Office de la Propriété Intellectuelle du Canada
Un organisme d'Industrie Canada

Canadian Intellectual Property Office
An agency of Industry Canada

CA 2548436 C 2012/07/03

(11)(21) 2 548 436

(12) BREVET CANADIEN
CANADIAN PATENT

(13) C

(86) Date de dépôt PCT/PCT Filing Date: 2004/11/24
(87) Date publication PCT/PCT Publication Date: 2005/06/16
(45) Date de délivrance/Issue Date: 2012/07/03
(85) Entrée phase nationale/National Entry: 2006/06/02
(86) N° demande PCT/PCT Application No.: CA 2004/002020
(87) N° publication PCT/PCT Publication No.: 2005/055545
(30) Priorité/Priority: 2003/12/05 (US60/527,335)

(51) Cl.Int./Int.Cl. *H04W 12/08* (2009.01),
H04W 80/04 (2009.01)

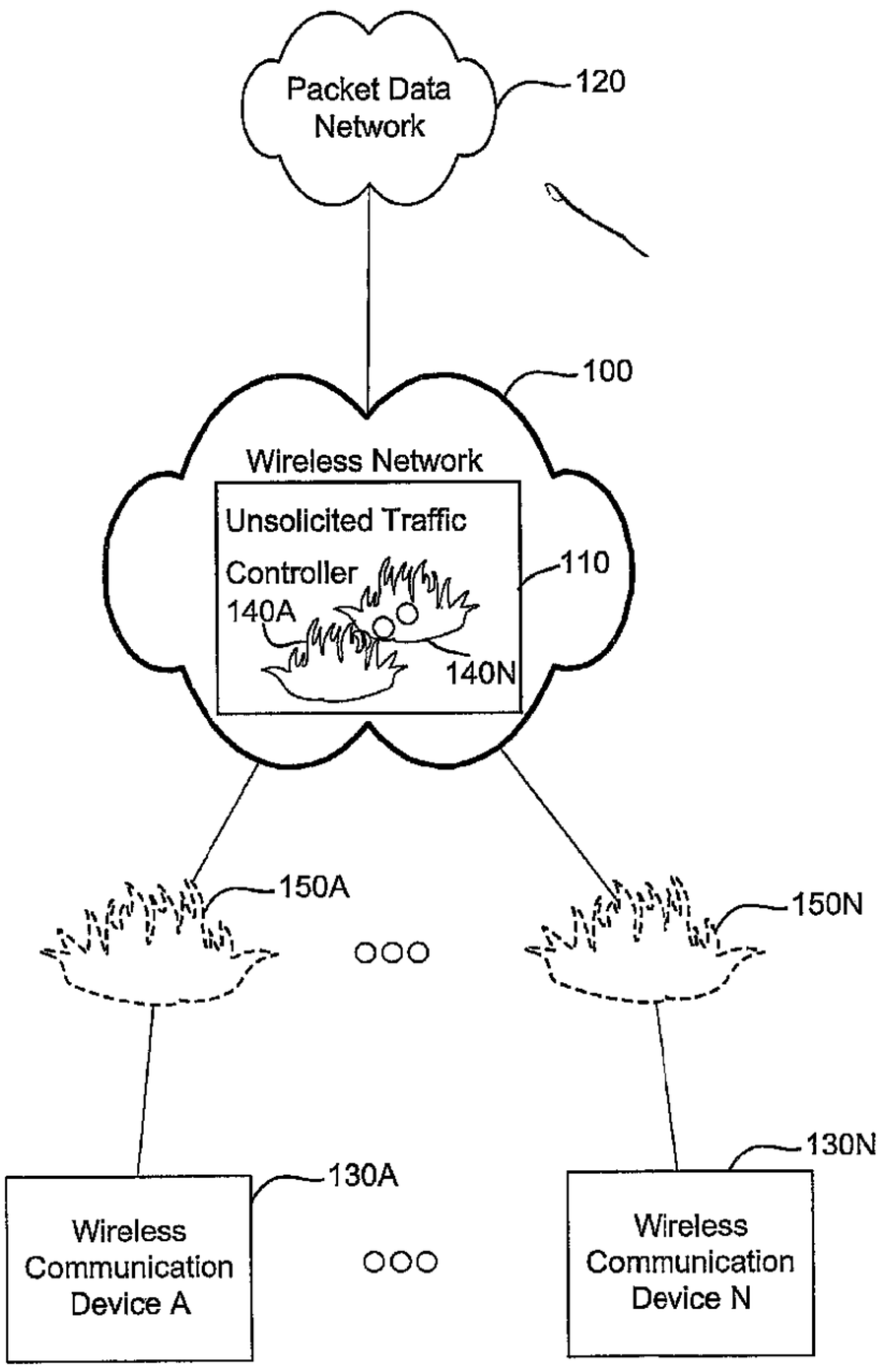
(72) Inventeurs/Inventors:
WILLEY, WILLIAM DANIEL, US;
ZHAO, WEN, CA;
PLESTID, THOMAS LEONARD TREVOR, CA;
DUNK, CRAIG, CA;
ESTABLE, LUIS PABLO, CA;
ISLAM, MUHAMMAD KHALEDUL, CA

