62** indicating whether the mesh network device is active. The mesh network device **58** further includes a cover **64** for the USB interface **28**.

In one specific exemplary embodiment, the mesh network device **58** is called "MOBEE®" and is a self-contained USB based-mesh network device for exchanging multimedia content between mesh network devices (e.g., host devices, PC/Laptop/PDA/Smart Phone/Mobile/Smart Home devices, etc.) through a meshed mobile network to maximize communication portability.

In one embodiment, functionality of the mesh network device **58** is implemented in a software application **61**. In such an embodiment, the software application **58** uses a wireless communications interface integral to mesh network device **14, 16, 18, 22**. In one specific embodiment, the software application **61** is a software application for a smart phone **16** or a tablet computer **22**. However, the present invention is not limited to such an embodiment and other types of software applications can be used to practice the invention.

In one embodiment, a mesh network device **26, 58** further includes a Smart Transducer Interface Modules (STIM) with an Ultra wideband transceiver (e.g., in a physical layer), a mesh network protocol adapter (e.g., in a data-link layer (e.g. MAC layer, with CCK, DBPSK, OFDM encoding etc.)) and authentication and encryption software (e.g., in data-link layer).

Ultra-wideband (UWB) refers to a radio communications technique based on transmitting very-short-duration pulses, often of duration of only nanoseconds or less, whereby the occupied bandwidth goes to very large values.

In another embodiment, the mesh network device **58** includes a Wireless Sensor Portal (WSP) with a Thin Film Transistor (TFT) high-resolution user graphic interface (GUI) **65** for displaying WSP information and sensor topology information and an Organizing Agent (OA). The OA manages the WSP and TFT. The OA is also responsible for collecting and organizing sensor data in a fashion that allows for a particular class of mesh network queries to be answered. However, the present invention is not limited to these embodiments and other embodiments can also be used.

16

As is known in the art, a TFT is type of LCD flat panel display screen in which each pixel is controlled by one to four transistors. TFT displays are sometimes called active matrix Liquid Crystal Diodes (LCDs).

In one exemplary embodiment, the mesh network device **26, 58** is a tiny device that integrates at least three elements together: (1) a wireless baseband module **40** such as 802.11g/b/a, 802.15.4 (ZigBee), Bluetooth, Ultra wideband 802.16x, (e.g., WiMAX, etc.) etc. (2) a flash memory **32**; and (3) an external power source **46**. The mesh network device **26, 58** may further include an external removable memory module **48** such as a Secure Digital (SD) card, Pro Multimedia Card (MMC), Memory Stick (MS), Microdrive, XD card or other external storage cards. However, the present invention is not limited to this embodiment and more, fewer or other components can also be used to practice the invention.

In one embodiment the mesh network device **26, 58** includes at least the features illustrated in Table 1. However, the present invention is not limited to the features listed in Table 1 and more, fewer or other components can also be used to practice the invention.

TABLE 1

Wireless module such as: IEEE802.11a/b/g, IEEE 802.15.4 (ZigBee), Bluetooth, Ultra wideband, or IEEE 802.16 (WiMAX)
Wireless + NAND Flash combo solution with external removable Flash memory such as Secure Digital (SD) card, Pro Multimedia Card (MMC), Memory Stick (MS), Microdrive, and XD.
Mesh networking and WPAN software
USB 2.0 interface and compatible with USB 1.1
IEEE 1394
TCP/IP/UDP
Programmable wireless RF interface
High level security includes, but are not limited to, WEP64/128/256, WPA (HW TKIP support) and AES128.
Auto-installation function
Software wireless access point

In another embodiment, the specific implementation **58** of the mesh network of FIG. **3** includes at least the features illustrated in Table 2. However, the present invention is not limited to the features listed in Table 2 and more, fewer or other components can also be used to practice the invention.

TABLE 2

Wireless Standards	IEEE 802.11 b/g, 802.15.4
Host Interface 28	USB 2.0 Plug and Play
Wireless Antenna	Chip Antenna
Connector 42	
Frequency Range	2.412 GHz-2.4835 GHz
Number of Selectable Channels	USA, Canada: 11 channels Europe: 13 channels Asia (e.g., Japan): 14 channels
Modulation Techniques	Direct Sequence Spread Spectrum (CCK, DQPSK, DBPSK) Orthogonal frequency division multiplexing (OFDM)
Security 46	64/128/256 bit WEP, WPA, WPA2, CCX1.0, CCX2.0, 802.1x
Data-Link 38 Protocol	CSMA/CA (Collision Avoidance) with acknowledgment
Output RF Power	11 g: 13 dBm 11 b: 16 dBm
Sensitivity	-71 dBm @ 54 Mbps -84 dBm @ 11 Mbps
Data Rate	802.11 g (54 Mbps, 48 Mbps, 36 Mbps, 24 Mbps, 18 Mbps, 12 Mbps, 9 Mbps, 6 Mbps) 802.11 b (11 Mbps, 5.5 Mbps, 2 Mbps, 1 Mbps)
Throughput	33 Mbps @ 11 g + mode 24 Mbps @ 11 g mode

TABLE 2-continued

LEDs 58, 60	Link: Green Active: Green
Weight	10 g
Dimensions	71.5 mm (L) × 19 mm (W) × 9 mm (H)
Power 48 Requirements	Operating Voltage: 5 V DC Continuous TX Current: 350 mA @ 54 Mbps Continuous TX Current: 330 mA @ 11 Mbps Continuous RX Current: 245 mA Typical Current 240 mA

Exemplary Mesh Network Device Method of Use

FIG. 4 is a flow diagram illustrating a Method 66 for mobile mesh networking. At Step 68, a first mobile mesh network device (e.g., 14) moves within a pre-determined distance of a second mobile mesh network device (e.g., 16), wherein the second mobile mesh network device 16 is also moving. At Step 70, mobile mesh network data is exchanged over a secure communications channel between the first mobile mesh network 14 and the second mesh network device 16. At 72, the mesh network data is verified on the second mobile mesh network device. At Step 74, the verified mesh network data is distributed to other mesh network devices (e.g., 18), if any, on the mesh network 12, thereby creating an N-way mobile mesh network 12 between the plural network devices 14, 16, 18.

Method 66 is illustrated with an exemplary embodiment. However, the present invention is not limited to such and embodiment and other embodiments can also be used to practice the invention. In such an exemplary embodiment at Step 68, a first mobile mesh network device (e.g., 14) moves within a pre-determined distance of a second mobile mesh network device (e.g., 16). The first mobile mesh network device 14 and the second mobile mesh network device 16 include implementations 26, 58 described above.

At Step 70, mesh network data is exchanged over a secure communications channel between the first mobile mesh network 14 and the second mesh network device 16 to create a mobile mesh network 12. The mesh network data includes, but is not limited to, routing data, spatial data, mesh network load data and other mesh network data.

At 72, the mesh network data is verified on the second mesh network device 16. The verification includes verifying routing paths, spatial data, mesh network load data and other mesh network data.

At Step 74, the verified mesh network device is distributed to other mesh network devices (e.g., 18), if any, on the mesh network 12, thereby creating an N-way mobile mesh network 12 between the plural network devices 14, 16, 18.

FIG. 5 is a block diagram 76 illustrating an N-way mesh network formed using the mesh network device of FIG. 2. FIG. 5 illustrates two additional network devices including a television 78 and a laptop computer 80. The network devices 14, 16, 18, 22, 78, 80 in FIG. 5 are attached to the mesh network device 26 that is used to create an N-way mesh network. FIG. 5 illustrates a full mesh topology 12. However, the mesh network devices 26, 58 can also be used to form a partial mesh topology 20 (not illustrated in FIG. 4).

Wireless Mesh Sensor Networks

Wireless sensor networks provide distributed network and Internet access to sensors, controls, and processors that are deeply embedded in equipment, facilities, and the environment. Wireless sensor networks provide monitoring and control capability for applications in transportation, manufacturing, health care, environmental monitoring, and safety and security. Wireless sensor networks provide low power signal processing, low power computation, and low power,

low cost wireless networking capability in a compact system. Wireless sensor networks provide sensing, local control, and embedded intelligent systems in structures, materials, and environments.

In one embodiment, the mesh network device 26, 56 is an embedded mesh network device. In such an embodiment, the mesh network device 26, 56 is embedded into a mobile telephone, PDA, hand-held gaming device, smart phone, RFID tag, and other portable/mobile electronic devices.

In another embodiment, the mesh network device 26, 56 is a wireless mesh network sensor to collect and monitor spatial data. In such an embodiment, the mesh network device 26, 56 may include only selected ones of the components illustrated in FIG. 2 to make the wireless mesh sensor device simpler, smaller and less expensive.

Mesh sensor networks are used to determine spatial data including the location of objects. Location prediction is used to determine locations of a spatial phenomenon from maps of other spatial features such as building walls, natural phenomenon such as mountains, etc.

The method and system described herein also integrate wireless and wired sensor data acquisition for distributed sensing and monitoring for example, for rocket propulsion testing, agricultural efficiency, coastal management, disaster management, ecological forecasting, energy management, homeland security, and detecting ice accretion and detection of emissions, air quality, other data sensed around specific environments and other applications.

