



(51) **International Patent Classification:**
H04W 12/04 (2009.01) H04W 12/12 (2009.01)
H04L 29/06 (2006.01)

(21) **International Application Number:**
PCT/US2011/031524

(22) **International Filing Date:**
7 April 2011 (07.04.2011)

(25) **Filing Language:** English

(26) **Publication Language:** English

(30) **Priority Data:**
61/321,553 7 April 2010 (07.04.2010) US

(71) **Applicant (for all designated States except US):** **INTER-DIGITAL PATENT HOLDINGS, INC.** [US/US]; 3411 Silverside Road, Concord Plaza, Suite 105, Hagley Building, Wilmington, DE 19810 (US).

(72) **Inventors; and**

(75) **Inventors/Applicants (for US only):** **STERNBERG, Gregory, S.** [US/US]; 7 Brookwood Road, Mount Laurel, NJ 08054 (US). **CASTOR, Douglas, R.** [US/US]; 8029 Fair View Lane, Norristown, PA 19403 (US). **SFAR, Sana** [TN/US]; 18 East Avenue, Atlantic Highlands, NJ 07716 (US). **KAUR, Samian, J.** [US/US]; 108 Campbell Drive, Conshohocken, PA 19428 (US). **PIETRASKI, Philip, J.** [US/US]; 7 Talbot Place, Huntington Station, NY 11746 (US). **YOGENDRA, Shah, C.** [GB/US]; 10 Regency Court, Exton, PA 19341 (US).

(74) **Agents:** **SAMUELS, Steven** et al.; Woodcock Washburn LLP, Cira Centre, 12th Floor, 2929 Arch Street, Philadelphia, PA 19104-2891 (US).

(81) **Designated States (unless otherwise indicated, for every kind of national protection available):** AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

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

Published:

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

(54) **Title:** METHOD AND SYSTEM FOR LASER AUTHENTICATION AND KEY ESTABLISHMENT

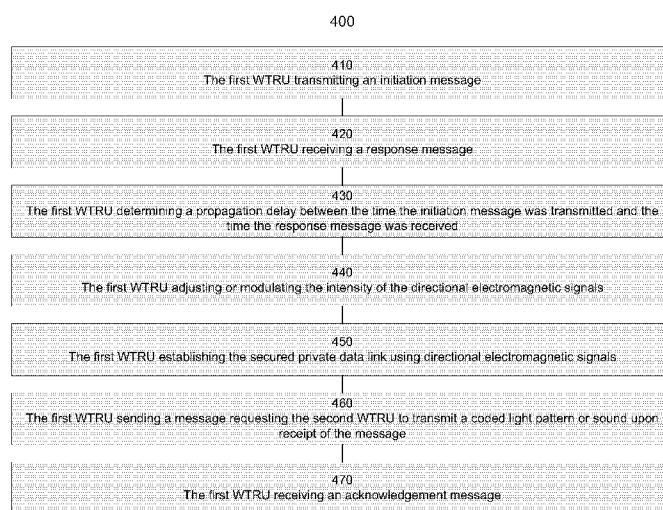


Figure 4

(57) **Abstract:** A vulnerable aspect of symmetric encryption systems is establishment of the key. During the key establishment, the key is often transmitted to authorized users; however, an unauthorized user may determine the key by eavesdropping. Directional electromagnetic signals, such as a laser, may be useful in preventing eavesdropping. For example, directional electromagnetic signals, such as laser signals, may be used to create a secured private data link associated with a secret key between a first wireless transmit/receive unit (WTRU) and a second WTRU.



METHOD AND SYSTEM FOR LASER AUTHENTICATION AND KEY ESTABLISHMENT

CROSS REFERENCE

[0001] This application claims the benefit of United States Provisional Patent Application No. 61/321,553, filed on April 7, 2010, the contents of which are hereby incorporated by reference in their entirety.

BACKGROUND

[0002] Symmetric key encryption systems are commonly used throughout the world of digital communications systems. Symmetric key encryption systems allow authorized users to maintain a private information link by encrypting data that can be decrypted by a key that is shared by the authorized users. A vulnerable aspect of these symmetric encryption systems is establishment of the key. Often the encryption key derived from a master key, which is provisioned on each end of the link or remotely provisioned. During the key establishment procedure, the parameters derived from the master key are often transmitted to authorized users; however, an unauthorized user may determine the key by eavesdropping. To prevent unauthorized users, systems use computationally difficult problems, such as factorization, to make the burden on the eavesdropper high in order to determine the key.

[0003] While the burden on the eavesdropper may be high, the eavesdropper may ultimately determine the key as computationally difficult problems are not impossible to crack. Other approaches used to prevent unauthorized users from determining a key include certificates.

SUMMARY

[0004] Disclosed herein are methods and systems for laser authentication and key establishment. This may be done, for example, to establish a secured private data link associated with a key by using directional electromagnetic signals.

[0005] In one example embodiment, directional electromagnetic signals may be used to create a secured private data link associated with a secret key between a first wireless transmit/receive unit (WTRU) and a second WTRU. The first WTRU may transmit an initiation message. The initiation message may indicate that the first WTRU wishes to establish the secured private data link associated with the secret key. The first WTRU may receive a response message. The

response message may notify the first WTRU to establish the secured private data link. The first WTRU may establish the secured private data link using directional electromagnetic signals. The first WTRU may receive an acknowledgement message. The acknowledgement message may indicate the secured private data link has been established.

[0006] In another example embodiment, directional electromagnetic signals may be used to create a secured private data link associated with a secret key between a first WTRU and a second WTRU. The first WTRU may receive an initiation message. The initiation message may indicate that the second WTRU wishes to establish the secured private data link associated with the secret key. The first WTRU may transmit a response message. The response message may notify the second WTRU to establish the secured private data link. The first WTRU may establish the secured private data link with the second WTRU using directional electromagnetic signals. The first WTRU may transmit an acknowledgement message. The acknowledgement message may indicate that the secured private data link has been established.

[0007] In another example embodiment, a WTRU may use directional electromagnetic signals to create a secured private data link associated with a secret key between the WTRU and a communications node. The WTRU may be configured to:

- transmit an initiation message, the initiation message indicating that the WTRU wishes to establish the secured private data link associated with the secret key;

- receive a response message, the response message notifying the WTRU to establish the secured private data link;

- establish the secured private data link using directional electromagnetic signals; and

- receive an acknowledgement message, the acknowledgement message indicating the secured private data link has been established.

[0008] This Summary is provided to introduce a selection of concepts in a simplified form that are further described below the Detailed Description. This Summary is not intended to identify key features or essential features of the claimed subject matter, nor is it intended to be used to limit the scope of the claimed subject matter. Furthermore, the claimed subject matter is not limited to limitations that solve any or all disadvantages noted in any part of this disclosure.

BRIEF DESCRIPTION OF THE DRAWINGS

[0009] A more detailed understanding may be had from the following description, given by way of example in conjunction with the accompanying drawings wherein:

[0010] Figure 1A is a system diagram of an example communications system in which one or more disclosed embodiments may be implemented;

[0011] Figure 1B is a system diagram of an example wireless transmit/receive unit (WTRU) that may be used within the communications system illustrated in Figure 1A;

[0012] Figure 1C is a system diagram of an example radio access network and an example core network that may be used within the communications system illustrated in Figure 1A;

[0013] Figure 2 illustrates an example embodiment of a system for using directional electromagnetic signals for authentication and key establishment.

[0014] Figure 3 illustrates another example embodiment of a system for using directional electromagnetic signals for authentication and key establishment.

[0015] Figure 4 illustrates an example embodiment of a method for using directional electromagnetic signals to create a secured private data link associated with a secret key between a first wireless transmit/receive unit (WTRU) and a second WTRU.

[0016] Figure 5 illustrates an example embodiment of a method for using directional electromagnetic signals to create a secured private data link associated with a secret key between a first WTRU and a second WTRU.

[0017] Figure 6 illustrates an example embodiment of a method for laser authentication and key establishment.

[0018] Figure 7 illustrates an example embodiment of a method for transmitting a message during laser authentication and key establishment.

[0019] Figure 8 illustrates an example embodiment of a method payment transaction using laser authentication and key establishment.

DETAILED DESCRIPTION OF ILLUSTRATIVE EMBODIMENTS

[0020] Symmetric key encryption systems allow authorized users to maintain a private information link by encrypting data that can only be decrypted by a key that is shared by the authorized users. A vulnerable aspect of these symmetric encryption systems is the establishment of the key. The key has to be shared or previously provisioned or

cryptographically protected and transmitted to authorized users; however, an unauthorized user may determine the key by eavesdropping. As disclosed herein, the use of directional electromagnetic signals, such as a laser beam, may be useful in preventing eavesdropping.

[0021] Directional electromagnetic signals, which may be any highly focused beam of electromagnetic radiation, may provide an extremely narrow beam on which information may be modulated. Because directional electromagnetic signals may provide a spatially coherent, narrow low-divergence beam, eavesdroppers may be avoided by focusing the directional electromagnetic signals on a specific target. For example, laser light may be focused on a specific target. Additionally, the directional electromagnetic signals may also be polarized to allow direct line of sight transmissions and to reduce the probability that an eavesdropper may receive signals from reflections.

[0022] Additionally, directional electromagnetic signals may be transmitted in the visible spectrum, which may be observed by the human eye. Transmitting directional electromagnetic signals in the visible spectrum may allow for the visual confirmation of an authentication procedure and a key establishment procedure. For example, the directional electromagnetic signals may be a green laser with Rayleigh scattering properties, as it may be visible when viewed from the side. Using such a laser, a user may be able to visually confirm that the laser has reached an intended recipient.

[0023] Directional electromagnetic signals, such as laser, may also have a high rate of data transfer that may allow a transmitter to pass large amounts of data to a receiver in a short amount of time. Due to the high rate of data transfer, directional electromagnetic signals may be used to provide authentication, short-range secure communication, and key transmission for long-range wireless communication. For example, a laser may be used to provide a cache of secret keys that may be used for secure short-range and/or long-range wireless communications. In one example embodiment, the laser may be used to transfer a cache of keys that may establish encryption, such as symmetric key encryption. The keys may then be buffered by a target user and may be used for secure wireless communications.

[0024] To further avoid eavesdroppers, directional electromagnetic signals may be used in conjunction with a receiver that has very low reflectivity. This may be done to minimize reflection, as any reflection of the directional electromagnetic signals may pose a risk to the security of the communication. To further minimize reflection, in one example embodiment, the directional electromagnetic signal transmitter and the receiver may be required to be aligned in such a way that reflections of the directional electromagnetic signals may be directed back toward the transmitted and/or receiver.

[0025] Additionally, the probability that an eavesdropper may reliably decode the transmitted key may be minimized by controlling the level or intensity at which the directional electromagnetic signals are transmitted. For example, the signal-to-noise ratio (SNR) at the intended receiver may be kept just above the detectability level to ensure that other receivers would not have sufficient SNR for reliable detection.

[0026] In one example embodiment, the intensity of the directional electromagnetic signals may be fixed and high to provide clear visibility. This may be done, for example, to retain the visibility of the carrier while controlling the power allocated to the information transmission. This may be achieved by setting the intensity of the directional electromagnetic signals according to:

[0027] $I(t) = C + A \cdot d(t)$

[0028] where C may be a fixed background intensity, A may be a modulation factor (the fraction of the symbol period during which the data is transmitted), and d(t) may be the information being transmitted. In one embodiment, the transmitter may gradually increase the modulation factor A while transmitting pseudo random coded packets and waiting for a response.

[0029] In another embodiment, the average laser intensity may be fixed to a level high enough to provide clear visibility. For example, the modulation factor A may be set to α in a set of slots and $(1-\alpha)$ in a different set of slots. The value of α may be initially a small number, or may be zero. Within each slot, α may be gradually increased; increasing the detectability while transmitting pseudo random coded packets and waiting for the expected response from the intended recipient.

[0030] In another example embodiment, the average intensity of the directional electromagnetic signals may always be fixed at or above a minimum to provide clear visibility. In some slots the directional electromagnetic signals may carry no information and may be used just for pointing. In other slots, the directional electromagnetic signals may be modulated in such a way that the data may be increasingly detectable while transmitting pseudo random coded packets and waiting for echo or other expected response.

[0031] Figure 1A is a diagram of an example communications system 100 in which one or more disclosed embodiments may be implemented. The communications system 100 may be a multiple access system that provides content, such as voice, data, video, messaging, broadcast, etc., to multiple wireless users. The communications system 100 may enable multiple wireless users to access such content through the sharing of system resources, including wireless

bandwidth. For example, the communications systems 100 may employ one or more channel access methods, such as code division multiple access (CDMA), time division multiple access (TDMA), frequency division multiple access (FDMA), orthogonal FDMA (OFDMA), single-carrier FDMA (SC-FDMA), and the like.