(73) Propriétaire/Owner:
RESEARCH IN MOTION LIMITED, CA

(74) Agent: BORDEN LADNER GERVAIS LLP

(54) Titre : DISPOSITIF ET PROCEDE SERVANT A CONTROLER LE TRAFIC NON SOLLICITE DESTINE A UN SYSTEME DE COMMUNICATION RADIO

(54) Title: APPARATUS AND METHOD OF CONTROLLING UNSOLICITED TRAFFIC DESTINED TO A WIRELESS COMMUNICATION DEVICE



(57) Abrégé/Abstract:
An apparatus and method of controlling unsolicited traffic are disclosed herein. The apparatus and method can be applied to wireless communication networks such as CDMA2000, UMTS, GPRS and the like so that traffic which is not solicited by wireless

CA 2548436 C 2012/07/03

(11)(21) 2 548 436

(13) C

(57) Abrégé(suite)/Abstract(continued):
communication devices operating on those networks is not sent over the air needlessly. The present application provides techniques to block unsolicited traffic based on the identity of a user (for example based on International Mobile Station Identity (IMSI), Network Access Identifier (NAI), Mobile Station Internet Services Digital Network Number (MSISDN), Session Initiation Protocol (SIP) Universal Resource Locator (url)) as opposed to techniques that are based on a session or IP address, such as a traditional firewall. In accordance to this application, user identity based techniques are applied to block unsolicited traffic whenever a user has established a data session. Further in accordance with this application, user identity based techniques are persisted across changes in IP address and/or session.

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
16 June 2005 (16.06.2005)

PCT

(10) International Publication Number
WO 2005/055545 A1

(51) International Patent Classification[7]: H04L 29/02, 12/56, H04Q 7/20

(21) International Application Number:
PCT/CA2004/002020

(22) International Filing Date:
24 November 2004 (24.11.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/527,335 5 December 2003 (05.12.2003) US

(71) Applicant *(for all designated States except US)*: **RESEARCH IN MOTION LIMITED** [CA/CA]; 295 Phillip Street, Waterloo, Ontario N2L 3W8 (CA).