The method and apparatus described herein can be used for at least these exemplary applications: (1) Sensing and monitoring for Aircraft—icing on wings—data from heaters and sensors; (2) Aircraft emissions—collection of data around airports; (3) Verification and validation of equipment (e.g., Radio Frequency Identifiers “RFID”); and (4) Security—geo-location and personal location. However, the present invention is not limited to these applications and the present invention can be applied to other applications.

The method and apparatus described herein may provide at least the following advantages: (1) Spatial data is Extremely Difficult to Intercept—Wideband pulsed radar spreads the signal and allows more users access to a limited amount of scarce frequency spectrum, thus allowing spectrum reuse; (2) Multipath Immunity—A low path loss and low energy density minimizes interference to other services. UWB is very tolerant of interference, enabling operation within buildings, urban areas, and forests; (3) Precision Network-wide timing—Real-time, continuous position location down to a centimeter of resolution results in precision geolocation systems (4) Low Cost—Requires minimal components resulting in small size and weight; (5) Low Power—Typical consumption is in microwatts; and (6) Antennas—Can be very small (2 cm) because they are non-resonant.

Mesh Network Device Dynamic Information Exchange

FIG. 6 is a flow diagram illustrating a Method 78 for dynamic information interchange for mesh network devices. At Step 80, a first set of profile information is received on a first mesh network device. At Step 82, a wireless signal is periodically sent from the first network device to a mesh network including plural other mesh network devices including other sets of profile information. At Step 84, one or more wireless signals from the plural other mesh network devices on the mesh network are received on the first mesh network device. The one or more wireless signals include other sets of profile information stored on the plural of other mesh network devices. At Step 86, a test is conducted to determine from the received one or more wireless signals whether any items in first set of profile information on the

first network device match any items in other sets of profile information stored on the plural other mesh network devices. At Step 88, if any profile items match, a set of data is exchanged between the first network device and the one or more other mesh network devices via the mesh network.

Method 78 is illustrated with one exemplary embodiment. However, the present invention is not limited to such an embodiment and other embodiments can also be used to practice the invention.

In such an exemplary embodiment at Step 80, the mesh network device 56 is equipped with a short-range wireless module and flash memory as is illustrated in FIGS. 2 and 3. In another embodiment, the small mesh network device is embedded within an audio player (e.g., MP3 player, etc.) or other popular handheld devices.

At Step 80, the user profile information 91, 91' (FIG. 7) includes, but is not limited to, an e-mail address, an IP address, a hardware address (e.g., Medium Access Control (MAC) address, etc.), a URL, a name, an address, an telephone number, an instant message identifier, a text message identifier, a encryption key, a digital signature, a secure message digest, a security identifier, a mesh network identifier or other types of profile information such as advertisements, public or emergency notices, location specific information including location-aware information and/or physical location information (e.g., Global Positioning Satellite (GPS) information, street address information, two-dimensional (2D) (e.g., X,Y) (e.g., building, floor), three-dimensional (3D) (X, Y, Z) (e.g., building, floor, floor location) or other physical location information. However, the present invention is not limited to such profile information and other profile information can also be used.

At Step 80, a user profile 91 is entered or edited through a template stored on the mesh network device 56 or via a web-site on a server on the mesh network 12 or on another public or private network such as the Internet or an intranet. The user profile 91 is saved to the first mesh network device 56 via USB connection. Personal information is stored in the flash 32. The user of the mesh network device selects one, several or all of the items in the user profile to match to user profiles in other mesh network devices. The profile information may also be entered through the display 66.

At Step 82, a wireless signal is periodically sent out via the wireless antenna 42 periodically to the mesh network 12. (e.g., sent out to other mesh network devices up to 10 meters away).

The user profile includes virtually any type of information such as, gender, age, Looking for . . . , Hobby, e-mail address, home address, home telephone number, work information, advertising, etc.

At Step 84, one or more wireless signals from the plural other mesh network devices 56', 56" on the mesh network 12 are received on the first mesh network device 56. The one or more wireless signals include other sets of profile information stored on the plural of other mesh network devices 56', 56".

At Step 86, a test is conducted to determine if the first set of profile information matches any other sets of profile information stored on other mesh network devices 56', 56", and if so, the first mesh network device 56 exchanges a set of data with the one or more other mesh network devices 56', 56".

At Step 88, when a mesh network device 56' 56", etc. matches any selected information (one, several, all items) in the first mesh network device 56, data is dynamically exchanged wirelessly and stored on each other's Flash memory in the mesh network devices. In one embodiment,

the data is securely exchanged using a pre-determined security and/or encryption method.

The received data is retrievable via display 66, a computer or other interface (e.g., web-site page, etc.). The data dynamically exchange includes one, several or all items stored in the profile and/or other types of data stored on the mesh network devices. For example, a user of the first mesh network device 26, 56, may wish to dynamically exchange audio files such as MP3 files, etc. with a friend's mesh network device 26', 56'. At Step 88, the two mesh user devices 26, 56 and 26' and 56' may exchange MP3 files based on a set of designated e-mail addresses (e.g., the first user's and the friend's e-mail, etc.).

As is known in the art Motion Picture Expert Group (MPEG) Audio Layer 3, more commonly referred to as "MP3," is a popular encoding format for audio information.

In such an example both the user profile on the first mesh network device 26, 56 and the friend's mesh network device 26', 56' may include both e-mail addresses. In another embodiment, the user profiles may only include one designated e-mail address (e.g., the e-mail address of the user of the first mesh network device, etc.).

FIG. 7 is a block diagram illustrating a data flow 90 for dynamic information interchange for mesh network devices using Method 78.

FIG. 8 is a flow diagram illustrating a Method 90 for enabling dynamic information interchange for mesh network devices. At Step 92, a user profile template is activated on a first mesh network device. At Step 94, plural profile information items are received on the first network device for the profile template. At Step 96, the profile information in the profile template is stored in non-volatile storage on the first mesh network device. At Step 98, a wireless signal including the stored profile information is periodically broadcast from the first mesh network device to plural other mesh network devices on a mesh network. The stored profile information allows the first mesh network device to exchange data with one or more of the plural other mesh network devices on the mesh network whose stored profile information that matches any of stored profile information of the first mesh network device.

Method 90 is illustrated with one exemplary embodiment. However, the present invention is not limited to such an embodiment and other embodiments can also be used to practice the invention.

In such an exemplary embodiment at Step 92, a user profile template 91 is activated on a first mesh network device 26, 56. In one embodiment the user profile template 91 is activated when a user plugs the mesh network device 26, 56 in a USB port on a computer or other device. In such an embodiment, flash 32 or EEPROM 34 includes a URL to allow the first mesh network device to obtain a profile template. The URL is used to access the user profile template 91 at another location on the mesh network 12. In such an embodiment, a user is directed via the URL to a user login page or web page from which the user is allowed to obtain, view and fill a profile template 91.

In another embodiment, at Step 92 the user profile template 91 is stored directly in flash 32 or EEPROM 34 of the first mesh network device 26, 56 and is activated as part of an initialization sequence for the first mesh network device 26, 56. In such an embodiment, the profile template can be reactivated at a later time to change profile items.

In one embodiment, the profile template is securely stored using a pre-determined security and/or encryption method.

21

In either embodiment, the profile items can be viewed via display **65** or via host **54** (e.g., a user computer via a USB port, etc).

At Step **94**, plural profile information items are received on the first network device **26**, **56** for the user profile template **91**.

At Step **96**, the profile information in the user profile template **91** is stored in non-volatile storage (e.g., flash **32**, etc.) on the first mesh network device **26**, **56**. The profile information may also be stored in other devices (e.g., a mesh network server) on other locations on the mesh network **12**. For example, if the profile template was activated via a URL, the profile template items may also be stored on the device identified by the URL.

At Step **98**, a wireless signal including the stored profile information is periodically broadcast from the first mesh network device **26**, **56** to plural other mesh network devices **56'**, **56"** on the mesh network **12**. The stored profile information allows the first mesh network device to exchange data with one or more of the plural other mesh network devices on the mesh network whose stored profile information that matches any of stored profile information of the first mesh network device using Method **78** and other methods. Social Networking Mesh Network Device Dynamic Information Exchange

FIGS. **9A** and **9B** are a flow diagram illustrating a Method **100** for dynamic information interchange for location aware mesh network devices. In FIG. **9A** at Step **102**, a wireless message including a first set of profile information is received from a first mesh network device with one or more processors on a second network device with one or more processors over a wireless mesh network. The first mesh network device includes an ultra wideband wireless transceiver and a mesh network protocol adapter with Complementary Code Keying (CCK), Differential Quaternary Phase Shift Keying (DQPSK) or Orthogonal Frequency Division Multiplexing (OFDM) encoders. The second network device resides at a pre-determined physical location. At Step **104**, The second network device obtains from the first set of profile information in the received wireless message a list of electronic identifiers for plural designated social contacts of an owner of the first mesh network device, wherein each of the plural designated social contacts include one or more electronic identifiers for one or more designated social contact network devices or one more social networking web-sites. At Step **106**, a first set of plural different types of wireless or wired communications messages are sent from the second network device over the wireless mesh network or a wired mesh network to selected ones of the one or more designed social contact network devices indicating the first message network device is physically located at a pre-determined distance from the pre-determined physical location of the second network device. The first set of the plurality of types of wireless and wired communications messages include an invitation message to join the owner of the first message network device at the pre-determined physical location of the second network device. In FIG. **9B** at Step **108**, a second set of a plural different types of wireless or wired communications messages are sent from the second network device to other selected ones of the one or more designed location contact network devices and to one more social networking web-sites over the non-mesh communications network indicating the first message network device is physically located at the predetermined distance from pre-determined physical location of the second network device. The second set of plural types of wireless and wired communications messages include an

22

invitation message to join the owner of the first message network device at the pre-determined physical location of the second network device.