[0032] As shown in Figure 1A, the communications system 100 may include wireless transmit/receive units (WTRUs) 102a, 102b, 102c, 102d, a radio access network (RAN) 104, a core network 106, a public switched telephone network (PSTN) 108, the Internet 110, and other networks 112, though it will be appreciated that the disclosed embodiments contemplate any number of WTRUs, base stations, networks, and/or network elements. Each of the WTRUs 102a, 102b, 102c, 102d may be any type of device configured to operate and/or communicate in a wireless environment. By way of example, the WTRUs 102a, 102b, 102c, 102d may be configured to transmit and/or receive wireless signals and may include user equipment (UE), a mobile station, a fixed or mobile subscriber unit, a pager, a cellular telephone, a personal digital assistant (PDA), a smartphone, a laptop, a netbook, a personal computer, a wireless sensor, consumer electronics, and the like.

[0033] The communications systems 100 may also include a base station 114a and a base station 114b. The base stations 114 may also be communications nodes. Each of the base stations 114a, 114b may be any type of device configured to wirelessly interface with at least one of the WTRUs 102a, 102b, 102c, 102d to facilitate access to one or more communication networks, such as the core network 106, the Internet 110, and/or the networks 112. By way of example, the base stations 114a, 114b may be a base transceiver station (BTS), a Node-B, an eNode B, a Home Node B, a Home eNode B, a site controller, an access point (AP), a wireless router, and the like. While the base stations 114a, 114b are each depicted as a single element, it will be appreciated that the base stations 114a, 114b may include any number of interconnected base stations and/or network elements.

[0034] The base station 114a may be part of the RAN 104, which may also include other base stations and/or network elements (not shown), such as a base station controller (BSC), a radio network controller (RNC), relay nodes, etc. The base station 114a and/or the base station 114b may be configured to transmit and/or receive wireless signals within a particular geographic region, which may be referred to as a cell (not shown). The cell may further be divided into cell sectors. For example, the cell associated with the base station 114a may be divided into three sectors. Thus, in one embodiment, the base station 114a may include three transceivers, i.e., one for each sector of the cell. In another embodiment, the base station 114a may employ multiple-

input multiple output (MIMO) technology and, therefore, may utilize multiple transceivers for each sector of the cell.

[0035] The base stations 114a, 114b may communicate with one or more of the WTRUs 102a, 102b, 102c, 102d over an air interface 116, which may be any suitable wireless communication link (e.g., radio frequency (RF), microwave, infrared (IR), ultraviolet (UV), visible light, etc.). The air interface 116 may be established using any suitable radio access technology (RAT).

[0036] More specifically, as noted above, the communications system 100 may be a multiple access system and may employ one or more channel access schemes, such as CDMA, TDMA, FDMA, OFDMA, SC-FDMA, and the like. For example, the base station 114a in the RAN 104 and the WTRUs 102a, 102b, 102c may implement a radio technology such as Universal Mobile Telecommunications System (UMTS) Terrestrial Radio Access (UTRA), which may establish the air interface 116 using wideband CDMA (WCDMA). WCDMA may include communication protocols such as High-Speed Packet Access (HSPA) and/or Evolved HSPA (HSPA+). HSPA may include High-Speed Downlink Packet Access (HSDPA) and/or High-Speed Uplink Packet Access (HSUPA).

[0037] In another embodiment, the base station 114a and the WTRUs 102a, 102b, 102c may implement a radio technology such as Evolved UMTS Terrestrial Radio Access (E-UTRA), which may establish the air interface 116 using Long Term Evolution (LTE) and/or LTE-Advanced (LTE-A).

[0038] In other embodiments, the base station 114a and the WTRUs 102a, 102b, 102c may implement radio technologies such as IEEE 802.16 (i.e., Worldwide Interoperability for Microwave Access (WiMAX)), CDMA2000, CDMA2000 1X, CDMA2000 EV-DO, Interim Standard 2000 (IS-2000), Interim Standard 95 (IS-95), Interim Standard 856 (IS-856), Global System for Mobile communications (GSM), Enhanced Data rates for GSM Evolution (EDGE), GSM EDGE (GERAN), and the like.

[0039] The base station 114b in Figure 1A may be a wireless router, Home Node B, Home eNode B, or access point, for example, and may utilize any suitable RAT for facilitating wireless connectivity in a localized area, such as a place of business, a home, a vehicle, a campus, and the like. In one embodiment, the base station 114b and the WTRUs 102c, 102d may implement a radio technology such as IEEE 802.11 to establish a wireless local area network (WLAN). In another embodiment, the base station 114b and the WTRUs 102c, 102d may implement a radio technology such as IEEE 802.15 to establish a wireless personal area network (WPAN). In yet

another embodiment, the base station 114b and the WTRUs 102c, 102d may utilize a cellular-based RAT (e.g., WCDMA, CDMA2000, GSM, LTE, LTE-A, etc.) to establish a picocell or femtocell. As shown in Figure 1A, the base station 114b may have a direct connection to the Internet 110. Thus, the base station 114b may not be required to access the Internet 110 via the core network 106.

[0040] The RAN 104 may be in communication with the core network 106, which may be any type of network configured to provide voice, data, applications, and/or voice over internet protocol (VoIP) services to one or more of the WTRUs 102a, 102b, 102c, 102d. For example, the core network 106 may provide call control, billing services, mobile location-based services, pre-paid calling, Internet connectivity, video distribution, etc., and/or perform high-level security functions, such as user authentication. Although not shown in Figure 1A, it will be appreciated that the RAN 104 and/or the core network 106 may be in direct or indirect communication with other RANs that employ the same RAT as the RAN 104 or a different RAT. For example, in addition to being connected to the RAN 104, which may be utilizing an E-UTRA radio technology, the core network 106 may also be in communication with another RAN (not shown) employing a GSM radio technology.

[0041] The core network 106 may also serve as a gateway for the WTRUs 102a, 102b, 102c, 102d to access the PSTN 108, the Internet 110, and/or other networks 112. The PSTN 108 may include circuit-switched telephone networks that provide plain old telephone service (POTS). The Internet 110 may include a global system of interconnected computer networks and devices that use common communication protocols, such as the transmission control protocol (TCP), user datagram protocol (UDP) and the internet protocol (IP) in the TCP/IP internet protocol suite. The networks 112 may include wired or wireless communications networks owned and/or operated by other service providers. For example, the networks 112 may include another core network connected to one or more RANs, which may employ the same RAT as the RAN 104 or a different RAT.

[0042] Some or all of the WTRUs 102a, 102b, 102c, 102d in the communications system 100 may include multi-mode capabilities, i.e., the WTRUs 102a, 102b, 102c, 102d may include multiple transceivers for communicating with different wireless networks over different wireless links. For example, the WTRU 102c shown in Figure 1A may be configured to communicate with the base station 114a, which may employ a cellular-based radio technology, and with the base station 114b, which may employ an IEEE 802 radio technology.

[0043] Figure 1B is a system diagram of an example WTRU 102. As shown in Figure 1B, the WTRU 102 may include a processor 118, a transceiver 120, a transmit/receive element 122, a speaker/microphone 124, a keypad 126, a display/touchpad 128, non-removable memory 106, removable memory 132, a power source 134, a global positioning system (GPS) chipset 136, and other peripherals 138. It will be appreciated that the WTRU 102 may include any sub-combination of the foregoing elements while remaining consistent with an embodiment.

[0044] The processor 118 may be a general purpose processor, a special purpose processor, a conventional processor, a digital signal processor (DSP), a plurality of microprocessors, one or more microprocessors in association with a DSP core, a controller, a microcontroller, Application Specific Integrated Circuits (ASICs), Field Programmable Gate Array (FPGAs) circuits, any other type of integrated circuit (IC), a state machine, and the like. The processor 118 may perform signal coding, data processing, power control, input/output processing, and/or any other functionality that enables the WTRU 102 to operate in a wireless environment. The processor 118 may be coupled to the transceiver 120, which may be coupled to the transmit/receive element 122. While Figure 1B depicts the processor 118 and the transceiver 120 as separate components, it will be appreciated that the processor 118 and the transceiver 120 may be integrated together in an electronic package or chip.

[0045] The transmit/receive element 122 may be configured to transmit signals to, or receive signals from, a base station (e.g., the base station 114a) or another WTRU over the air interface 116. For example, in one embodiment, the transmit/receive element 122 may be an antenna configured to transmit and/or receive RF signals. In another embodiment, the transmit/receive element 122 may be an emitter/detector configured to transmit and/or receive directional electromagnetic signals, IR, UV, laser, visible light signals, or the like. For example, the directional electromagnetic energy may be any highly focused beam of radiation, such as a laser, that may provide an extremely narrow beam on which information may be modulated. The directional electromagnetic energy may provide a partially coherent, narrow low-divergence beam that may prevent eavesdroppers. Additionally, the directional electromagnetic energy may be polarized to allow direct line of sight transmission and to reduce the probability that an eavesdropper may receive signals from reflections. In yet another embodiment, the transmit/receive element 122 may be configured to transmit and receive both RF and directional electromagnetic signals. For example, the directional electromagnetic signals may be any highly focused beam of radiation, such as a laser, that may provide an extremely narrow beam on which information may be modulated. The directional electromagnetic signals may provide a partially

coherent, narrow low-divergence beam that may prevent eavesdroppers. Additionally, the directional electromagnetic signals may be polarized to allow direct line of sight transmission and to reduce the probability that an eavesdropper may receive signals from reflections. It will be appreciated that the transmit/receive element 122 may be configured to transmit and/or receive any combination of wireless signals.

[0046] In addition, although the transmit/receive element 122 is depicted in Figure 1B as a single element, the WTRU 102 may include any number of transmit/receive elements 122. For example, the WTRU 102 may employ MIMO technology. Thus, in one embodiment, the WTRU 102 may include two or more transmit/receive elements 122 (e.g., multiple antennas) for transmitting and receiving wireless signals over the air interface 116. In another embodiment, the WTRU 102 may include at least two transmit/receive elements 122; a first transmit/receive element 122 to be used for RF communications and a second transmit/receive element 122 to be used for directional electromagnetic signal communications.

[0047] The transceiver 120 may be configured to modulate the signals that are to be transmitted by the transmit/receive element 122 and to demodulate the signals that are received by the transmit/receive element 122. As noted above, the WTRU 102 may have multi-mode capabilities. Thus, the transceiver 120 may include multiple transceivers for enabling the WTRU 102 to communicate via multiple RATs, such as UTRA and IEEE 802.11, for example.

[0048] The processor 118 of the WTRU 102 may be coupled to, and may receive user input data from, the speaker/microphone 124, the keypad 126, and/or the display/touchpad 128 (e.g., a liquid crystal display (LCD) display unit or organic light-emitting diode (OLED) display unit). The processor 118 may also output user data to the speaker/microphone 124, the keypad 126, and/or the display/touchpad 128. In addition, the processor 118 may access information from, and store data in, any type of suitable memory, such as the non-removable memory 106 and/or the removable memory 132. The non-removable memory 106 may include random-access memory (RAM), read-only memory (ROM), a hard disk, or any other type of memory storage device. The removable memory 132 may include a subscriber identity module (SIM) card, a memory stick, a secure digital (SD) memory card, and the like. In other embodiments, the processor 118 may access information from, and store data in, memory that is not physically located on the WTRU 102, such as on a server or a home computer (not shown).

[0049] The processor 118 may receive power from the power source 134, and may be configured to distribute and/or control the power to the other components in the WTRU 102. The power source 134 may be any suitable device for powering the WTRU 102. For example,

the power source 134 may include one or more dry cell batteries (e.g., nickel-cadmium (NiCd), nickel-zinc (NiZn), nickel metal hydride (NiMH), lithium-ion (Li-ion), etc.), solar cells, fuel cells, and the like.

[0050] The processor 118 may also be coupled to the GPS chipset 136, which may be configured to provide location information (e.g., longitude and latitude) regarding the current location of the WTRU 102. In addition to, or in lieu of, the information from the GPS chipset 136, the WTRU 102 may receive location information over the air interface 116 from a base station (e.g., base stations 114a, 114b) and/or determine its location based on the timing of the signals being received from two or more nearby base stations. It will be appreciated that the WTRU 102 may acquire location information by way of any suitable location-determination method while remaining consistent with an embodiment.

[0051] The processor 118 may further be coupled to other peripherals 138, which may include one or more software and/or hardware modules that provide additional features, functionality and/or wired or wireless connectivity. For example, the peripherals 138 may include an accelerometer, an e-compass, a satellite transceiver, a digital camera (for photographs or video), a universal serial bus (USB) port, a vibration device, a television transceiver, a hands free headset, a Bluetooth® module, a frequency modulated (FM) radio unit, a digital music player, a media player, a video game player module, an Internet browser, and the like.