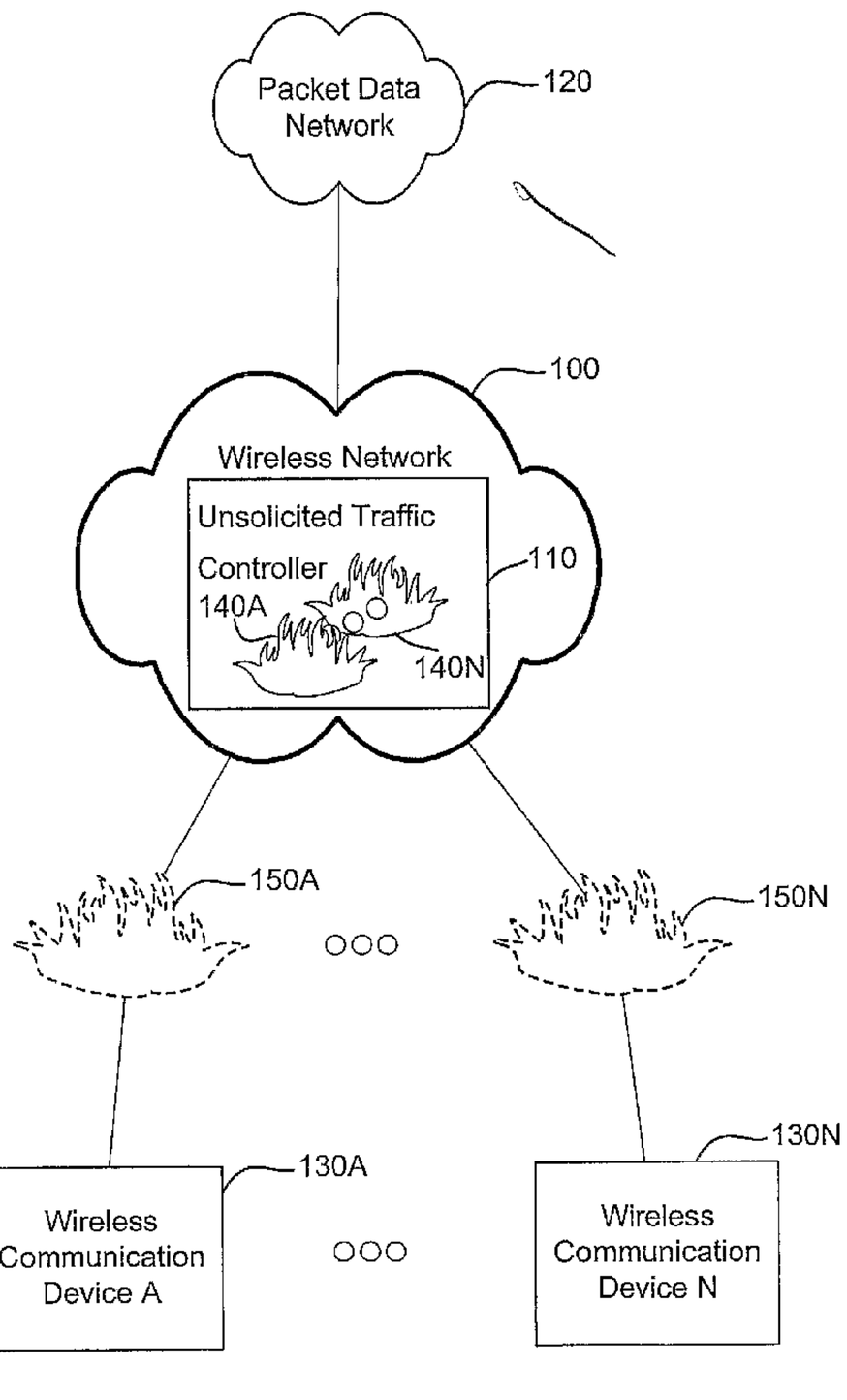
(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: **ZHAO, Wen** [CA/CA]; 27 Wynridge Place, Kanata, Ontario K2M 2S8 (CA). **PLESTID, Thomas Leonard Trevor** [CA/CA]; 180 Bradford Street, Ottawa, Ontario K2B 5Z4 (CA). **DUNK, Craig** [CA/CA]; 23 Grey Oak Drive, Guelph, Ontario N1L 1P2 (CA). **ISLAM, Muhammad Khaledul** [CA/CA]; 88 Broughton Street, Ottawa, Ontario K2K 3N4 (CA). **ESTABLE, Luis Pablo** [CA/CA]; 51 rue de l'Alouette, Gatineau, Quebec J9A 3J3 (CA). **WILLEY, William Daniel** [US/US]; # 22E, 1200 Gough Street, San Francisco, California 94109 (US).

(74) Agent: **CASSAN MACLEAN**; Suite 401, 80 Aberdeen Street, Ottawa, Ontario K1S 5R5 (CA).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD,

[Continued on next page]

(54) Title: APPARATUS AND METHOD OF CONTROLLING UNSOLICITED TRAFFIC DESTINED TO A WIRELESS COMMUNICATION DEVICE



(57) Abstract: An apparatus and method of controlling unsolicited traffic are disclosed herein. The apparatus and method can be applied to wireless communication networks such as CDMA2000, UMTS, GPRS and the like so that traffic which is not solicited by wireless communication devices operating on those networks is not sent over the air needlessly. The present application provides techniques to block unsolicited traffic based on the identity of a user (for example based on International Mobile Station Identity (IMSI), Network Access Identifier (NAI), Mobile Station Internet Services Digital Network Number (MSISDN), Session Initiation Protocol (SIP) Universal Resource Locator (url)) as opposed to techniques that are based on a session or IP address, such as a traditional firewall. In accordance to this application, user identity based techniques are applied to block unsolicited traffic whenever a user has established a data session. Further in accordance with this application, user identity based techniques are persisted across changes in IP address and/or session.

WO 2005/055545 A1

WO 2005/055545 A1

MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

APPARATUS AND METHOD OF CONTROLLING UNSOLICITED TRAFFIC DESTINED TO A WIRELESS COMMUNICATION DEVICE

BACKGROUND

TECHNICAL FIELD

[0001] This application relates to wireless communication techniques in general, and to an apparatus and method of controlling unsolicited traffic destined to a wireless communication device in particular.

RELATED ART

[0002] Some wireless communication devices are known to receive unsolicited traffic. For example, a Code Division Multiple Access (CDMA) 2000 wireless communication device operating in simple Internet Protocol (IP) configuration can receive unsolicited IP packets. Although other non-wireless devices are known to receive unsolicited traffic, techniques traditionally used with non-wireless devices may be inappropriate as there is a significant waste of resources, both in the wireless network, as well as in a wireless communication device, whenever unsolicited traffic gets sent over the air interfaces.