Method **100** is illustrated with one exemplary embodiment. However, the present invention is not limited to such an embodiment and other embodiments can also be used to practice the invention.

In such an exemplary embodiment in FIG. **9A** at Step **102**, a wireless message including a first set of profile information **91** is received from a first mesh network device (e.g., **14**, **26**, **56**, etc.) with one or more processors on a second network device **[25]** (e.g., **25**) with one or more processors over a wireless mesh network **12**. The first mesh network device **14**, **26**, **56** includes an ultra wideband wireless transceiver **40** and a mesh network protocol adapter with Complementary Code Keying (CCK), Differential Quaternary Phase Shift Keying (DQPSK) or Orthogonal Frequency Division Multiplexing (OFDM) encoders (Table 1 and 2, etc.).

The second network device resides at a pre-determined physical location. For example, the second network device may be a wireless access point at a coffee shop, retail store, bar, restaurant, park, health club, recreational facility, etc.

In one embodiment, the ultra-wideband wireless transceiver **40** includes a (WiMAX) wireless transceiver. In another embodiment, the first mesh network device **14**, **26**, **56** includes a baseband wireless transceiver **40**. However, the present invention is not limited to the wireless transceivers described and other wireless transceivers can also be used to practice the invention.

In one embodiment, first mesh network device **14** includes a mobile telephone, personal digital/data assistant (PDA), smart phone, Radio Frequency Identification (RFID) tag, RFID sensor or RFID biometric tag mesh network device or a the mesh network device **26**, **56** is embedded into another non-mesh network device **16**, **18**, **22**. However, the present invention is not limited to the mesh network devices described and other mesh network devices and other non-mesh network devices can also be used to practice the invention.

In one embodiment, the second network device **25** includes a mesh or non-mesh server network device, a gateway, router, switch, wired access point, wireless access point or Radio Frequency Identification (RFID) sensor portal, RFID tag portal, or RFID biometric tag portal network device. The second network device **25** also includes a mesh network device **14**, **16**, **18**, **22**, **26**, **56**, etc. However, the present invention is not limited to the network devices described and other network devices and/or mesh network devices and/or non-mesh network devices can also be used to practice the invention.

At Step **104**, The second network device **25** obtains from the first set of profile information **91** in the received wireless message a list of electronic identifiers for plural designated social contacts of an owner of the first mesh network device **14**, **26**, **56**, wherein each of the plural designated social contacts include one or more electronic identifiers for one or more designated social contact network devices **16**, **18**, **22** or one more social networking web-sites **19** (e.g., FACEBOOK, U-TUBE, TWITTER, MY-SPACE, MATCH.COM, E-HARMONY, etc.), electronic couponing sites (e.g., GROUPON, SOCIAL LIVING, etc.), etc. The social networking web-sites include dating web-sites, blogs, RSS feeds, and other types of information web-sites in which messages can be left or posted for a variety of activities. However, the present invention is not limited to the social

23

networking sites described and other public and private social networking sites can also be used to practice the invention.

In one embodiment, the first set of profile information **91** includes an e-mail address, an Internet Protocol (IP) address, a hardware address, a universal resource locator (URL), a name, a street address, a telephone number, an instant message identifier, a text message identifier, a encryption key, a digital signature, a secure message digest, a security identifier, a mesh network identifier, a physical location information, public or emergency notices or location specific information including location-aware information or a social networking web-site login identifier. However, the present invention is not limited to the first set of profile information described and more fewer or other types of profile information **91** can also be used to practice the invention.

In one embodiment, the one or more electronic identifiers for one or more designated location contact network devices include a telephone number, an e-mail identifier, an instant message identifier, a text message identifier, a multi-media identifier, a mesh network identifier, a Radio Frequency Identifier (RFID) identifier or a social networking web-site login identifier. However, the present invention is not limited to the electronic identifiers described and other electronic identifiers can also be used to practice the invention.

At Step **106**, a first set of plural different types of wireless or wired communications messages are sent from the second network device **25** over the wireless mesh network **3** or wired mesh network **5** to selected ones of the one or more designed social contact network devices **16, 18, 22** indicating the first message network device **14** is physically located at a predetermined distance **21** from the pre-determined physical location of the second network device **25**. The first set of the plurality of types of wireless and wired communications messages include an invitation message to join the owner of the first message network device **14, 26, 56** at the pre-determined physical location of the second network device **25**.

For example, a user of a mesh network device **14, 26, 56**, may be in close proximity to other mesh network devices **16, 18, 22**, etc. that form a mesh network **12** or a partial mesh network **20** because of their close proximity. Step **106** is used to send messages directly on the mesh network **12** or partial mesh network **20** without having to use a non-mesh network **[25]** **23** (e.g., the Internet, etc.). This allows for much faster message sending and receiving than can be accomplished by accessing and using a non-mesh network **[25]** **23**. The mesh network **12** and partial mesh network are ad hoc networks. Mesh network devices join and leave the mesh network by moving in range and out of range of other mesh network devices.

In one embodiment, the first set of plural different types of wireless or wired communications messages include text messages, instant messages, multi-media messages, voice messages, RFID messages, social networking site messages (e.g., FACEBOOK post, a TWITTER tweet, etc.)

For example, the first mesh network device **14, 26, 56** may be located inside a coffee shop within **250** feet of the second network device **25** which may include a wireless access point, etc.

In FIG. **9B** at Step **108**, a second set of a plural different types of wireless or wired communications messages are sent from the second network device **25** to other selected ones of the one or more designed social contact network devices **16, 18, 22** and to one more social networking web-sites **19** over the non-mesh communications network **23**

24

indicating the first message network device **14** is physically located at the pre-determined distance **21** from pre-determined physical location of the second network device **25**. The second set of plural types of wireless and wired communications messages include an invitation message to join the owner of the first message network device **14** at the pre-determined physical location of the second network device **25**.

For example, there are likely mesh network devices and non-mesh network devices that are not on a mesh network **12** or partial mesh network **20** that are included in the user profile information **91** associated with the first mesh network device **14, 26, 56**. Such devices are contacted using a non-mesh network **23** such as the Internet, PSTN, an intranet, etc.

In one embodiment, if the second network device is successful using Step **106** to contact a designated social contact network device, then Step **108** is not executed. In another embodiment, both step **106** and **108** are executed to ensure all designate social contact network devices are contacted on mesh networks and non-mesh networks.

In one embodiment, the first set and second set of the plural different types of wireless communications messages include an IEEE 802.15.4 (ZigBee), IEEE 802.11a, 802.11b, 802.11g, 802.11n, 802.16a, 802.16g, Bluetooth or Infrared wireless protocol communications messages. However, the present invention is not limited to the wireless communications messages described and more, fewer or other types of wireless communications messages can also be used to practice the invention.

Activity Event Mesh Network Device Dynamic Information Exchange

FIGS. **10A** and **10B** are a flow diagram illustrating a Method **110** for dynamic information interchange for location aware mesh network devices. In FIG. **10A** at Step **112**, a selected type of wireless communications message from a first set of plural wireless activity messages is sent over a wireless mesh network or a wireless non-mesh communications network from a first mesh network device with one or more processors to a second network device with one or more processors located at a pre-determined physical location. The first mesh network device includes an ultra wide-band wireless transceiver and a mesh network protocol adapter with Complementary Code Keying (CCK), Differential Quaternary Phase Shift Keying (DQPSK) or Orthogonal Frequency Division Multiplexing (OFDM) encoders. The first set of plural wireless activity messages includes: a first type of wireless activity message including a security identification authorization message to determine if the first mesh network device is allowed access to a secure area within a pre-determined distance of the pre-determined physical location of the second network device, a second type of wireless activity message including a building management message to dynamically and automatically manage heating, ventilation or air conditioning (HVAC) of an area with the pre-determined distance of the pre-determined physical location of the second network device, or a third type of wireless activity message including a emergency location information message that includes physical location information to dynamically and automatically locate the first mesh network device at a three dimensional (3D) physical location in the building at the pre-determined physical location of the second network device in the event of an emergency situation. At Step **114**, the first mesh network device receives over the wireless mesh network or the wireless non-mesh communications network from the second network device a request for a first set of profile

25

information stored on the first mesh network device in response to sending the selected type of wireless communications message. At Step 116, the first set of profile information is sent from the first mesh network device to the second network device over the wireless mesh network or the wireless non-mesh communications network. In FIG. 10B At Step 118, one or more wireless acknowledgement messages are received on the first mesh network device from the second network device over the wireless mesh network or the wireless non-mesh communications network indicating that the second network device has acknowledged the first mesh network device being physically located within the pre-determined distance of the physical location of the second network device.