[0052] Figure 1C is a system diagram of the RAN 104 and the core network 106 according to an embodiment. As noted above, the RAN 104 may employ an E-UTRA radio technology to communicate with the WTRUs 102a, 102b, 102c over the air interface 116. The RAN 104 may also be in communication with the core network 106.

[0053] The RAN 104 may include eNode-Bs 140a, 140b, 140c, though it will be appreciated that the RAN 104 may include any number of eNode-Bs while remaining consistent with an embodiment. The eNode-Bs 140a, 140b, 140c may each include one or more transceivers for communicating with the WTRUs 102a, 102b, 102c over the air interface 116. In one embodiment, the eNode-Bs 140a, 140b, 140c may implement MIMO technology. Thus, the eNode-B 140a, for example, may use multiple antennas to transmit wireless signals to, and receive wireless signals from, the WTRU 102a.

[0054] Each of the eNode-Bs 140a, 140b, 140c may be associated with a particular cell (not shown) and may be configured to handle radio resource management decisions, handover decisions, scheduling of users in the uplink and/or downlink, and the like. As shown in Figure 1C, the eNode-Bs 140a, 140b, 140c may communicate with one another over an X2 interface.

[0055] The core network 106 shown in Figure 1C may include a mobility management gateway (MME) 142, a serving gateway 144, and a packet data network (PDN) gateway 146. While each of the foregoing elements are depicted as part of the core network 106, it will be appreciated that any one of these elements may be owned and/or operated by an entity other than the core network operator.

[0056] The MME 142 may be connected to each of the eNode-Bs 142a, 142b, 142c in the RAN 104 via an S1 interface and may serve as a control node. For example, the MME 142 may be responsible for authenticating users of the WTRUs 102a, 102b, 102c, bearer activation/deactivation, selecting a particular serving gateway during an initial attach of the WTRUs 102a, 102b, 102c, and the like. The MME 142 may also provide a control plane function for switching between the RAN 104 and other RANs (not shown) that employ other radio technologies, such as GSM or WCDMA.

[0057] The serving gateway 144 may be connected to each of the eNode Bs 140a, 140b, 140c in the RAN 104 via the S1 interface. The serving gateway 144 may generally route and forward user data packets to/from the WTRUs 102a, 102b, 102c. The serving gateway 144 may also perform other functions, such as anchoring user planes during inter-eNode B handovers, triggering paging when downlink data is available for the WTRUs 102a, 102b, 102c, managing and storing contexts of the WTRUs 102a, 102b, 102c, and the like.

[0058] The serving gateway 144 may also be connected to the PDN gateway 146, which may provide the WTRUs 102a, 102b, 102c with access to packet-switched networks, such as the Internet 110, to facilitate communications between the WTRUs 102a, 102b, 102c and IP-enabled devices.

[0059] The core network 106 may facilitate communications with other networks. For example, the core network 106 may provide the WTRUs 102a, 102b, 102c with access to circuit-switched networks, such as the PSTN 108, to facilitate communications between the WTRUs 102a, 102b, 102c and traditional land-line communications devices. For example, the core network 106 may include, or may communicate with, an IP gateway (e.g., an IP multimedia subsystem (IMS) server) that serves as an interface between the core network 106 and the PSTN 108. In addition, the core network 106 may provide the WTRUs 102a, 102b, 102c with access to the networks 112, which may include other wired or wireless networks that are owned and/or operated by other service providers.

[0060] Figure 2 illustrates an example embodiment of a system for using directional electromagnetic signals for authentication and key establishment. In an example embodiment,

the system may include initiator WTRU 205, directional electromagnetic communication link 210, radio frequency (RF) communication link 215, and/or target WTRU 250. Initiator WTRU 205 may be WTRU 102. Additionally, initiator WTRU 205 may be any device that may transmit and/or receive directional electromagnetic signals, such as the smart phone 252, the PDA 255, the cell phone 260, the laptop 265, the directional electromagnetic signal transmitter/receiver equipped credit card 270, or the like. For example, initiator WTRU 205 may be a device that contains a laser transmitter/receiver. Target WTRU 250 may be WTRU 102. Additionally, target WTRU 250 may be any device that may transmit and/or receive directional electromagnetic signals, such as the smart phone 220, the PDA 225, the cell phone 230, the laptop 235, the directional electromagnetic signal transmitter/receiver equipped credit card 245, or the like. For example, target WTRU 250 may be a device that contains a laser transmitter/receiver. Directional electromagnetic link 210 and/or RF communication link 215 may operatively connect initiator WTRU 205 and target WTRU 250. RF communication link 215 may be a radio frequency communication link, a Wi-Fi communication link, a Long Term Evolution (LTE) communication link, a High Speed Packet Access (HSPA) communication link, the internet, or the like.

[0061] In another example embodiment, initiator WTRU 205 may use directional electromagnetic link 210 to establish a private data link on directional electromagnetic link 210. To establish a private data link, initiator WTRU 205 may transmit an initiation message to the target WTRU. Upon receiving the initiation message, target WTRU 250 may determine whether it is able to establish secured communications and if it is able to establish secured communications, target WTRU 250 may transmit a ready to authenticate message to initiator WTRU 205. Initiator WTRU 205 may then transmit an authentication ID to target WTRU 250. Target WTRU 250 may then authenticate the ID and when the ID has been authenticated, target WTRU 250 may respond with an authentication ID assigned message. Initiator WTRU 205 may then transmit the key. When the key is received by target WTRU 250, the key may then be used to create a private data link on directional electromagnetic link 210.

[0062] In another example embodiment, initiator WTRU 205 may use directional electromagnetic link 210 to establish a private data link on RF communication link 215. To establish a private data link, initiator WTRU 205 may transmit an initiation message to the target WTRU using RF communication link 215. Upon receiving the initiation message, target WTRU 250 may determine whether it is able to establish secured communications and if it is able to establish secured communications, target WTRU 250 may transmit a ready to authenticate message to initiator WTRU 205 using RF communication link 215. Initiator WTRU 205 may

then transmit an authentication ID to target WTRU 250 using RF communication link 215. Target WTRU 250 may then authenticate the ID and when the ID has been authenticated, target WTRU 250 may respond with an authentication ID assigned message using RF communication link 215. Initiator WTRU 205 may then transmit the key using directional electromagnetic link 210. When the key is received by target WTRU 250, the key may then be used to create a private data link on RF communication link 215. In another example embodiment, all messaging may take place on laser link 210 and when the key has been established, the private data link may be created on RF communication link 215.

[0063] Figure 3 illustrates another example embodiment of a system for using directional electromagnetic signals for authentication and key establishment. In an example embodiment, the system may include initiator WTRU 205, directional electromagnetic link 310, RF communication link 315, and/or the communications node 300. Communications node 300 may be the router 320, the RF tower 325, or the directional electromagnetic signal transmitter/receiver equipped credit card reader 330. Directional electromagnetic link 310 and/or RF communication link 315 may operatively connect initiator WTRU 205 and communications node 300. RF communication link 315 may be a RF communication link, a Wi-Fi communication link, a LTE communication link, a HSPA communication link, the internet, or the like.

[0064] Initiator WTRU 205 may use directional electromagnetic link 310 to establish a private data link on directional electromagnetic link 310. To establish the private data link, initiator WTRU 205 may transmit an initiation message to the communications node 300. Upon receiving the initiation message, communications node 300 may determine whether it is able to establish secured communications and if it is able to establish secured communications, communications node 300 may transmit a ready to authenticate message to initiator WTRU 205. Initiator WTRU 205 may then transmit an authentication ID to communications node 300. Communications node 300 may then authenticate the ID and when the ID has been authenticated, target WTRU 250 may respond with an authentication ID assigned message. Initiator WTRU 205 may then transmit the key. When the key is received by communications node 300, the key may then be used to create a private data link on directional electromagnetic link 310.

[0065] In another example embodiment, initiator WTRU 205 may use directional electromagnetic link 310 to establish a private data link on RF communication link 315. To establish a private data link, initiator WTRU 205 may transmit an initiation message to target WTRU 250 using RF communication link 315. Upon receiving the initiation message, target WTRU 250 may determine whether it is able to establish secured communications and if it is

able to establish secured communications, communications node 300 may transmit a ready to authenticate message to initiator WTRU 205 using RF communication link 315. Initiator WTRU 205 may then transmit an authentication ID to communications node 300 using RF communication link 315. Communications node 300 may then authenticate the ID and when the ID has been authenticated, the communications node 300 may respond with an authentication ID assigned message using RF communication link 315. Initiator WTRU 205 may then transmit the key using directional electromagnetic link 310. When the key is received by communications node 300, the key may then be used to create a private data link on RF communication link 315. In another example embodiment, all messaging may take place on laser link 310 and when the key has been established, the private data link is created on RF communication link 315.

[0066] In another example embodiment, communications node 300 may use directional electromagnetic link 310 to establish a private data link on directional electromagnetic link 310. To establish the private data link, communications node 300 may transmit an initiation message to the initiator WTRU 205. Upon receiving the initiation message, initiator WTRU 205 may determine whether it is able to establish secured communications and if it is able to establish secured communications, initiator WTRU 205 may transmit a ready to authenticate message to communications node 300. Initiator WTRU 205 may then transmit an authentication ID to initiator WTRU 205. Initiator WTRU 205 may then authenticate the ID and when the ID has been authenticated, initiator WTRU 205 may respond with an authentication ID assigned message. Communications node 300 may then transmit the key. When the key is received by initiator WTRU 205, the key may then be used to create a private data link on directional electromagnetic link 310.

[0067] In another example embodiment, communications node 300 may use directional electromagnetic link 310 to establish a private data link on RF communication link 315. To establish a private data link, communications node 300 may transmit an initiation message to initiator WTRU 205 using RF communication link 315. Upon receiving the initiation message, initiator WTRU 205 may determine whether it is able to establish secured communications and if it is able to establish secured communications, initiator WTRU 205 may transmit a ready to authenticate message to communications node 300 using RF communication link 315. Communications node 300 may then transmit an authentication ID to initiator WTRU 205 using RF communication link 315. Initiator WTRU 205 may then authenticate the ID and when the ID has been authenticated, initiator WTRU 205 may respond with an authentication ID assigned message using RF communication link 315. Communications node 300 may then transmit the key using directional electromagnetic link 310. When the key is received by initiator WTRU

205, the key may then be used to create a private data link on RF communication link 315. In another example embodiment, all messaging may take place on directional electromagnetic 310 and when the key has been established, the private data link may be created on RF communication link 315.

[0068] In one example embodiment, initiator WTRU 250 may be configured for using directional electromagnetic signals to create a secured private data link associated with a secret key between the WTRU and a communications node. For example, the WTRU 250 may be transmit an initiation message. The initiation message may indicate that the initiator WTRU 250 wishes to establish the secured private data link associated with the secret key between the initiator WTRU 250 and the communications node 300. The initiator WTRU 250 may also be configured to receive a response message. The response message may notify the initiator WTRU 250 to establish the secured private data link. The initiator WTRU 250 may establish the secured private data link using directional electromagnetic signals and may receive an acknowledgement message. The acknowledgement message may indicate that the secured private data link has been established.

[0069] Figure 4 illustrates an example embodiment of a method 400 for using directional electromagnetic signals to create a secured private data link associated with a secret key between a first wireless transmit/receive unit (WTRU) and a second WTRU. The method 400 may also be used to create a secured private data link associated with a secret key between the first WTRU and a communications node, such as the communications node shown with respect to Figure 3. The method 400 may enable a user associated with the first WTRU to establish a secured private data link with a second WTRU. Additionally, the method 400 may allow for authentication and key establish to occur with a positive visual confirmation of authentication. For example, the directional electromagnetic signals used may be a visible laser that may enable a user to visually confirm that the directional electromagnetic signals have reached an intended recipient.

[0070] To reduce the possibility that the directional electromagnetic signals may be intercepted by a man-in-the-middle attack, the first WTRU may enforce tight latency requirements for responses received from the second WTRU such that an attack is afforded very little time, and may even be barred by the propagation delay, to perform a successful attack. For example, when a first reflection is received by the first WTRU, a range measurement may be made that may provide an estimate of the round-trip propagation delay. This measurement of the propagation delay may be used to set thresholds beyond which authentication and key establishment will be terminated due to a perceived attack.

[0071] In one example embodiment, messages transmitted from the first WTRU and/or the second WTRU may occur via the directional electromagnetic signals and may include sufficient random key for a response to be encrypted. Responses from the second WTRU may be over a public channel and may be protected by a secret key.

[0072] In another example embodiment, the method 400 may be carried out using at least two completely different means of communication. For example, messages between the first WTRU and the second WTRU may be transmitted and/or received interchangeably between an open channel protected by a secret key, such as an RF channel, and a directional channel, such as a channel carried over directional electromagnetic signals.

[0073] Referring now to Figure 4, a user associated with the first WTRU may wish to establish secured communications between the first WTRU and the second WTRU. To establish secured communications, at 410, the first WTRU may transmit an initiation message. The initiation message may indicate that the first WTRU wishes to establish a secured private data link associated with a secret key between the first WTRU and the second WTRU. The initiation message may also include a first token that may be combined with a second token provided by the second WTRU to generate the secret key.

[0074] In one example embodiment, the initiation message may include seeding data that may enable the second WTRU to derive an initiation key. The second WTRU may then use the initiation key to encrypt a response message that is transmitted by the second WTRU and received by the first WTRU. In another example embodiment, the initiation message may include the initiation key.

[0075] At 420, the first WTRU may receive a response message from the second WTRU. The response message may notify the first WTRU to establish the secured private data link. For example, the response message may inform the first WTRU that the second WTRU is capable of transmitting and/or receiving directional electromagnetic signals and establishing the secured private data link with the first WTRU.

[0076] In one example embodiment, the response message may include a second token. When the response message is received by the first WTRU, the first WTRU may retrieve a first token stored on the first WTRU. The first WTRU may then generate a secret key from the first token and the second token. The secret key may then be used to establish a private data link between the first WTRU and the second WTRU. For example, the first WTRU may use the secret key to encrypt a message and transmit the encrypted message to the second WTRU.

[0077] In another example embodiment, the response message may be encrypted with an initiation key. As describe above, the initiation key may be included within the initiation message, or may be derived from the initiation message.

[0078] At 430, the first WTRU may determine a propagation delay between the time the initiation message was transmitted and the time the response message was received. For example, the first WTRU may receive a reflection of directional electromagnetic signals and may calculate a range measurement. The range measurement may provide the first WTRU with an estimate of the round-trip propagation delay. This measurement of propagation delay may then be used by the first WTRU to set thresholds beyond which method 400 will terminate due to a perceived man-in-the-middle attack.

[0079] At 440, the first WTRU may adjust or modulate the intensity of the directional electromagnetic signals. This may be done, for example, to reduce the probability that an eavesdropper may reliably decode key data transmitted by the first WTRU and/or the second WTRU.

[0080] In one example embodiment, the first WTRU may adjust the intensity of the directional electromagnetic signals to keep the signal-to-noise ratio at the second WTRU at or above a detectable level. For example, the signal-to-noise ratio (SNR) at the second WTRU may be kept just above the detectability level to ensure that other receivers would not have sufficient SNR for reliable detection. The first WTRU may then transmit key information at the adjust intensity of the directional electromagnetic signals in order to establish the secured private data link.

[0081] In another example embodiment, the first WTRU may modulate the intensity of the directional signals to control the power allocated to the transmission of key information while ensuring that the directional electromagnetic signals are visible. For example, the intensity of the directional electromagnetic signals may be fixed and high to provide clear visibility.

[0082] In another example embodiment, the first WTRU may increase a modulation factor of the directional electromagnetic signals while transmitting pseudo random coded packets. This may be done, for example, to retain the visibility of the carrier while controlling the power allocated to the information transmission. When a response message has been received, the first WTRU may fix or set the modulation factor. The first WTRU may then transmit key information to the second WTRU at the fixed modulation factor.

[0083] In another example embodiment, the first WTRU may set the average intensity of the directional magnetic signals to a level that provides visibility. The first WTRU may then modulate the power of data slots the directional electromagnetic signals carries to keep the signal-to-noise ratio at the second WTRU at or above a detectable level. For example, the

modulation factor A may be set to α in a set of slots and $(1-\alpha)$ in a different set of slots. The value of α may be initially a small number, or may be zero. Within each slot, α may be gradually increased; increasing the detectability while transmitting pseudo random coded packets and waiting for the expected response from the second WTRU. The first WTRU may then transmit key information to the second WTRU using the modulated data slots in order to establish the secured private data link.

[0084] At 450, the first WTRU may establish the secured private data link using directional electromagnetic signals. In one example embodiment, the first WTRU may establish the private data link by using directional electromagnetic signals to transmit key information to the second WTRU. The first WTRU may transmit key information when the propagation delay is below a security threshold determined at 430. In one example embodiment, the key information includes the secret key. In another example embodiment, the key information may include a message that is encrypted with the secret key.

[0085] In another example embodiment, the key information includes seeding data that may enable the second WTRU to generate the secret key. For example, a conventional authentication and key agreement protocol may take place over a RF communications link while additional seeding material may be exchanged over the private data link.

[0086] In another example embodiment, the key information may include payment information that is encrypted with the secret key. The payment information may provide payment for a purchase. For example, a user associated with the first WTRU may submit a payment to a user that may be associated with the second WTRU. Upon receiving the payment information, the second WTRU may decrypt the payment information using the secret key and then may then complete the transaction by using the payment information to receive the appropriate funds.

[0087] At 460, the first WTRU may send a message requesting the second WTRU transmit a coded light pattern or sound upon receipt of the message. For example, the first WTRU may request the second WTRU transmit an acknowledgement message via directional electromagnetic signals according to a set pattern.

[0088] At 470, the first WTRU may receive an acknowledgement message. The first WTRU may receive optical and/or audible feedback of key establishment from the second WTRU. For example, the second WTRU may notify the first WTRU and/or the user associated with the first WTRU that the key information was successfully transferred via the illumination of an indicator light as light from an incandescent, fluorescent, LED, or the like, and/or an audio signal. The acknowledgement message may be a coded light pattern.

[0089] Figure 5 illustrates an example embodiment of a method 500 for using directional electromagnetic signals to create a secured private data link associated with a secret key between a first wireless transmit/receive unit (WTRU) and a second WTRU. The method 500 may also be used to create a secured private data link associated with a secret key between the first WTRU and a communications node, such as the communications node shown with respect to Figure 3. The method 500 may enable a user associated with the second WTRU to establish a secured private data link with a first WTRU. Additionally, the method 500 may allow for authentication and key establish to occur with a positive visual confirmation of authentication. For example, the directional electromagnetic signals used may be a visible laser that may enable a user to visually confirm that the directional electromagnetic signals have reached an intended recipient.

[0090] To reduce the possibility that the directional electromagnetic signals may be intercepted by a man-in-the-middle attack, the second WTRU may enforce tight latency requirements for responses received from the first WTRU such that an attack is afforded very little time, and may even be barred by the propagation delay, to perform a successful attack. For example, when a first reflection is received by the second WTRU, a range measurement may be made that may provide an estimate of the round-trip propagation delay. This measurement of the propagation delay may be used to set thresholds beyond which authentication and key establishment will be terminated due to a perceived attack.

[0091] In one example embodiment, messages transmitted from the second WTRU and/or the first WTRU may occur via the directional electromagnetic signals and may include sufficient random key for a response to be encrypted. Responses from the first WTRU may be over a public channel and may be protected by a secret key.

[0092] In another example embodiment, the method 500 may be carried out using at least two completely different means of communication. For example, messages between the second WTRU and the first WTRU may be transmitted and/or received interchangeably between an open channel protected by a secret key, such as an RF channel, and a directional channel, such as a channel carried over directional electromagnetic signals.

[0093] Referring now to Figure 5, a user associated with the second WTRU may wish to establish secured communications between the second WTRU and the first WTRU. To establish secured communications, at 510, the first WTRU may receive initiation message. The initiation message may indicate that the second WTRU wishes to establish a secured private data link associated with a secret key between the second WTRU and the first WTRU. The initiation message may also include a first token that may be combined with a second token provided by the first WTRU to generate the secret key.

[0094] In one example embodiment, the initiation message may include seeding data that may enable the first WTRU to derive a initiation key. The first WTRU may then use the initiation key to encrypt a response message that may be transmitted by the first WTRU and received by the second WTRU. In another example embodiment, the initiation message may include the initiation key.

[0095] At 520, the first WTRU may transmit a response message to the second WTRU. The response message may notify the second WTRU to establish the secured private data link. For example, the response message may inform the second WTRU that the first WTRU is capable of transmitting and/or receiving directional electromagnetic signals and establishing the secured private data link with the second WTRU.

[0096] In one example embodiment, the response message may include a second token. When the response message is received by the second WTRU, the second WTRU may retrieve a first token stored on the second WTRU. The second WTRU may then generate a secret key from the first token and the second token. The secret key may then be used to establish a private data link between the second WTRU and the first WTRU. For example, the second WTRU may use the secret key to encrypt a message and transmit the encrypted message to the first WTRU.

[0097] In another example embodiment, the response message may be encrypted with an initiation key. As describe above, the initiation key may be included within the initiation message, or may be derived from the initiation message.

[0098] At 530, the first WTRU may determine a propagation delay between the time the response message was transmitted and the time the response message was acknowledged by the second WTRU. For example, the first WTRU may receive a reflection of directional electromagnetic signals and may calculate a range measurement. The range measurement may provide the first WTRU with an estimate of the round-trip propagation delay. This measurement of propagation delay may then be used by the first WTRU to set thresholds beyond which method 500 will determinate due to a perceived man-in-the-middle attack.

[0099] At 540, the first WTRU may receive adjusted or modulated directional signals.

[0100] In one example embodiment, the second WTRU may adjust the intensity of the directional electromagnetic signals to keep the signal-to-noise ratio at the first WTRU at or above a detectable level. When the first WTRU receives an adjusted or modulated directional signal at or above a detectable level, the first WTRU may transmit a response message. For example, the first WTRU may transmit a response message when an initiation message is received at or above a detectable level. The first WTRU may then receive key information at the

adjust intensity of the directional electromagnetic signals in order to establish the secured private data link.

[0101] In another example embodiment, the second WTRU may increase a modulation factor of the directional electromagnetic signals while transmitting pseudo random coded packets. This may be done, for example, to retain the visibility of the carrier while controlling the power allocated to the information transmission. The first WTRU may receive pseudo random coded packets from the directional electromagnetic signals at an increasing a modulation factor. The first WTRU may determine the received modulation factor of the received pseudo random coded packets. When the modulation factor exceeds a security threshold, the first WTRU may transmit a response message to the second WTRU to fix or set the modulation factor. The second WTRU may then transmit key information to the first WTRU at the fixed modulation factor.

[0102] In another example embodiment, the second WTRU may set the average intensity of the directional magnetic signals to a level that provides visibility. The second WTRU may then modulate the power of the data slots that the directional electromagnetic signals carries to keep the signal-to-noise ratio at the first WTRU at or above a detectable level. For example, the modulation factor A may be set to α in a set of slots and $(1-\alpha)$ in a different set of slots. The value of α may be initially a small number, or may be zero. Within each slot, α may be gradually increased; increasing the detectability while transmitting pseudo random coded packets and waiting for the expected response from the first WTRU. The first WTRU may receive data the data slots carried by the directional electromagnetic signals. The first WTRU may determine the power of the data slots. The first WTRU may then derive the key information from the data slots when the power of the data slots achieves a signal-to-noise ration above a power threshold.

[0103] At 550, the first WTRU may establish the secured private data link using directional electromagnetic signals. In one example embodiment, the first WTRU may establish the private data link by using directional electromagnetic signals to receive key information from the second WTRU. In one example embodiment, the key information may include the secret key. In another example embodiment, the key information may include a message that is encrypted with the secret key.

[0104] In another example embodiment, the key information may include seeding data to enable the first WTRU to generate the secret key. For example, a conventional authentication and key agreement protocol may take place over a RF communications link while additional seeding material may be exchanged over the private data link.

[0105] In another example embodiment, the key information may include payment information that is encrypted with the secret key. The payment information may provide payment for a purchase. For example, a user associated with the second WTRU may submit a payment to a user that may be associated with the first WTRU. Upon receiving the payment information, the first WTRU may decrypt the payment information using the secret key and then may then complete the transaction by using the payment information to receive the appropriate funds.

[0106] At 560, the first WTRU may receive a message to transmit a coded light pattern or sound upon receipt of the message. For example, the second WTRU may request that the first WTRU transmit an acknowledgement message via directional electromagnetic signals according to a set pattern.

[0107] At 570, the first WTRU may transmit an acknowledgement message. The first WTRU may transmit optical and/or audible feedback of key establishment to the second WTRU. For example, the first WTRU may notify the second WTRU and/or the user associated with the second WTRU that the key information was successfully transferred via the illumination of an indicator light as light from an incandescent, fluorescent, LED, or the like, and/or an audio signal. The acknowledgement message may be a coded light pattern.

[0108] Figure 6 illustrates an example embodiment of a method for laser authentication and key establishment. The method may enable a user associated with initiator WTRU 205 to establish a secured private data link with target WTRU 250. Additionally, the method may allow for authentication and key establishment with a positive visual confirmation of authentication.

[0109] To reduce the possibility that laser authentication and key establishment may be susceptible to a man-in-the-middle attack, initiator WTRU 205 may enforce tight latency requirements for the response of target WTRU 250 such that an attacker is afforded very little time, and may even be barred by the propagation delay, to perform a successful attack. For example, when a first reflection is received by initiator WTRU 205, a range measurement may be made that may provide an estimate of the round-trip propagation delay. This measurement of propagation delay may be used to set thresholds beyond which laser authentication and key establishment will terminate due to a perceived attack.