FIG. 11A is a block diagram 120 illustrating a mesh activity message 122 for entering a secure area 124.

FIG. 11B is a block diagram 126 illustrating a mesh activity message 128 for automatically and dynamically managing HVAC 130.

FIG. 11C is a block diagram illustrating a mesh activity message 132 for providing 3D emergency location information 134.

Method 110 is illustrated with one exemplary embodiment. However, the present invention is not limited to such an embodiment and other embodiments can also be used to practice the invention.

In such an exemplary embodiment in FIG. 10A at Step 112, selected type of wireless communications message from a first set of plural wireless activity messages is sent over a wireless 3 mesh network 12 or a wireless non-mesh communications network 23 from a first mesh network device (e.g., 14, 26, 56, etc.) with one or more processors to a second network device 25 with one or more processors located at a pre-determined physical location. The first mesh network device 14, 26, 56 includes an ultra wideband wireless transceiver 40 and a mesh network protocol adapter with Complementary Code Keying (CCK), Differential Quaternary Phase Shift Keying (DQPSK) or Orthogonal Frequency Division Multiplexing (OFDM) encoders.

The first set of plural wireless activity messages includes the first type of wireless activity message 122 (FIG. 11A) including a security identification authorization message to determine if the first mesh network device 14, 26, 56, is allowed access to a secure area 124 (e.g., room, laboratory, building, etc.) within a pre-determined distance 21 of the pre-determined physical location of the second network device 25.

The first set of plural wireless activity messages further includes the second type of wireless activity message 128 (FIG. 11B) including a building management message to dynamically and automatically manage heating, ventilation or air conditioning (HVAC) 130 of an area with the pre-determined distance 21 of the pre-determined physical location of the second network device 25.

The first set of plural wireless activity messages further includes the third type of wireless activity message 134 (FIG. 11C) including a emergency location information message that includes physical location information to dynamically and automatically locate the first mesh network device 14, 26, 56 at a three dimensional (3D) physical location 136 in the building at the pre-determined physical location of the second network device 25 in the event of an emergency situation.

Returning to FIG. 10A at Step 114, the first mesh network device 14, 26, 56 receives over the wireless 3 mesh network 12 or the wireless non-mesh communications network 23 from the second network device 25 a request for a first set

26

of profile information stored on the first mesh network device 14, 26, 56 in response to sending the selected type of wireless communications message.

At Step 116, the first set of profile information is sent from the first mesh network device 14, 26, 56 to the second network device 25 over the wireless 3 mesh network 12 or the wireless non-mesh communications network 23.

In FIG. 10B at Step 118, one or more wireless acknowledgement messages are received on the first mesh network device 14, 26, 56 from the second network device 25 over the wireless 3 mesh network 12 or the wireless non-mesh communications network 23 indicating that the second network device 25 has acknowledged the first mesh network device 14, 26, 56 being physically located within the pre-determined distance of the physical location of the second network device 25.

In one embodiment, Method 110 further includes the additional steps of: the selected type of wireless communications message is received over the wireless 3 mesh network 12 or a wireless non-mesh communications network 23 on the second network device 25. The second network device 25 sends the first mesh network device 14, 26, 56 over the wireless 3 mesh network 12 or the wireless non-mesh communications network 23 a request for a first set of profile information 91 stored on the first mesh network device 14, 26, 56 in response to receiving the selected type of wireless communications message. The first set of profile information 91 from the first mesh network device 14, 26, 56 is received on the second network device 25 over the wireless 3 mesh network 12 or the wireless non-mesh communications network 23. The one or more wireless acknowledgement messages are sent to the first mesh network device 14, 26, 56 from the second network device 25 over the wireless 3 mesh network 12 or the wireless non-mesh communications network 23 indicating that the second network device 25 has acknowledged the first mesh network device 14, 26, 26 being physically located within the pre-determined distance 21 of the physical location of the second network device 25. The first set of profile information 91 is stored in a non-transitory computer readable medium (e.g., database, etc.) on the second network device 25 to indicate the first mesh network device being physically located within the pre-determined distance 21 of the physical location of the second network device 25. However, the present invention is not limited the additional steps described and more, fewer or other steps can also be used to practice the invention.

The dynamic information exchange includes allowing a mesh network device to communicate location information with a network device at pre-determined physical location and invite social contacts of the mesh network device to come to the pre-determined physical location. The network device sends various types of electronic messages (e.g., text message, e-mail, etc.) on a mesh network and/or a non-mesh communications network (e.g., the Internet, etc.) and to social networking sites. The dynamic information exchange also includes exchanging plural activity messages including a security identification authorization message for allowing access to a secure area, a building management message for automatically and dynamically managing heating, ventilation and/or air conditioning (HVAC) and/or an emergency location message for providing three-dimensional (3D) emergency location information.

The dynamic information exchange includes allowing a mesh network device to communicate location information with a network device at pre-determined physical location and invite social contacts of the mesh network device to

come to the pre-determined physical location. The network device sends various types of electronic messages (e.g., voice, text message, e-mail, etc.) on a mesh network and/or a non-mesh communications network (e.g., the Internet, etc.) and to social networking sites. The dynamic information exchange also includes exchanging plural activity messages including a security identification authorization message, a building management message and/or an emergency location message.

Bar Codes

A “barcode” is an optical machine-readable representation of data, which shows data about the object to which it attaches. Originally, barcodes represented data by varying the widths and spacings of parallel lines, and may be referred to as linear or 1 dimensional (1D). Later they evolved into rectangles, dots, hexagons and other geometric patterns in 2 dimensions (2D). Although 2D systems use a variety of symbols, they are generally referred to as barcodes as well. Barcodes originally were scanned by special—optical scanners called barcode readers, scanners and interpretive software are available on devices including desktop printers (not illustrated) and smart phones **16** and tablet computers **22**.

Table 3 illustrates exemplary linear barcodes, the standards of all of which are incorporated by reference. However, the present invention is not limited to the exemplary linear barcodes listed in Table 3, and more fewer and other linear barcodes can also be used to practice the invention.

TABLE 3

Linear Bar Codes	
U.P.C.	
Codabar	
Code 25 - Non-interleaved 2 of 5	
Code 25 - Interleaved 2 of 5	
Code 39	
Code 93	
Code 128	
Code 128A	
Code 128B	
Code 128C	
Code 11	
CPC Binary	
DUN 14	
EAN 2	
EAN 5	
EAN 8, EAN 13	
Facing Identification Mark	
GS1-128 (formerly known as UCC/EAN-128), incorrectly referenced as EAN 128 and UCC 128	
GS1 DataBar, formerly Reduced Space Symbology (RSS)	
HIBC (HIBCC Health Industry Bar Code)	
ITF-14	
Latent image barcode	
Pharmacode	
Plessey	
PLANET	
POSTNET	
Intelligent Mail barcode	
MSI	
PostBar	
RM4SCC/KIX	
JAN	
Telepen	

Table 4 illustrates exemplary matrix (2D) barcodes, the standards of all of which are incorporated by reference. However, the present invention is not limited to the exemplary matrix barcodes listed in Table 4, and more fewer and other matrix barcodes can also be used to practice the invention.

TABLE 4

Matrix Bar Codes	
	3-DI
	ArrayTag
	Aztec Code
	Small Aztec Code
	Chromatic Alphabet
	Codablock
	Code 1
	Code 16K
	Code 49
	ColorCode
	Compact Matrix Code
	CP Code
	CyberCode
	d-touch
	DataGlyphs
	Datamatrix
	Datastrip Code
	Dot Code A
	EZcode
	Grid Matrix Code
	High Capacity Color Barcode
	HueCode
	INTACTA.CODE
	InterCode
	JAGTAG
	Lorem ipsum
	MaxiCode
	mCode
	MiniCode
	MicroPDF417
	MMCC
	Nintendo e-Reader#Dot code
	Optar
	PaperDisk
	PDF417
	PDMark
	QR Code
	QuickMark Code
	SmartCode
	Snowflake Code
	ShotCode
	SPARQCode
	SuperCod
	Trillcode
	UltraCode
	UnisCode
	VeriCode, VSCode
	WaterCode

In one specific embodiment, application **61** interacts with a bar code reader application. However, the present invention is not limited to a bar code reader application and other applications can also be used to practice the invention.

In one specific exemplary embodiment, a QR bar code is used. However, the present invention is not limited to QR codes and other types of bar codes can also be used to practice the invention

A “QR Code” is a specific matrix barcode (or two-dimensional code), readable by dedicated QR barcode readers and camera phones. The code consists of black modules arranged in a square pattern on a white background. The information encoded can be text, URL or other data. QR codes are defined in ISO/IEC 18004:2006 Information technology—Automatic identification and data capture techniques—QR Code 2005 bar code symbology specification, 1 Sep. 2006, the contents of which are incorporated by reference.

Users with a camera equipped smart phone **16** (or tablet computer **22**, etc.) with a the camera component, a bar code reader application appropriate for the bar code processes the digital image of the QR Code can include a QR Code **166** (FIG. **14**). The camera component is used to capture existing

QR codes from print and electronic documents and other sources (e.g., from other network devices, etc.)

QR codes **166** are also used to display text, contact information, connect to a wireless network, open a web page in the phone's browser, download music, communicate a social event or electronic coupon, or initiate a communications event over the communications networks **12**, **20**, **23** (e.g., voice call, data call, etc.) This act of linking from physical world objects is known as a "hardlink" or "physical world hyperlinks."

For example, Google's smart phone Android operating system supports the use of QR codes by natively including the barcode scanner (e.g., Zxing, etc.) on some models, and the browser supports Uniform Resource Identifier (URI) redirection, which allows QR Codes to send metadata to existing applications on the device. Nokia's Symbian operating system is also provided with a barcode scanner, which is able to read QR codes, while mbarcode is a QR code reader for the Maemo operating system. In the Apple iOS, a QR code reader is not natively included, but hundreds of free applications available with reader and metadata browser URI redirection capability. However, the present invention is not limited to these network device operating systems and other bar code readers and device operating systems can also be used to practice the invention.

In one embodiment, a user may scan a number of QR bar codes **166** from non-electronic information such as magazines, business cards, billboards, other non-electronic advertising, etc. A user may also scan a number of QR bar codes **166** from electronic advertising such from web-sites, other target network devices **14**, **16**, **18**, **22**, from e-mails, text messages, instant messages, etc.

Location Event Mesh Network Device Dynamic Information Exchange

Mobile location aware devices automatically exchange information with other mobile location aware devices that are located at a pre-determined distance of each other at a desired physical location. A server network device compares electronic profiles that include stated interests of the mobile location aware devices. The server network device also provides additional information based on stated interests in the electronic profiles.

FIGS. **12A** and **12B** are a flow diagram illustrating a Method **138** for dynamic information exchange for location aware network devices.

FIG. **13** is a block diagram **154** illustrating a data flow **156** for Method **148** of FIG. **12**.

FIG. **14** is a block diagram **164** illustrating display of an exemplary QR bar code **166**. The QR bar code **166** in FIG. **14** is an actual valid, QR bar code generated and including the encoded text "This QR code generated by Ray Wang."

At FIG. **12A** at Step **140**, a first wireless message is received including a first set of profile information from a first mesh network device with one or more processors on a server network device with one or more processors over a wireless communications network. The first wireless message includes a request to track a physical location of the first mesh network device. The first wireless message includes comparison information that is used to connect the first mesh network device with one or more other mesh network devices that have similar comparison information. The first mesh network device includes an ultra-wideband wireless transceiver and a mesh network protocol adapter with Complementary Code Keying (CCK), Differential Quaternary Phase Shift Keying (DQPSK) or Orthogonal Frequency Division Multiplexing (OFDM) encoders. At Step **142**, the first set of profile information is stored in a

database associated with the server network device. At Step **144**, a current physical location of the first mesh network device is tracked from the server network device via the wireless communications network. At Step **146**, a second wireless message is received on the server network device via the wireless communications network indicating the first mesh network device is located at a new physical location. In FIG. **12B** at Step **148**, the server network device compares the stored first set of profile information from the first mesh network device to a plural other stored sets of profile information from plural other mesh network devices that have comparison information similar to the first mesh network device. At Step **150**, one or more third wireless messages are received from the server network device via the wireless communications network to the first mesh network device and one or more of the plural other mesh network devices that are located within a pre-determined distance of the new physical location of the first mesh network device and have comparison information similar to the first mesh network device. At Step **152**, one or more fourth wireless messages are automatically exchanged between the first mesh network device, the one or more of the plural other mesh network devices and the server network device via the wireless communications network. Selected ones one or more fourth wireless messages including a first set of additional information generated by the server network device as a result of the match in the comparison information. Other selected ones include a second set of additional information generated by the first mesh network device and the one or more of the plural other mesh network devices as the result of the match in comparison information and the pre-determined distance of the new physical location.

Method **138** is illustrated with one exemplary embodiment. However, the present invention is not limited to such an embodiment and other embodiments can also be used to practice the invention.

In such an exemplary embodiment in FIG. **12A** at Step **140**, a first wireless message is received including a first set of profile information **91**, **160** from a first mesh network device (e.g., smart phone **16**, **26**, etc.) with one or more processors on a server network device (e.g., **25**) with one or more processors over a wireless communications network **12**, **20**, **23**. The wireless communications includes a mesh network **12**, **20** or a non-mesh network **23**. However, the present invention is not limited to such an embodiment and more, fewer and other types of wireless networks can be used to practice the invention.

The first wireless message includes a request to track a physical location of the first mesh network device **16**. In one embodiment, the profile gives the server network device **25** an indication to track the first mesh network device through GPS, through cell tower reference locations or using other types of physical location information. The first message can also restrict the location tracking frequency to specific geographic areas and/or specific days and/or specific time periods during a day.

The first wireless message includes comparison information that is used to connect the first mesh network device **16** with one or more other mesh network devices **14**, **18**, **22** that have similar comparison information. The first mesh network device **16** includes an ultra-wideband wireless transceiver and a mesh network protocol adapter with Complementary Code Keying (CCK), Differential Quaternary Phase Shift Keying (DQPSK) or Orthogonal Frequency Division Multiplexing (OFDM) encoders.

In one embodiment, first mesh network device 16 includes a software application 61 as was described above and uses wireless hardware interfaces included on first mesh network device 16 to practice the invention. The software application 61 includes software for ultra-wideband wireless transceiver and a mesh network protocol adapter with Complementary Code Keying (CCK), Differential Quaternary Phase Shift Keying (DQPSK) or Orthogonal Frequency Division Multiplexing (OFDM) encoders. In a specific embodiment, the software application 61 functions as a virtual machine on the first mesh network 16. However, the present invention is not limited to such embodiment and more, fewer and other types of wireless transceivers and mesh network protocol adapters can be used to practice the invention. (e.g. FIG. 9, etc.). The invention may also be practiced with or without software application 61.

In one embodiment, the profile includes text, voice, electronic text, QR barcode information, etc. is created according to templates offered by an information provider. Templates can also be downloaded through 3rd parties over wired or wireless network connections. Users can also create their own templates according to specified syntax and rules. However, the present invention is not limited to such embodiment and more, fewer and other types profiles can be used to practice the invention.

At Step 142, the first set of profile information 91, 160 is stored in a database 25' associated with the server network device 25 (e.g., FIG. 7, etc.).

At Step 144, a current physical location of the first mesh network device 16 is tracked from the server network device 25 via the wireless communications network 12, 20, 23 (e.g., FIG. 4, FIG. 10, FIG. 11, etc.). The current physical location information, includes, but is not limited to, Global Positioning Satellite (GPS), cellular telephone tower information, street address information, two-dimensional (2D) (e.g., X,Y) (e.g., building, floor), three-dimensional (3D) (X, Y, Z) (e.g., building, floor, floor location) or other types of physical location information.

At Step 146, a second wireless message is received on the server network device 25 via the wireless communications network 12, 20, 23 indicating the first mesh network device 16 is located at a new physical location.

In FIG. 12B at Step 148, the server network device 25 compares the stored first set of profile information 91, 160 from the first mesh network device 16 to a plural other stored sets of profile information (e.g., 91', 160', etc.) from plural other mesh network devices 14, 18, 22 that have comparison information similar to the first mesh network device 16 (e.g., FIGS. 4, 6, 8, 9, 10, 11, etc.).

At Step 150, one or more third wireless messages are received from the server network device 25 via the wireless communications network 18 to the first mesh network device 16, 26 and one or more of the plural other mesh network devices 14, 18, 22 that are located within a pre-determined distance 21 of the new physical location of the first mesh network device 16, 26 and have comparison information (e.g., 91, 91', 160, 160') similar to the first mesh network device 16, 26 (e.g., FIGS. 4, 6, 9, 10, 11, etc.).

At Step 152, one or more fourth wireless messages are exchanged automatically between the first mesh network device 16, 26, the one or more of the plural other mesh network devices 14, 18, 22 and the server network device 25 via the wireless communications network 12, 20, 23. Selected ones or more fourth wireless messages including a first set of additional information 158 generated by the server network device 25 as a result of the match in the comparison information (e.g., 91, 91', 160, 160', etc.). Other

selected ones include a second set of additional information 162 generated by the first mesh network device 16, 26 and the one or more of the plural other mesh network devices 14, 18, 22 as the result of the match in comparison information (e.g., 91, 91', 160, 160' etc.) and the pre-determined distance 21 of the new physical location (e.g., FIGS. 4-11, etc.).

Selected ones or more fourth wireless messages including a first set of additional information 158 generated by the server network device 25 as a result of the match in the comparison information (e.g., 91, 91', 160, 160', etc.) include electronic information with electronic links (e.g., Hyper Text Markup Language (HTML) links, Universal Resource Locator (URLs) links, etc.) to other web-sites or other sites on the communications network 12, 20, 23. However, the present invention is not limited to such embodiment and more, fewer and other types of electronic links can be used to practice the invention.