[0110] In one example embodiment, messages transmitted from initiator WTRU 205 and/or target WTRU 250 may occur over a secure laser link and may include sufficient random key for a response to be encrypted. Responses from target WTRU 250 may be over a public channel and may be protected by a key provided by initiator WTRU 205.

[0111] In another example embodiment, the method may be carried out by using at least two completely different means of communication. For example, messages between initiator WTRU

205 and target WTRU 250 may be transmitted and/or received interchangeably between an open channel protected by a key provided by initiator WTRU 205 and a secure laser link.

[0112] Referring now to Figure 6, a user associated with initiator WTRU 205 may wish to establish secured communications between initiator WTRU 205 and target WTRU 250. To establish secured communications, at 620, initiator WTRU 205 may transmit an initiate laser authentication and key establishment process message to the target WTRU. Upon receiving the initiate message, target WTRU 250 may determine whether it is able to establish secured communications and if it is able to establish secured communications, target WTRU 250 may transmit a ready to authenticate message to initiator WTRU 205 at 630. At 640, initiator WTRU 205 may then transmit an authentication ID to target WTRU 250. Target WTRU 250 may then authenticate the ID and when the ID has been authenticated, target WTRU 250 may respond with an authentication ID assigned message at 650.

[0113] At 660, initiator WTRU 205 may then transmit the key. In one example embodiment, when the key is received by target WTRU 250, the key may be used to create symmetrical key encryption that may provide a secured data link between initiator WTRU 205 and target WTRU 250.

[0114] In another example embodiment, the key may be established between initiator WTRU 205 and target WTRU 250 using existing means such as Diffie-Helman key exchange. Moreover, existing means may be used to seed the key establishment procedure through additional keying material or data transferred over the laser link with the additional security of visual confirmation. This may enable positive authentication of the established keys by way of visual authentication by way of exchanging tokens or data through the RF and laser communications paths. This may be done, for example, to provide an additional layer of physical protection if the Diffie-Helman key exchange were compromised.

[0115] At 670, target WTRU 250 notifies initiator WTRU 205 that the key has been established.

[0116] In one example embodiment, target WTRU 250 may utilize optical and/or audible feedback of key establishment. For example, target WTRU 250 may notify initiator WTRU 205 and/or the user associated with initiator WTRU 205 that the key was successfully transferred via the illumination of an indicator light as light from an incandescent, fluorescent, LED, or the like, and/or an audio signal.

[0117] In another example embodiment, optical and/or audio feedback may provide an additional level of positive authentication that may identify a UE with a particular user. The messaging between initiator WTRU 205 and target WTRU 250 may occur over both a public

channel and a laser channel. As an example, a conventional authentication and key agreement protocol could take place over a radio link while additional seeding material may be exchanged over the laser link. Providing optical and/or audio feedback may enable the user associated with initiator WTRU 205 and the user associated with target WTRU 250 to identify and authenticate each other.

[0118] Figure 7 illustrates an example embodiment of a method for transmitting a message during laser authentication and key establishment. The method may enable a user associated with initiator WTRU 205 to transmit a secured message to target WTRU 250. Additionally, the method may allow for authentication and key establishment with a positive visual confirmation of authentication.

[0119] To reduce the possibility that laser authentication and key establishment may be susceptible to a man-in-the-middle attack, initiator WTRU 205 may enforce tight latency requirements for the response of target WTRU 250 such that an attacker is afforded very little time, and may even be barred by the propagation delay, to perform a successful attack. For example, when a first reflection is received by the initiator WTRU 205, a range measurement may be made that may provide an estimate of the round-trip propagation delay. This measurement of propagation delay may be used to set thresholds beyond which laser authentication and key establishment will terminate due to a perceived attack.

[0120] In one example embodiment, messages transmitted from initiator WTRU 205 and/or target WTRU 250 may occur over a secure laser link and may include sufficient random key for a response to be encrypted. Responses from target WTRU 250 may be over a public channel and maybe protected by a key provided by initiator WTRU 205.

[0121] In another example embodiment, the method may be carried out by using at least two completely different means of communication. For example, messages between initiator WTRU 205 and target WTRU 250 may be transmitted and/or received interchangeably between an open channel protected by a key provided by initiator WTRU 205 and a secure laser link.

[0122] Referring now to Figure 7, a user associated with initiator WTRU 205 may wish to transmit a secured message to the target WTRU 250. To transmit the secured message, at 720, initiator WTRU 205 may transmit an initiate laser authentication and key establishment process message to the target WTRU. Upon receiving the initiate message, target WTRU 250 may determine whether it is able to establish secured communications and if it is able to establish secured communications, target WTRU 250 may transmit a ready to authenticate message to initiator WTRU 205 at 730. At 740, initiator WTRU 205 may then transmit an authentication ID to target WTRU 250. Target WTRU 250 may then authenticate the ID and when the ID has been

authenticated, target WTRU 250 may respond with an authentication ID assigned message at 750.

[0123] At 760, initiator WTRU 205 may then transmit the key. Additionally, a message may accompany, or “piggyback” the key. For example, when target WTRU 250 responds with an authentication ID assigned message at 750, initiator WTRU 205 may respond by transmitting the key and a message at 760. The message may be encrypted according to the key. When target WTRU 250 receives the key and the message, target WTRU 250 may decrypt the key and/or use the key to establish a secured data link between initiator WTRU 205 and target WTRU 250. At 770, target WTRU 250 may transmit a message to initiator WTRU 205 to acknowledge the piggybacked message and/or the key establishment.

[0124] In one example embodiment, target WTRU 250 may utilize optical and/or audible feedback of key establishment. For example, target WTRU 250 may notify initiator WTRU 205 and/or the user associated with initiator WTRU 205 that the key was successfully transferred via the illumination of an indicator light as light from an incandescent, fluorescent, LED, or the like, and/or an audio signal.

[0125] In another example embodiment, optical and/or audio feedback may provide an additional level of positive authentication that may identify a UE with a particular user. The messaging between initiator WTRU 205 and target WTRU 250 may occur over both a public channel and a laser channel. As an example, a conventional authentication and key agreement protocol could take place over a radio link while additional seeding material may be exchanged over the laser link. Providing optical and/or audio feedback may enable the user associated with initiator WTRU 205 and the user associated with target WTRU 250 to identify and authenticate each other.

[0126] Figure 8 illustrates an example embodiment of a method payment transaction using laser authentication and/or key establishment. In one example embodiment, the method may enable a user associated with initiator WTRU 205 to submit a payment to a user that may be associated with target WTRU 250. For example, the user associated with initiator WTRU 205 may transmit payment information to target WTRU 250. Target WTRU 250 may then complete the transaction by using the payment information to receive the appropriate funds. In another example embodiment, communications node 300 may be used instead of target WTRU 250. In another example embodiment, the method may enable a user associated with initiator WTRU 205 to provide payment for a purchase to a vendor that may be associated with infrastructure, such as communications node 300 shown with respect to Figure 3. For example, initiator WTRU 205 may be a laser transmitter/receiver equipped credit card that a user may use to purchase an

item at a store. In purchasing the item, the user may use the credit card to transmit payment information to a laser transmitter/receiver equipped credit card reader via laser.

[0127] To reduce the possibility that laser authentication and key establishment may be susceptible to a man-in-the-middle attack, initiator WTRU 205 may enforce tight latency requirements for the response of target WTRU 250 such that an attacker is afforded very little time, and may even be barred by the propagation delay, to perform a successful attack. For example, when a first reflection is received by the initiator WTRU 205, a range measurement may be made that may provide an estimate of the round-trip propagation delay. This measurement of propagation delay may be used to set thresholds beyond which laser authentication and key establishment will terminate due to a perceived attack.

[0128] In one example embodiment, messages transmitted from initiator WTRU 205 and/or target WTRU 250 may occur over a secure laser link and may include sufficient random key for a response to be encrypted. Responses from target WTRU 250 may be over a public channel and maybe protected by a key provided by initiator WTRU 205.

[0129] In another example embodiment, the method may be carried out by using at least two completely different means of communication. For example, messages between initiator WTRU 205 and target WTRU 250 may be transmitted and/or received interchangeably between an open channel protected by a key provided by initiator WTRU 205 and a secure laser link.

[0130] Referring now to Figure 8, a user associated with initiator WTRU 205 may wish to transmit payment information to target WTRU 250. To transmit payment information, at 820, initiator WTRU 205 may first transmit an initiate laser authentication and key establishment process message to the target WTRU. Upon receiving the initiate message, target WTRU 250 may determine whether it is able to establish secured communications and if it is able to establish secured communications, target WTRU 250 may transmit a ready to authenticate message to initiator WTRU 205 at 830. At 840, initiator WTRU 205 may then transmit an authentication ID to target WTRU 250. Target WTRU 250 may then authenticate the ID and when the ID has been authenticated, target WTRU 250 may respond with an authentication ID assigned message at 850.

[0131] At 860, initiator WTRU 205 may then transmit a key. Additionally, payment information may accompany the key. For example, when target WTRU 250 responds with an authentication ID assigned message at 850, initiator WTRU 205 may respond by transmitting the key and payment information at 860. The payment information may be encrypted according to the key. When target WTRU 250 receives the key and the message, target WTRU 250 may decrypt the key and/or use the key to establish a secured data link between initiator WTRU 205

and target WTRU 250. In one example embodiment, the key may be transmitted and a secured data link may be established before the payment information is transmitted.

[0132] At 870, target WTRU 250 may transmit a message to initiator WTRU 205 to acknowledge the payment information has been received, that the payment has been made and/or the key established. In one example embodiment, target WTRU 250 may utilize optical and/or audible feedback of key establishment. For example, target WTRU 250 may notify initiator WTRU 205 and/or the user associated with initiator WTRU 205 that the key was successfully transferred via the illumination of an indicator light as light from an incandescent, fluorescent, LED, or the like, and/or an audio signal

[0133] In another example embodiment, optical and/or audio feedback may provide an additional level of positive authentication that may identify a UE with a particular user. The messaging between initiator WTRU 205 and target WTRU 250 may occur over both a public channel and a laser channel. As an example, a conventional authentication and key agreement protocol could take place over a radio link while additional seeding material may be exchanged over the laser link. Providing optical and/or audio feedback may enable the user associated with initiator WTRU 205 and the user associated with target WTRU 250 to identify and authenticate each other.

[0134] Although features and elements are described above in particular combinations, one of ordinary skill in the art will appreciate that each feature or element can be used alone or in any combination with the other features and elements. In addition, the methods described herein may be implemented in a computer program, software, or firmware incorporated in a computer-readable medium for execution by a computer or processor. Examples of computer-readable media include electronic signals (transmitted over wired or wireless connections) and computer-readable storage media. Examples of computer-readable storage media include, but are not limited to, a read only memory (ROM), a random access memory (RAM), a register, cache memory, semiconductor memory devices, magnetic media such as internal hard disks and removable disks, magneto-optical media, and optical media such as CD-ROM disks, and digital versatile disks (DVDs). A processor in association with software may be used to implement a radio frequency transceiver for use in a WTRU, UE, terminal, base station, RNC, or any host computer.

*

*

*

What is Claimed:

1. A method for creating a secured private data link associated with a secret key between a first wireless transmit/receive unit (WTRU) and a second WTRU, the method comprising:
 - the first WTRU transmitting an initiation message, the initiation message indicating that the first WTRU wishes to establish the secured private data link associated with the secret key;
 - receiving a response message, the response message notifying the first WTRU to establish the secured private data link;
 - establishing the secured private data link using directional electromagnetic signals; and
 - receiving an acknowledgement message, the acknowledgement message indicating the secured private data link has been established.
2. The method of claim 1, wherein establishing the private data link using directional electromagnetic signals comprises transmitting key information.
3. The method of claim 1 where in the initiation message includes a first token and the response message includes a second token.
4. The method of claim 3 further comprising:
 - generating the secret key from the first token and the second token; and
 - transmitting a message using the secret key.
5. The method of claim 1 further comprising sending a message requesting the second WTRU transmit a coded light pattern or sound upon receipt of the message.
6. The method of claim 1 further comprising determining a propagation delay between the time the initiation message was transmitted and the time the response message was received.
7. The method of claim 6, wherein transmitting the key information occurs when the propagation delay is below a security threshold.
8. The method of claim 2 further comprising:

adjusting the intensity of the directional electromagnetic signals to keep the signal-to-noise ratio at the second WTRU at or above a detectable level; and
and transmitting the key information at the adjusted intensity of the directional electromagnetic signals.

9. The method of claim 2 further comprising modulating the intensity of the directional electromagnetic signals to control the power allocated to the transmission of the key information while ensuring that the directional electromagnetic signals are visible.