In one embodiment, the other selected ones of the one or more fourth wireless messages including the first set of additional information 158 includes preferences for mobile commerce information, advertising information, electronic coupon information (e.g., from GROUPON, SOCIAL LIVING, etc.), social networking information (e.g., FACEBOOK, TWITTER, etc.), dating information (e.g., MATCH.COM, EHARMONY.COM, etc.), lost and found information, and/or physical presence information. However, the present invention is not limited to such embodiment and more, fewer and other types of additional information can be used to practice the invention.

In another embodiment, the other selected ones of the one or more fourth wireless messages including the second set of additional information 162 includes exchange of an e-mail address, a name, a street address, a telephone number, an instant message identifier, a text message identifier, an encryption key, a mesh network identifier, a physical location information, a QR barcode 166, a dating web-site identifier, and/or a social networking web-site login identifier. However, the present invention is not limited to such embodiment and more, fewer and other types of additional information can be used to practice the invention.

The mobile commerce information includes when a profile matches desired mobile commerce preferences, a product offering and with a merchant's product (e.g., price and picture of the product, etc.) and location (e.g., map and contact information, etc.) is sent to the mesh network device.

The advertising information includes when a profile matches desired advertising preferences and the mesh network device is within the pre-determined distance of a physical location, product advertising (e.g., price and picture of the product, etc.) is sent to the mesh network device.

The electronic coupon information includes when a profile matches desired electronic coupon preferences and the mesh network device is within the pre-determined distance of a physical location, an electronic coupon along with the description (e.g., item type, color, price, location, etc.) is sent to the mesh network device.

The social networking information includes when a profile matches desired social networking preferences and the mesh network device is within the pre-determined distance of a physical location, social networking information and location information is sent to the mesh network device.

The dating information includes when dating profiles match, and the mesh network devices are within the pre-determined distance of a physical location, interested parties sent dating information and location information is sent to mesh network devices.

The lost and found information includes when lost and found profile information matches for a lost item, a lost pet, a lost person, and the mesh network device is within the pre-determined distance of a physical location, lost and found information including the item's description (e.g., 5 item type, model, brand, color, height, weight, sex, type of pet, lost location, found location, etc.), E911/911 information, weather information, AMBER alert/missing child information, etc. is sent to the mesh network device.

However, the present invention is not limited to such embodiments and more, fewer and other types of information can be used to practice the invention. 10

In one embodiment, the one or more fourth wireless messages include a voice message, an e-mail message, a text message and/or an instant message. 15

However, the present invention is not limited to such embodiment and more, fewer and other types of wireless and/or wired messages can be used to practice the invention.

In another embodiment, the invention is practiced on a wired network, or various combinations thereof of wireless 20 and wired devices and/or networks.

The method and system described herein includes mobile location aware devices that automatically exchange information with other mobile location aware devices located at a pre-determined distance of each other at a desired physical 25 location. A server network device compares electronic profiles that include stated interests of the mobile location aware devices. The server network device provides additional information to the mobile location aware devices based on stated interests in the electronic profiles. 30

It should be understood that the architecture, programs, processes, methods and It should be understood that the architecture, programs, processes, methods and systems described herein are not related or limited to any particular type of computer or network system (hardware or software), 35 unless indicated otherwise. Various types of general purpose or specialized computer systems may be used with or perform operations in accordance with the teachings described herein.

In view of the wide variety of embodiments to which the principles of the present invention can be applied, it should be understood that the illustrated embodiments are exemplary only, and should not be taken as limiting the scope of the present invention. For example, the steps of the flow diagrams may be taken in sequences other than those 45 described, and more or fewer elements may be used in the block diagrams.

While various elements of the preferred embodiments have been described as being implemented in software, in other embodiments hardware or firmware implementations 50 may alternatively be used, and vice-versa.

The claims should not be read as limited to the described order or elements unless stated to that effect. In addition, use of the term "means" in any claim is intended to invoke 35 U.S.C. §112, paragraph 6, and any claim without the word "means" is not so intended. 55

Therefore, all embodiments that come within the scope and spirit of the following claims and equivalents thereto are claimed as the invention.

I claim:

1. A method for dynamic information interchange for mesh network devices, comprising:

receiving a first wireless message including a first set of profile information from a first mesh network device with one or more processors on a server network device 60 with one or more processors over a wireless communications network, 65

wherein the first wireless message includes a request to track a physical location of the first mesh network device,

wherein the first wireless message includes comparison information that is used to connect the first mesh network device with one or more other mesh network devices that have similar comparison information, and wherein the first mesh network device includes an ultra-wideband wireless transceiver and a mesh network protocol adapter with Complementary Code Keying (CCK), Differential Quaternary Phase Shift Keying (DQPSK) or Orthogonal Frequency Division Multiplexing (OFDM) encoders;

storing the first set of profile information in a database associated with the server network device;

tracking a current physical location of the first mesh network device from the server network device via the wireless communications network;

receiving a second wireless message on the server network device via the wireless communications network indicating the first mesh network device [has] is located at a new physical location;

comparing on the server network device the stored first set of profile information from the first mesh network device to a plurality of other stored sets of profile information from a plurality of other mesh network devices that have comparison information similar to the first mesh network device;

sending one or more third wireless messages from the server network device via the wireless communications network to the first mesh network device and one or more of the plurality of other mesh network devices that are located within a pre-determined distance of the new physical location of the first mesh network device and have comparison information similar to the first mesh network device; and

exchanging automatically [one or more] *a plurality of* fourth wireless messages between the first mesh network device, the one or more of the plurality of other mesh network devices and the server network device via the wireless communications network, wherein selected ones of the [one or more] *plurality of* fourth wireless messages [including] *include* a first set of additional information generated by the server network device as a result of the match in the comparison information and other selected ones of the [one or more] *plurality of* fourth wireless messages [includes] *include* a second set of additional information generated by the first mesh network device and the one or more of the plurality of other mesh network devices as the result of the match in comparison information and the pre-determined distance of the new physical location.

2. A non-transitory computer readable medium having stored therein a plurality of instructions for causing one or more processors to execute the steps of:

receiving a first wireless message including a first set of profile information from a first mesh network device with one or more processors on a server network device with one or more processors over a wireless communications network,

wherein the first wireless message includes a request to track a physical location of the first mesh network device,

wherein the first wireless message includes comparison information that is used to connect the first mesh

35

network device with one or more other mesh network devices that have similar comparison information, and wherein the first mesh network device includes an ultra-wideband wireless transceiver and a mesh network protocol adapter with Complementary Code Keying (CCK), Differential Quaternary Phase Shift Keying (DQPSK) or Orthogonal Frequency Division Multiplexing (OFDM) encoders;

storing the first set of profile information in a database associated with the server network device;

tracking a current physical location of the first mesh network device from the server network device via the wireless communications network;

receiving a second wireless message on the server network device via the wireless communications network indicating the first mesh network device [has] is located at a new physical location;

comparing on the server network device the stored first set of profile information from the first mesh network device to a plurality of other stored sets of profile information from a plurality of other mesh network devices that have comparison information similar to the first mesh network device;

sending one or more third wireless messages from the server network device via the wireless communications network to the first mesh network device and one or more of the plurality of other mesh network devices that are located within a pre-determined distance of the new physical location of the first mesh network device and have comparison information similar to the first mesh network device; and

exchanging automatically [one or more] *a plurality of* fourth wireless messages between the first mesh network device, the one or more of the plurality of other mesh network devices and the server network device via the wireless communications network, wherein selected ones of the [one or more] *plurality of* fourth wireless messages [including] *include* a first set of additional information generated by the server network device as a result of the match in the comparison information and other selected ones of the [one or more] *plurality of* fourth wireless messages [includes] *include* a second set of additional information generated by the first mesh network device and the one or more of the plurality of other mesh network devices as the result of the match in comparison information and the pre-determined distance of the new physical location.

3. The method of claim 1 wherein the first set of profile information includes an e-mail address, an Internet Protocol (IP) address, a hardware address, a universal resource locator (URL), a name, a street address, a telephone number, an instant message identifier, a text message identifier, an encryption key, a digital signature, a secure message digest, a security identifier, a mesh network identifier, a physical location information, a QR barcode, public or emergency notices or location specific information including location-aware information, an electronic coupon site identifier, a dating web-site identifier or a social networking web-site login identifier.

4. The method of claim 1 wherein the wireless communications messages include an IEEE 802.15.4 (ZigBee), IEEE 802.11a, 802.11b, 802.11g, 802.11n, 802.16a, 802.16g, Bluetooth or Infrared wireless protocol communications message.

5. The method of claim 1 wherein the [step of the step of sending] *receiving* a first wireless message includes securely

36

[sending] *receiving* the first wireless message from the first mesh network device [to] *with* the server network device using a pre-determined security method [over the wireless communications network].

6. The method of claim 1 wherein the one or more electronic identifiers for one or more designated location contact network devices include a telephone number, an e-mail identifier, an instant message identifier, a text message identifier, a mesh network identifier, a Radio Frequency Identifier (RFID) identifier a QR barcode identifier or a social networking web-site identifier.