10. The method of claim 2, further comprising:
increasing a modulation factor of the directional electromagnetic signals while transmitting pseudo random coded packets;
fixing the modulation factor when the response message has been received; and
and transmitting the key information at the fixed modulation factor.

11. The method of claim 2 further comprising:
setting the average directional electromagnetic signals intensity of the directional electromagnetic signals to a level that provides visibility;
modulating the power of data slots the directional electromagnetic signals carries to keep the signal-to-noise ratio at the second WTRU at or above a detectable level; and
transmitting the key information using the modulated data slots.

12. The method of claim 2, wherein the key information includes the secret key.

13. The method of claim 2, wherein the key information includes a message that is encrypted with the secret key.

14. The method of claim 2, wherein the key information includes seeding data to enable the second WTRU to generate the secret key.

15. The method of claim 2, wherein the key information includes a cache of keys to be used for encrypted communications, the cache of keys including the secret key.

16. The method of claim 2, wherein the key information includes payment information that is encrypted with the secret key and provides payment for a purchase.
17. A method for creating a secured private data link associated with a secret key between a first wireless transmit/receive unit (WTRU) and a second WTRU, the method comprising:
the first WTRU receiving an initiation message, the initiation message indicating that the second WTRU wishes to establish the secured private data link associated with the secret key;
transmitting a response message, the response message notifying the second WTRU to establish the secured private data link;
establishing the secured private data link with the second WTRU using directional electromagnetic signals; and
transmitting an acknowledgement message, the acknowledgement message indicating the secured private data link has been established.
18. The method of claim 17, wherein establishing the secured private data link using directional electromagnetic signals comprises receiving key information.
19. The method of claim 17, wherein the initiation message includes a first token and the response message includes a second token.
20. The method of claim 17 further comprising:
generating the secret key from the first token and the second token; and
transmitting a message using the secret key.
21. The method of claim 17 further comprising receiving a message requesting the first WTRU to transmit a coded light pattern or sound upon receipt of the message.
22. The method of claim 17 further comprising determining a propagation delay between the time the initiation message was received and the time the response message was transmitted.
23. The method of claim 22, wherein establishing the secured private data link occurs when the propagation delay is below a security threshold.

24. The method of claim 17 further comprising receiving an authentication ID from the second WTRU.
25. The method of claim 24 further comprising:
 authenticating the second WTRU with the authentication ID; and
 transmitting an authentication response to the second WTRU when the second WTRU has been authenticated.
26. The method of claim 17, wherein the initiation message includes an initiation key.
27. The method of claim 26 further comprising encrypting the response message with the initiation key.
28. The method of claim 17, wherein the response message is transmitted when an initiation message is received at or above a detectable level.
29. The method of claim 17 further comprising:
 receiving pseudo random coded packets from the directional electromagnetic signals at an increasing a modulation factor;
 determining the received modulation factor of the received pseudo random coded packets; and
 transmitting the response message when the received modulation factor exceeds a security threshold.
30. The method of claim 17 wherein receiving the key information comprises:
 receiving data slots carried by the directional electromagnetic signals;
 determining the power of the data slots; and
 deriving the key information from the data slots when the power of the data slots achieves a signal-to-noise ratio above a power threshold.
31. A wireless transmit/receive unit (WTRU) for creating a secured private data link associated with a secret key between the WTRU and a communications node, the WTRU configured to:

transmit an initiation message, the initiation message indicating that the WTRU wishes to establish the secured private data link associated with the secret key;

receive a response message, the response message notifying the WTRU to establish the secured private data link;

establish the secured private data link using directional electromagnetic signals; and

receive an acknowledgement message, the acknowledgement message indicating that the secured private data link has been established.

32. The WTRU of claim 31 further configured to transmit key information using the directional electromagnetic signals.

33. The WTRU of claim 31, wherein the initiation message includes a first token and the response message includes a second token.

34. The WTRU of claim 33 further configured to:
generate the secret key from the first token and the second token; and
transmit a message using the secret key.

35. The WTRU of claim 31 further configured to send a message requesting that the communications node transmit a coded light pattern or sound upon receipt of the message.

36. The WTRU of claim 31 further configured to determine a propagation delay between the time the initiation message was transmitted and the time the response message was received.

37. The WTRU of claim 36 further configured to transmit the key information when the propagation delay is below a security threshold.

38. The WTRU of claim 31 further configured to:
adjust the intensity of the directional electromagnetic signals to keep the signal-to-noise ratio at the communications node at or above a detectable level; and
and transmit the key information at the adjusted intensity of the directional electromagnetic signals.

39. The WTRU of claim 31 further configured to modulate the intensity of the directional electromagnetic signals to control the power allocated to the transmission of the key information while enabling the directional electromagnetic signals to be visible.

40. The WTRU of claim 31 further configured to:
increase a modulation factor of the directional electromagnetic signals while transmitting pseudo random coded packets;
set the modulation factor when the response message has been received; and
and transmit the key information at the set modulation factor.

41. The WTRU of claim 31 further configured to:
set the average directional electromagnetic signals intensity of the directional electromagnetic signals to a level that provides visibility;
modulate the power of data slots the directional electromagnetic signals carries to keep the signal-to-noise ratio at the communications node at or above a detectable level; and .
transmit the key information using the modulated data slots.