7. The method of claim 1 wherein the first mesh network device includes a mobile telephone, personal digital/data assistant (PDA), smart phone, tablet computer, Radio Frequency Identification (RFID) tag, RFID sensor or RFID biometric tag mesh network device.

8. The method of claim 1 wherein the ultra-wideband wireless transceiver includes a Worldwide Interoperability for Microwave Access (WiMAX) wireless transceiver.

9. The method of claim 1 wherein the server network device further includes a gateway, router, switch, wired access point, wireless access point or Radio Frequency Identification (RFID) sensor portal, RFID tag portal, or RFID biometric tag portal network device.

10. The method of claim 1 wherein the similar comparison information includes desired preferences for mobile commerce information, advertising information, electronic coupon information, social networking information, dating information, lost and found information or physical presence information.

11. The method of claim 1 wherein the first set of profile information includes information decoded from a QR barcode.

12. The method of claim 1 wherein the first mesh network device includes a smart phone or a tablet computer.

13. The method of claim 12 wherein the first mesh network device includes a smart software application including a software mesh network protocol adapter.

14. The method of claim 1 wherein the selected ones of the [one or more] *plurality of* fourth wireless messages include mobile commerce information, advertising information, electronic coupon information, social networking information, dating information, lost and found information or physical presence information.

15. The method of claim 1 wherein the other selected ones of the [one or more] *plurality of* fourth wireless messages include an e-mail address, a name, a street address, a telephone number, an instant message identifier, a text message identifier, an encryption key, a mesh network identifier, a physical location information, a QR barcode, an electronic coupon identifier, a dating web-site identifier or a social networking web-site identifier.

16. The method of claim 1 wherein the [one or more] *plurality of* fourth wireless messages include a voice message, an e-mail message, a text message or an instant message.

17. The method of claim 1 wherein the current physical location includes Global Positioning Satellite (GPS) information, cellular telephone tower information, street address information, two-dimensional (2D) (X,Y) or three-dimensional (3D) (X, Y, Z) physical location information.

[18. A system for dynamic information interchange for mesh network devices, comprising in combination:
means for receiving a first wireless message including a first set of profile information from a first mesh network

37

device with one or more processors on a server network device with one or more processors over a wireless communications network,
 wherein the first wireless message includes a request to track a physical location of the first mesh network device,
 wherein the first wireless message includes comparison information that is used to connect the first mesh network device with one or more other mesh network devices that have similar comparison information, and
 wherein the first mesh network device includes an ultra-wideband wireless transceiver and a mesh network protocol adapter with Complementary Code Keying (CCK), Differential Quaternary Phase Shift Keying (DQPSK) or Orthogonal Frequency Division Multiplexing (OFDM) encoders;
 means for storing the first set of profile information in a database associated with the server network device;
 means for tracking a current physical location of the first mesh network device from the server network device via the wireless communications network;
 means for receiving a second wireless message on the server network device via the wireless communications network indicating the first mesh network device has is located at a new physical location;
 means for comparing on the server network device the stored first set of profile information from the first mesh network device to a plurality of other stored sets of profile information from a plurality of other mesh network devices that have comparison information similar to the first mesh network device;
 means for sending one or more third wireless messages from the server network device via the wireless communications network to the first mesh network device and one or more of the plurality of other mesh network devices that are located within a pre-determined distance of the new physical location of the first mesh network device and have comparison information similar to the first mesh network device; and
 means for exchanging automatically one or more fourth wireless messages between the first mesh network device, the one or more of the plurality of other mesh network devices and the server network device via the wireless communications network, wherein selected ones of the one or more fourth wireless messages including a first set of additional information generated by the server network device as a result of the match in the comparison information and other selected ones of the one or more fourth wireless messages includes a second set of additional information generated by the first mesh network device and the one or more of the plurality of other mesh network devices as the result of the match in comparison information and the pre-determined distance of the new physical location.]

19. A method for dynamic information interchange for mesh network devices, comprising:

receiving, with a server network device over a wireless communications network, a first wireless message including a first set of profile information from a first mesh network device, wherein the first wireless message includes a request to track a physical location of the first mesh network device and comparison information that is used to connect the first mesh network device with one or more other mesh network devices that have similar comparison information;
 storing the first set of profile information in a database associated with the server network device;

38

tracking a current physical location of the first mesh network device from the server network device via the wireless communications network;
 receiving a second wireless message on the server network device via the wireless communications network indicating the first mesh network device is located at a new physical location;
 comparing on the server network device the stored first set of profile information from the first mesh network device to a plurality of other stored sets of profile information from a plurality of other mesh network devices that have comparison information similar to the first mesh network device;
 sending one or more third wireless messages from the server network device via the wireless communications network to the first mesh network device and one or more of the plurality of other mesh network devices that are located within a pre-determined distance of the new physical location of the first mesh network device and have comparison information similar to the first mesh network device; and
 exchanging a plurality of fourth wireless messages between the first mesh network device, the one or more of the plurality of other mesh network devices and the server network device via the wireless communications network, wherein selected ones of the plurality of fourth wireless messages include additional information as a result of the match in the comparison information.

20. The method of claim 19 wherein the first set of profile information includes an e-mail address, an Internet Protocol (IP) address, a hardware address, a universal resource locator (URL), a name, a street address, a telephone number, an instant message identifier, a text message identifier, an encryption key, a digital signature, a secure message digest, a security identifier, a mesh network identifier, a physical location information, a QR barcode, public or emergency notices or location specific information including location-aware information, an electronic coupon site identifier, a dating web-site identifier or a social networking web-site login identifier.

21. The method of claim 19 wherein the receiving a first wireless message includes securely receiving the first wireless message from the first mesh network device with the server network device using a pre-determined security method.

22. The method of claim 19 wherein the one or more electronic identifiers for one or more designated location contact network devices include a telephone number, an e-mail identifier, an instant message identifier, a text message identifier, a mesh network identifier, a Radio Frequency Identifier (RFID) identifier a QR barcode identifier or a social networking web-site identifier.

23. The method of claim 19 wherein the similar comparison information includes desired preferences for mobile commerce information, advertising information, electronic coupon information, social networking information, dating information, lost and found information or physical presence information.

24. The method of claim 19 wherein the first set of profile information includes information decoded from a QR barcode.

25. The method of claim 19 wherein the selected ones of the plurality of fourth wireless messages include mobile commerce information, advertising information, electronic coupon information, social networking information, dating information, lost and found information or physical presence information.

39

26. The method of claim 19 wherein the other selected ones of the plurality of fourth wireless messages include an e-mail address, a name, a street address, a telephone number, an instant message identifier, a text message identifier, an encryption key, a mesh network identifier, a physical location information, a QR barcode, an electronic coupon identifier, a dating web-site identifier or a social networking web-site identifier.

27. The method of claim 19 wherein the plurality fourth wireless messages include a voice message, an e-mail message, a text message or an instant message.

28. The method of claim 19 wherein the current physical location includes Global Positioning Satellite (GPS) information, cellular telephone tower information, street address information, two-dimensional (2D) (X,Y) or three-dimensional (3D) (X, Y, Z) physical location information.

29. A system for dynamic information interchange for mesh network devices, the system comprising a database storage device and an associated server network device, wherein the server network device is configured to:

receive a first wireless message including a first set of profile information from a first mesh network device over a wireless communications network, wherein the first wireless message includes a request to track a physical location of the first mesh network device, and wherein the first wireless message includes comparison information that is used to connect the first mesh network device with one or more other mesh network devices that have similar comparison information;

store the first set of profile information in the database storage device associated with the server network device;

track a current physical location of the first mesh network device from the server network device via the wireless communications network;

receive a second wireless message via the wireless communications network indicating the first mesh network device is located at a new physical location;

compare the stored first set of profile information from the first mesh network device to a plurality of other stored sets of profile information from a plurality of other mesh network devices that have comparison information similar to the first mesh network device;

send one or more third wireless messages from the server network device via the wireless communications network to the first mesh network device and one or more of the plurality of other mesh network devices that are located within a pre-determined distance of the new physical location of the first mesh network device and have comparison information similar to the first mesh network device; and

exchange a plurality of fourth wireless messages between the first mesh network device, the one or more of the plurality of other mesh network devices and the server network device via the wireless communications network, wherein selected ones of the plurality of fourth wireless messages include a first set of additional information generated by the server network device as a result of the match in the comparison information and other selected ones of the plurality of fourth wireless messages include a second set of additional information generated by the first mesh network device and the one or more of the plurality of other mesh network devices as the result of the match in comparison information and the pre-determined distance of the new physical location.

40

30. The system of claim 29 wherein the first set of profile information includes an e-mail address, an Internet Protocol (IP) address, a hardware address, a universal resource locator (URL), a name, a street address, a telephone number, an instant message identifier, a text message identifier, an encryption key, a digital signature, a secure message digest, a security identifier, a mesh network identifier, a physical location information, a QR barcode, public or emergency notices or location specific information including location-aware information, an electronic coupon site identifier, a dating web-site identifier or a social networking web-site login identifier.

31. The system of claim 29 wherein the server network device is further configured to securely receive the first wireless message from the first mesh network device using a pre-determined security method.