1/10

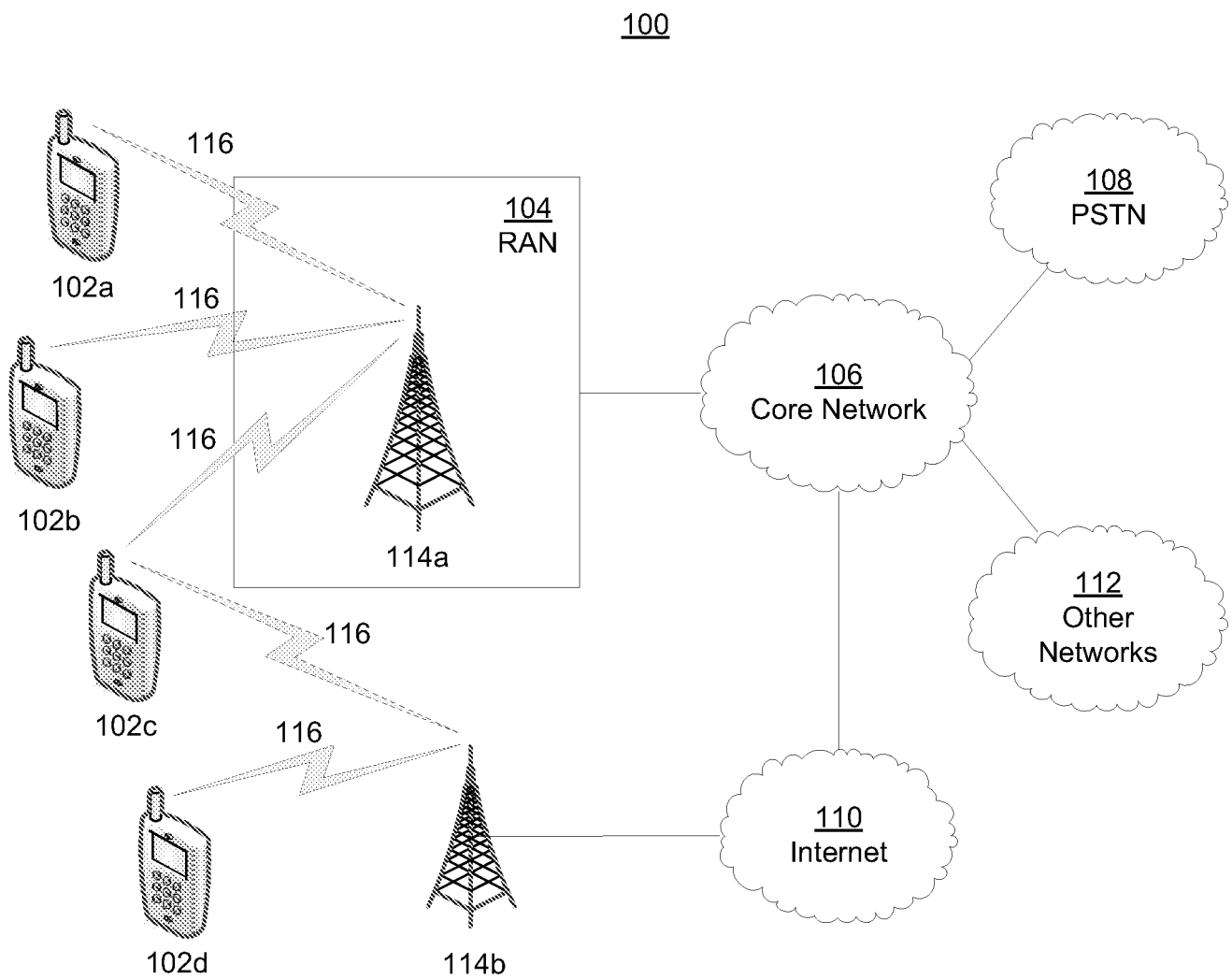


FIG. 1A

2/10

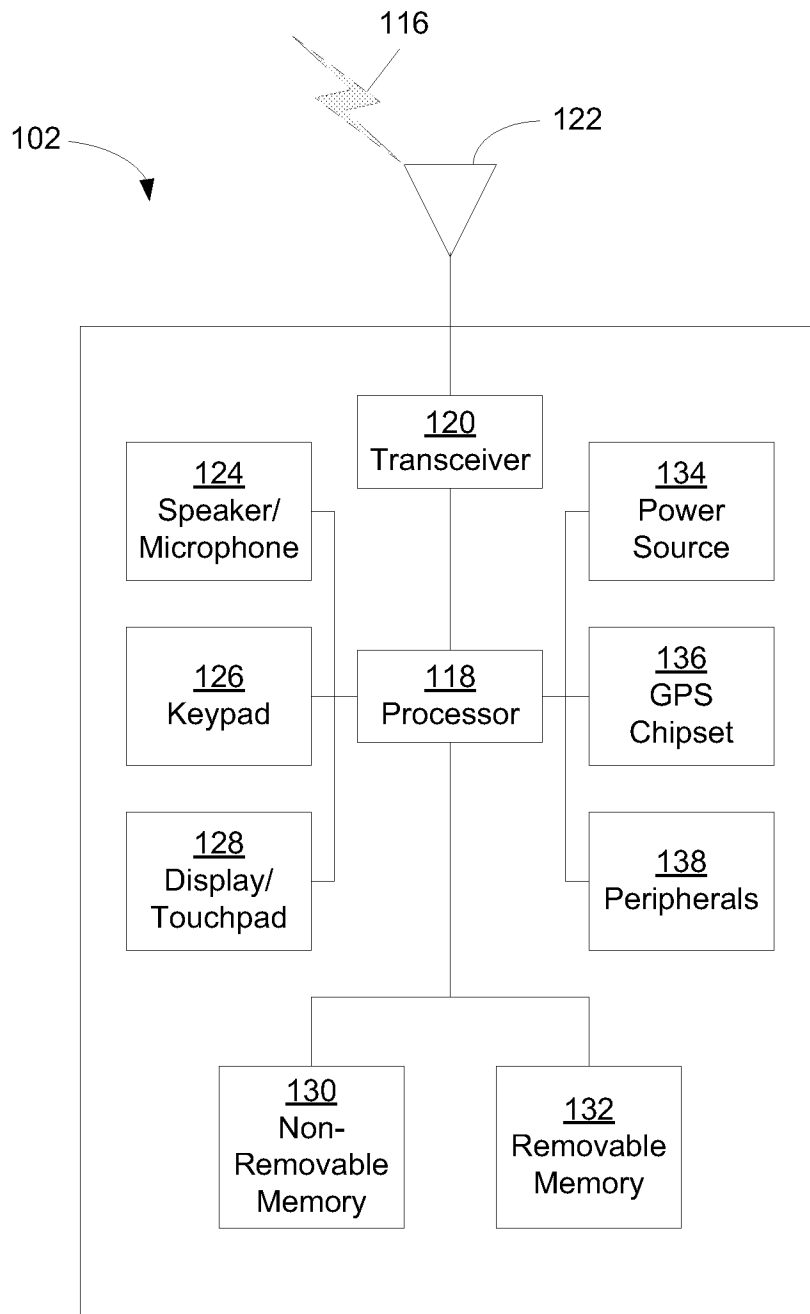


FIG. 1B

3/10

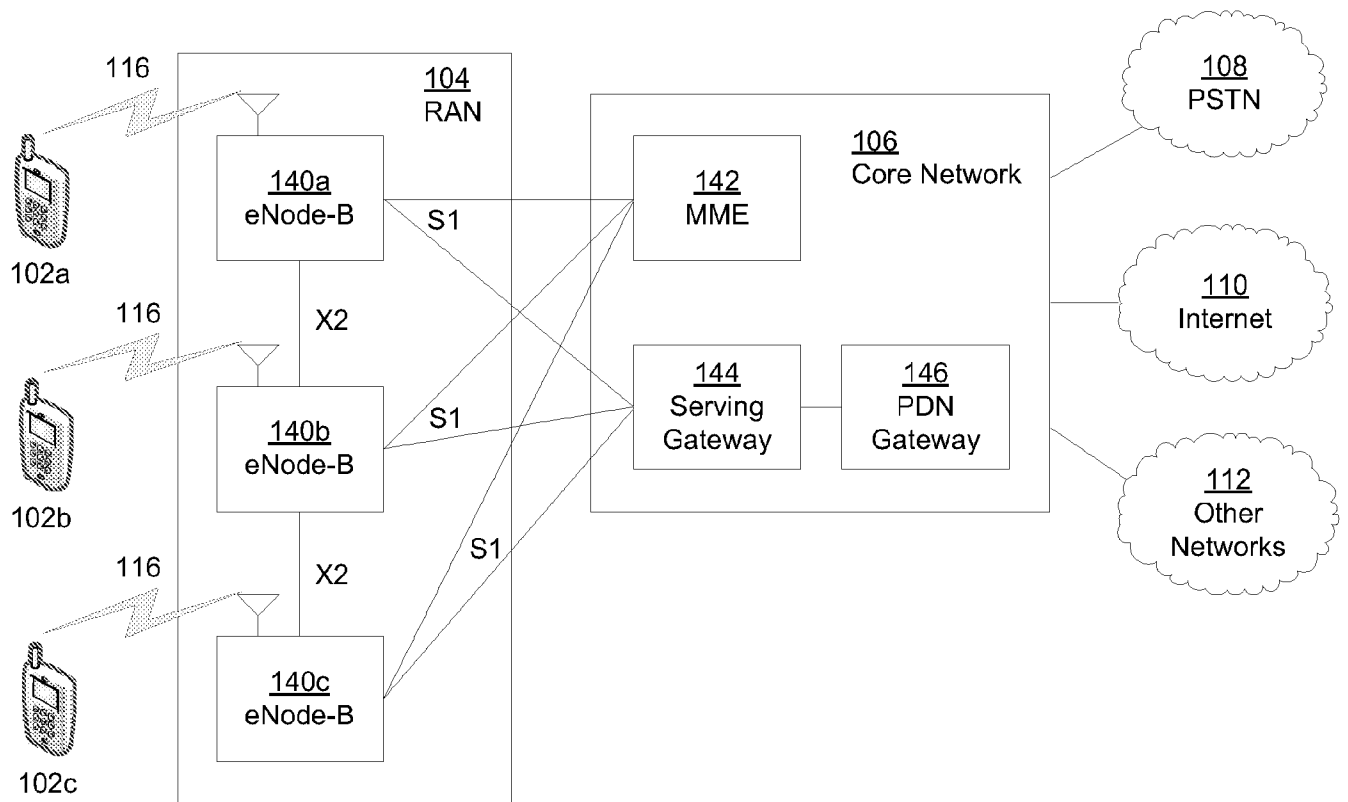


FIG. 1C

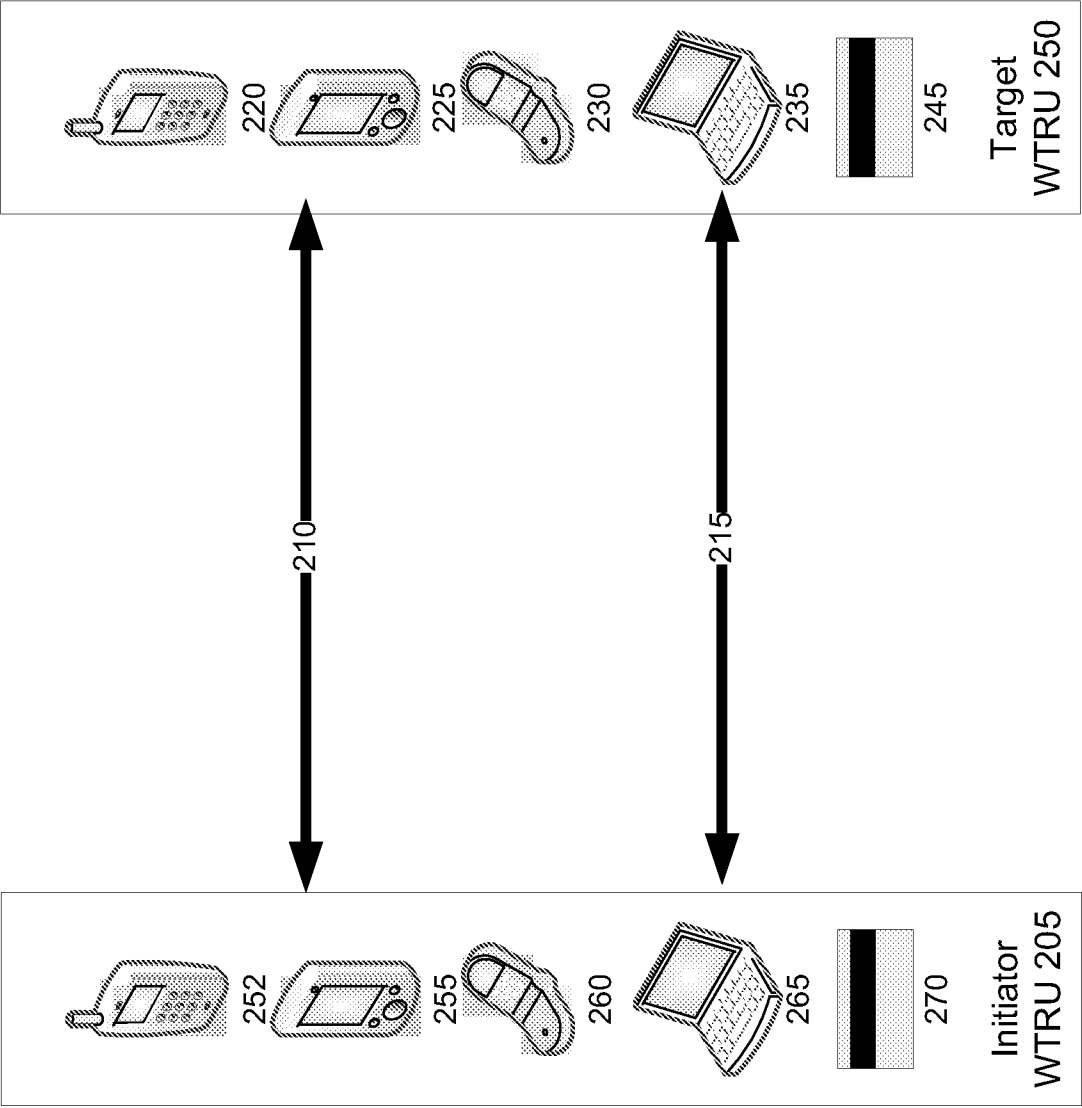


Figure 2

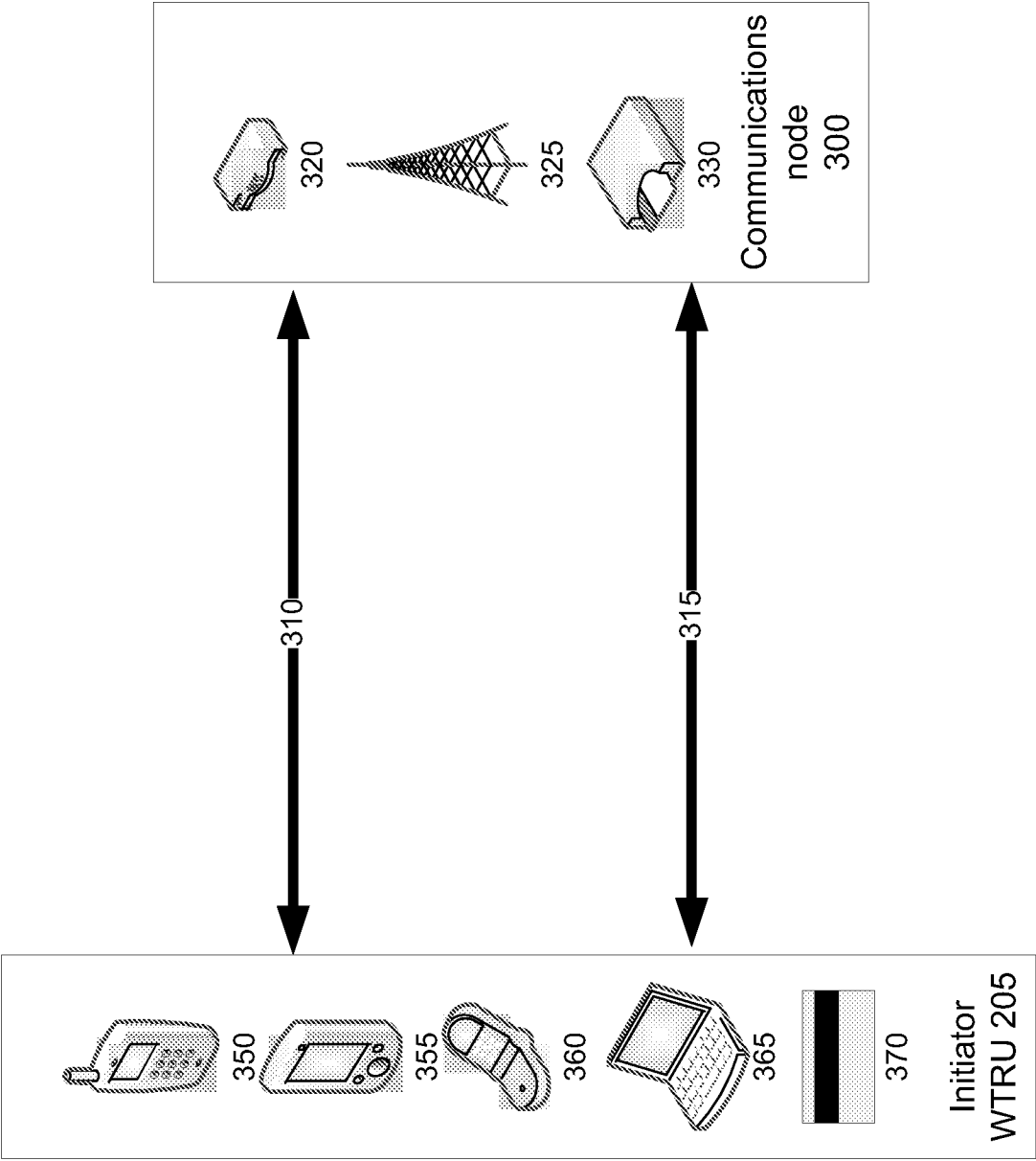


Figure 3

400



Figure 4

500



Figure 5

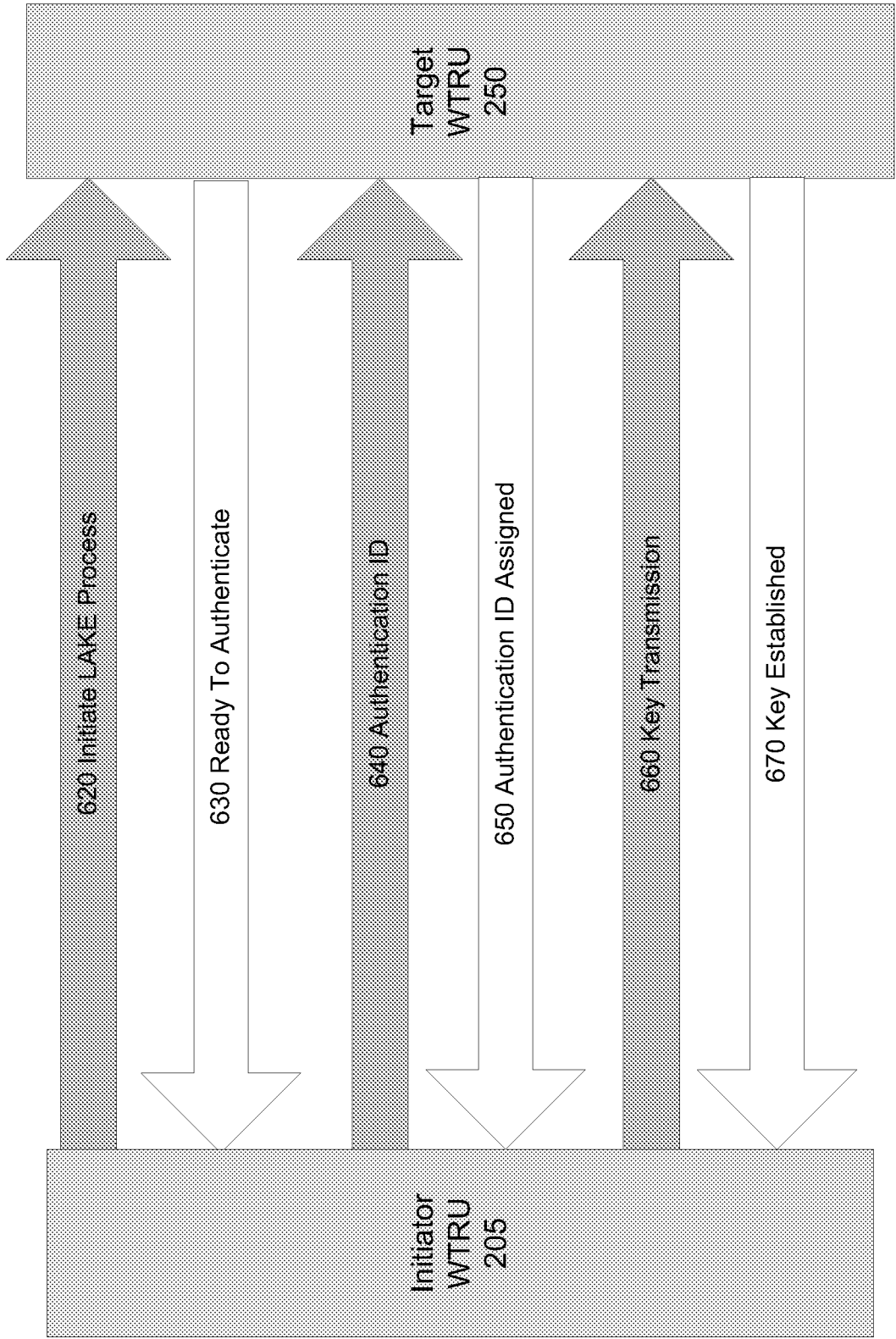


Figure 6

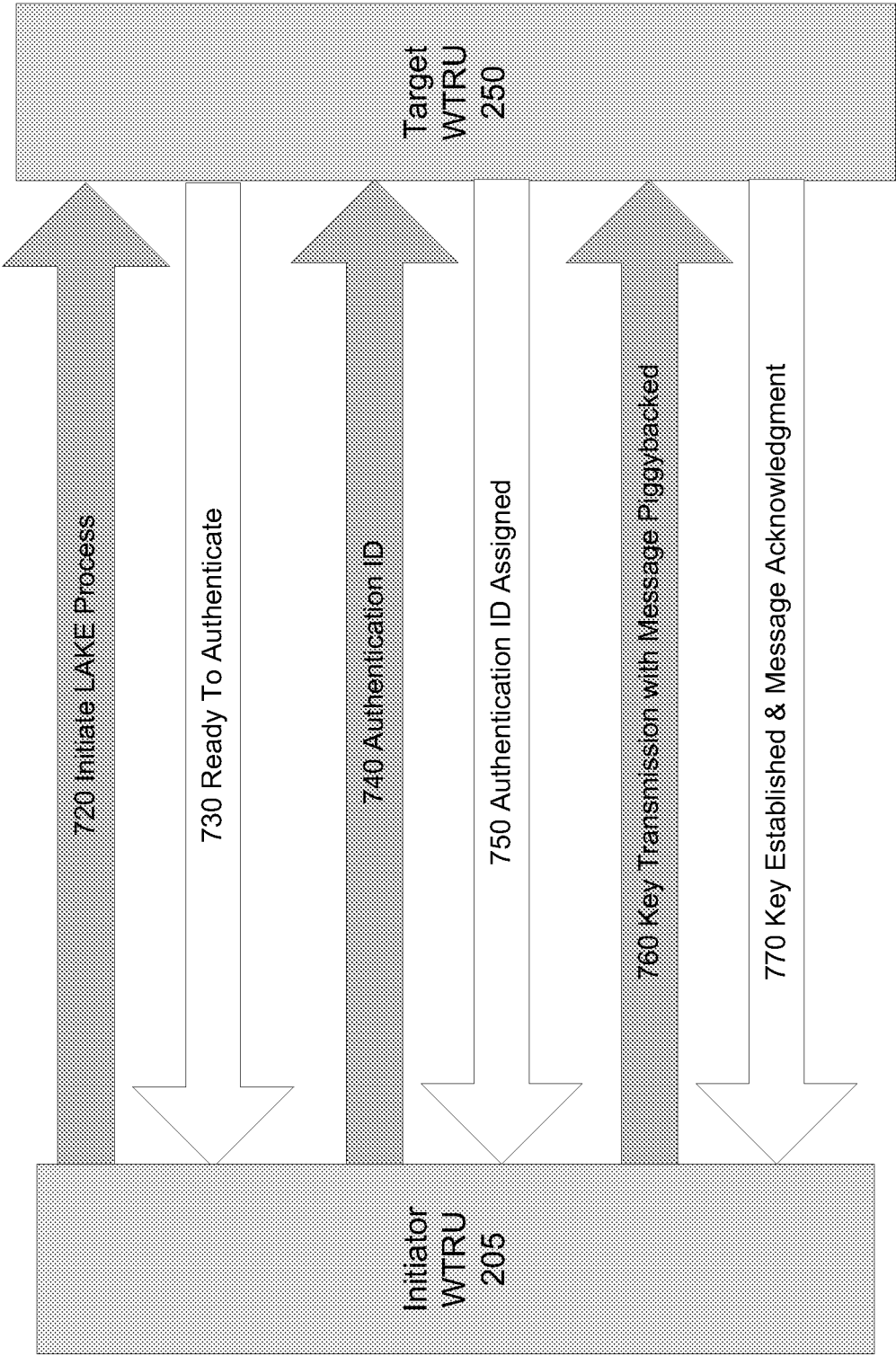


Figure 7

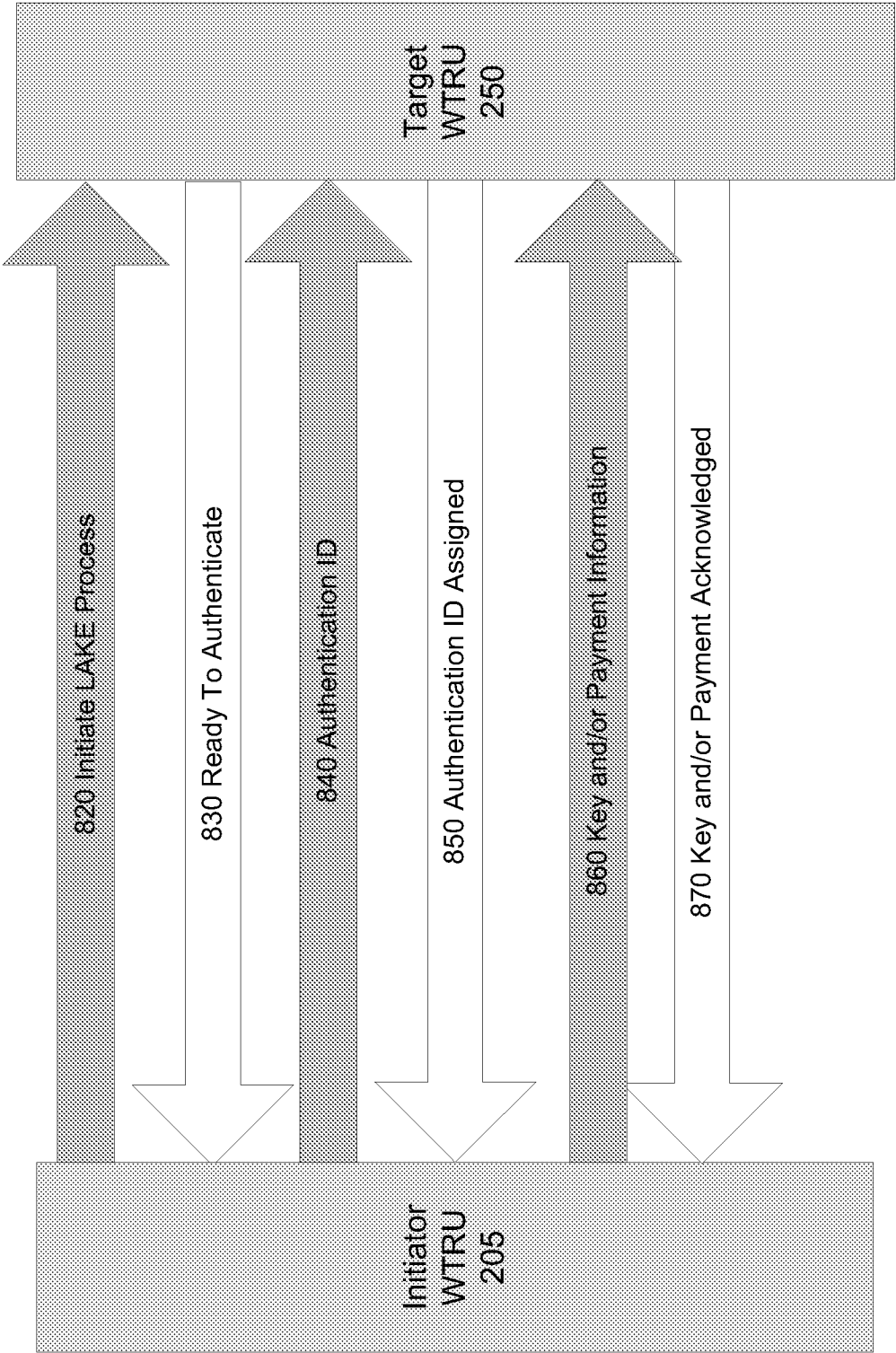


Figure 8

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2011/031524

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04W12/04 H04L29/06
ADD. H04W12/12

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L H04W

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

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

EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	RENE MAYRHOFFER ET AL: "A Human-Verifiable Authentication Protocol Using Visible Laser Light", AVAILABILITY, RELIABILITY AND SECURITY, 2007. ARES 2007. THE SECOND INTERNATIONAL CONFERENCE ON, IEEE, PI, 1 April 2007 (2007-04-01), pages 1143-1148, XP031079701, ISBN: 978-0-7695-2775-8 the whole document ----- -/--	1-41



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
"&" document member of the same patent family

Date of the actual completion of the international search

12 July 2011

Date of mailing of the international search report

20/07/2011

Name and mailing address of the ISA/

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040,
Fax: (+31-70) 340-3016

Authorized officer

Kopp, Klaus

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2011/031524