32. The system of claim 29 wherein the one or more electronic identifiers for one or more designated location contact network devices include a telephone number, an e-mail identifier, an instant message identifier, a text message identifier, a mesh network identifier, a Radio Frequency Identifier (RFID) identifier a QR barcode identifier or a social networking web-site identifier.

33. The system of claim 29 wherein the similar comparison information includes desired preferences for mobile commerce information, advertising information, electronic coupon information, social networking information, dating information, lost and found information or physical presence information.

34. The system of claim 29 wherein the selected ones of the plurality of fourth wireless messages include mobile commerce information, advertising information, electronic coupon information, social networking information, dating information, lost and found information or physical presence information.

35. The system of claim 29 wherein the other selected ones of the plurality of fourth wireless messages include an e-mail address, a name, a street address, a telephone number, an instant message identifier, a text message identifier, an encryption key, a mesh network identifier, a physical location information, a QR barcode, an electronic coupon identifier, a dating web-site identifier or a social networking web-site identifier.

36. The system of claim 29 wherein the plurality of fourth wireless messages include a voice message, an e-mail message, a text message or an instant message.

37. The system of claim 29 wherein the current physical location includes Global Positioning Satellite (GPS) information, cellular telephone tower information, street address information, two-dimensional (2D) (X,Y) or three-dimensional (3D) (X, Y, Z) physical location information.

38. A non-transitory computer readable medium having stored therein a plurality of instructions that, in response to being executed, cause a server network device to:

receive a first wireless message including a first set of profile information from a first mesh network device over a wireless communications network, wherein the first wireless message includes a request to track a physical location of the first mesh network device, and wherein the first wireless message includes comparison information that is used to connect the first mesh network device with one or more other mesh network devices that have similar comparison information;

store the first set of profile information in a database associated with the server network device;

track a current physical location of the first mesh network device via the wireless communications network;

41

receive a second wireless message via the wireless communications network indicating the first mesh network device is located at a new physical location;

compare on the server network device the stored first set of profile information from the first mesh network device to a plurality of other stored sets of profile information from a plurality of other mesh network devices that have comparison information similar to the first mesh network device;

send one or more third wireless messages from the server network device via the wireless communications network to the first mesh network device and one or more of the plurality of other mesh network devices that are located within a pre-determined distance of the new physical location of the first mesh network device and have comparison information similar to the first mesh network device; and

exchange a plurality of fourth wireless messages between the first mesh network device, the one or more of the plurality of other mesh network devices and the server network device via the wireless communications network, wherein selected ones of the plurality of fourth wireless messages include a first set of additional information generated by the server network device as a result of the match in the comparison information and other selected ones of the plurality of fourth wireless messages include a second set of additional information generated by the first mesh network device and the one or more of the plurality of other mesh network devices as the result of the match in comparison information and the pre-determined distance of the new physical location.

39. The non-transitory computer readable medium of claim 38 wherein the first set of profile information includes an e-mail address, an Internet Protocol (IP) address, a hardware address, a universal resource locator (URL), a name, a street address, a telephone number, an instant message identifier, a text message identifier, an encryption key, a digital signature, a secure message digest, a security identifier, a mesh network identifier, a physical location information, a QR barcode, public or emergency notices or location specific information including location-aware information, an electronic coupon site identifier, a dating web-site identifier or a social networking web-site login identifier.

40. The non-transitory computer readable medium of claim 38 wherein the plurality of instructions further cause the server network device to securely receive the first wireless message from the first mesh network device using a pre-determined security method.

41. The non-transitory computer readable medium of claim 38 wherein the one or more electronic identifiers for one or more designated location contact network devices include a telephone number, an e-mail identifier, an instant message identifier, a text message identifier, a mesh network identifier, a Radio Frequency Identifier (RFID) identifier a QR barcode identifier or a social networking web-site identifier.

42. The non-transitory computer readable medium of claim 38 wherein the similar comparison information includes desired preferences for mobile commerce information, advertising information, electronic coupon information, social networking information, dating information, lost and found information or physical presence information.

43. The non-transitory computer readable medium of claim 38 wherein the selected ones of the plurality of fourth wireless messages include mobile commerce information,

42

advertising information, electronic coupon information, social networking information, dating information, lost and found information or physical presence information.

44. The non-transitory computer readable medium of claim 38 wherein the other selected ones of the plurality of fourth wireless messages include an e-mail address, a name, a street address, a telephone number, an instant message identifier, a text message identifier, an encryption key, a mesh network identifier, a physical location information, a QR barcode, an electronic coupon identifier, a dating web-site identifier or a social networking web-site identifier.

45. The non-transitory computer readable medium of claim 38 wherein the plurality of fourth wireless messages include a voice message, an e-mail message, a text message or an instant message.

46. The non-transitory computer readable medium of claim 38 wherein the current physical location includes Global Positioning Satellite (GPS) information, cellular telephone tower information, street address information, two-dimensional (2D) (X,Y) or three-dimensional (3D) (X, Y, Z) physical location information.

47. A method for dynamic information interchange for mesh network devices, comprising:

sending a selected type of wireless communications message from a first set of a plurality of wireless activity messages from a mesh network device to a network device located at a pre-determined physical location, wherein the first set of plurality of wireless activity messages includes:

a first type of wireless activity message including a security identification authorization message to determine if the mesh network device is allowed access to a secure area within a pre-determined distance of the pre-determined physical location of the network device,

a second type of wireless activity message including a building management message to dynamically and automatically manage heating, ventilation or air conditioning (HVAC) of an area with the pre-determined distance of the pre-determined physical location of the network device, or

a third type of wireless activity message including a emergency location information message that includes physical location information to dynamically and automatically locate the mesh network device at a three dimensional (3D) physical location in the building at the pre-determined physical location of the network device in the event of an emergency situation;

receiving on the mesh network device from the network device a request for a first set of profile information stored on the mesh network device in response to sending the selected type of wireless communications message;

sending the first set of profile information from the mesh network device to the network device; and

receiving one or more wireless acknowledgement messages on the mesh network device from the network device indicating that the network device has acknowledged the mesh network device being physically located within the pre-determined distance of the physical location of the network device.

48. The method of claim 47 further comprising: receiving the selected type of wireless communications message on the network device; sending to the mesh network device from the network device a request for a first set of profile information

43

stored on the mesh network device in response to receiving the selected type of wireless communications message;

receiving the first set of profile information from the mesh network device on the network device;

sending one or more wireless acknowledgement messages to the mesh network device from the network device indicating that the network device has acknowledged the mesh network device being physically located within the pre-determined distance of the physical location of the network device; and

storing the first set of profile information in a non-transitory computer readable medium on the network device to indicate the mesh network device being physically located within the pre-determined distance of the physical location of the network device.

49. The method of claim 47 wherein the first set of profile information includes an e-mail address, an Internet Protocol (IP) address, a hardware address, a universal resource locator (URL), a name, a street address, a telephone number, an instant message identifier, a text message identifier, a encryption key, a digital signature, a secure message digest, a security identifier, a mesh network identifier, a physical location information, public or emergency notices or location specific information including location-aware information or a social networking web-site login identifier.

50. The method of claim 47 wherein the sending a selected type of wireless communications message includes securely sending the selected type of wireless message from the mesh network device to the network device using a pre-determined security method.

51. The method of claim 47 wherein the network device includes a server network device, a gateway, router, switch, wired access point, wireless access point or Radio Frequency Identification (RFID) sensor portal, RFID tag portal, or RFID biometric tag portal network device.

52. A non-transitory computer readable medium having stored therein a plurality of instructions, that in response to being executed, cause a mesh network device to:

send a selected type of wireless communications message from a first set of a plurality of wireless activity messages to a network device located at a pre-determined physical location, wherein the first set of plurality of wireless activity messages includes:

a first type of wireless activity message including a security identification authorization message to

44

determine if the mesh network device is allowed access to a secure area within a pre-determined distance of the pre-determined physical location of the network device,

a second type of wireless activity message including a building management message to dynamically and automatically manage heating, ventilation or air conditioning (HVAC) of an area with the pre-determined distance of the pre-determined physical location of the network device, or

a third type of wireless activity message including a emergency location information message that includes physical location information to dynamically and automatically locate the mesh network device at a three dimensional (3D) physical location in the building at the pre-determined physical location of the network device in the event of an emergency situation;

receive from the network device a request for a first set of profile information stored on the mesh network device in response to sending the selected type of wireless communications message;

send the first set of profile information to the network device; and

receive one or more wireless acknowledgement messages from the network device indicating that the network device has acknowledged the mesh network device being physically located within the pre-determined distance of the physical location of the network device.

53. The non-transitory computer readable medium of claim 52 wherein the first set of profile information includes an e-mail address, an Internet Protocol (IP) address, a hardware address, a universal resource locator (URL), a name, a street address, a telephone number, an instant message identifier, a text message identifier, a encryption key, a digital signature, a secure message digest, a security identifier, a mesh network identifier, a physical location information, public or emergency notices or location specific information including location-aware information or a social networking web-site login identifier.

54. The non-transitory computer readable medium of claim 52 wherein the plurality of instructions further cause the mesh network device to securely send the selected type of wireless message from the mesh network device to the network device using a pre-determined security method.

* * * * *