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 1 940 115 A2 (INTEL CORP [US]) 2 July 2008 (2008-07-02) abstract paragraph [0001] paragraph [0005] paragraph [0007] - paragraph [0008] paragraph [0011] paragraph [0014] - paragraph [0015] paragraph [0020] - paragraph [0031] figures 2,3	1-41
X	----- ZISIADIS D ET AL: "ViDPsec Visual Device Pairing Security Protocol", COMPUTATIONAL SCIENCE AND ENGINEERING, 2009. CSE '09. INTERNATIONAL CONFERENCE ON, IEEE, PISCATAWAY, NJ, USA, 29 August 2009 (2009-08-29), pages 359-364, XP031544005, ISBN: 978-1-4244-5334-4 abstract page 360 - page 362	1-41
A	----- KUMAR A ET AL: "A comparative study of secure device pairing methods", PERVASIVE AND MOBILE COMPUTING, ELSEVIER, NL, vol. 5, no. 6, 1 December 2009 (2009-12-01), pages 734-749, XP026772140, ISSN: 1574-1192, DOI: DOI:10.1016/J.PMCJ.2009.07.008 [retrieved on 2009-07-18] abstract page 734 - page 738	1-27, 31-41
A	----- GB 2 449 485 A (ITI SCOTLAND LTD [GB]) 26 November 2008 (2008-11-26) abstract claims 2-6	4,20,34
A	----- WO 2004/047461 A2 (INTERDIGITAL TECH CORP [US]) 3 June 2004 (2004-06-03) abstract paragraph [0018] - paragraph [0023] -----	28-30

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/US2011/031524

Patent document cited in search report		Publication date	Patent family member(s)		Publication date
EP 1940115	A2	02-07-2008	CN	101286839 A	15-10-2008
			JP	2008178092 A	31-07-2008
			KR	20080063130 A	03-07-2008
			US	2008162937 A1	03-07-2008

GB 2449485	A	26-11-2008	AU	2008252713 A1	27-11-2008
			CN	101711471 A	19-05-2010
			EP	2147538 A2	27-01-2010
			WO	2008142367 A2	27-11-2008
			JP	2010528358 A	19-08-2010
			KR	20100027155 A	10-03-2010
			US	2011119745 A1	19-05-2011

WO 2004047461	A2	03-06-2004	AT	443377 T	15-10-2009
			AU	2003287680 A1	15-06-2004
			EP	1568141 A2	31-08-2005
			TW	I271041 B	11-01-2007