[0003] One technique that is known, which partly addresses this problem, involves using a private addressing scheme. However, even if a private addressing scheme is used, this technique may not prevent unsolicited traffic initiated from within the private address space from reaching the wireless communication device. Furthermore, this technique may be unacceptable if a public address is desired, as is the case for example with certain CDMA2000 wireless carriers. Another technique that is known, which partly addresses this problem, involves using a firewall within the wireless

communication network. However, firewall rules may have to be manually configured, and may be ineffective if the rules depend on the wireless communication devices addresses, which may be subject to change due to mobility. For example, in the case of CDMA2000, IP address can be dynamically assigned and reused, which may render the firewall rules ineffective for the wireless communication device.

[0004] Generally speaking there are three categories of unsolicited traffic which require screening: (a) Stale Session Unsolicited Traffic - When a mobile device stops using an IP address A without first terminating communications previously established to other servers, packets may continue to be sent to the same IP address A. Examples are Virtual Private Network (VPN) packets, Peer-to-Peer (P2P) file sharing, spy ware and many more. Such packets often are sent continuously to the device. Unsolicited traffic can arrive via a stale IP session when a second mobile device acquires IP address A, and starts receiving packets from stale IP session(s), the unsolicited traffic originally intended to reach the first mobile device; and (b) Inter-subscriber Intra-subnet Unsolicited Packets – Subnet constrained broadcasts or serial unicast from one mobile to another are effectively unsolicited packets received from other subscriber served by the same operator (e.g. worms exploiting subnet discovery protocols such as Internet Control and Management Protocol (ICMP) or Simple Service Discovery Protocol (SSDP); and (c) malicious packets.

[0005] A mobile device may not be able to block a network from sending packets, since a connection to the network or a call must be established and IP data examined prior to a packet's validity being determined. Packets from Stale IP sessions can be considered unsolicited packets. There are network and mobile device impacts which arise from unsolicited packets. First, the network impact is such that unsolicited traffic means inefficient use of network resources (sending undesired data to users),

resulting in data delivery delays for other users as well as the possibility of complete network unavailability for voice or data service for many users within a geographic area. Second, the device impact is such that unsolicited traffic means a mobile device may be paged to set up calls on an ongoing basis, resulting in very rapid battery drain as well as erroneous accounting of data usage records for a particular data capable mobile device. Thirdly, receiving undesired unsolicited traffic can be irritating to customers.

BRIEF SUMMARYOF THE INVENTION

[0006] In order to overcome the negative impacts highlighted above, the present application provides an apparatus and method of controlling unsolicited traffic which can be applied to wireless communication networks such as CDMA2000, Universal Mobile Telecommunications System (UMTS), General Packet Radio Service (GPRS) and the like so that traffic which is not solicited by wireless communication devices operating on those networks is not sent over the air needlessly. The present application provides techniques to block unsolicited traffic based on the identity of a user (for example based on International Mobile Station Identity (IMSI), Network Access Identifier (NAI), Mobile Station Internet Services Digital Network Number (MSISDN), Session Initiation Protocol (SIP) Universal Resource Locator (url)) as opposed to techniques that are based on a session or IP address, such as a traditional firewall. In accordance to this application, user identity based techniques are applied to block unsolicited traffic whenever a user has established a data session. Further in accordance with this application, user identity based techniques are persisted across changes in IP address and/or session.

[0007] According to a first aspect of the present application, there is provided in a wireless communication network, the wireless communications network comprising

an unsolicited traffic controller (UTC) coupled to a packet data network and a plurality of wireless communication devices, a method of controlling traffic destined to a first one of the plurality of wireless communication devices comprising the steps of: storing a set of traffic control rules associated with the first one of the plurality of wireless communication devices; determining a first identify corresponding to a user of the first one of the plurality of wireless communication devices; determining that a first packet received from the packet data network is destined to the first one of the plurality of wireless communication devices; selecting the stored traffic control rules associated with the determined first identify; applying the selected traffic control rules to determine if the first packet is unsolicited by said user; and preventing the first packet from being sent to the first one of the plurality of communication devices if the first packet is determined to be unsolicited.

[0008] According to a second aspect of the present application there is provided a computer readable medium having stored thereon, computer executable instructions which when executed by a processor in an unsolicited traffic controller (UTC), cause the UTC to: store a set of traffic control rules associated with a specified one of a plurality of wireless communication devices; determine an identify corresponding to a user of the specified one of the plurality of wireless communication devices; determine that a first packet received from a packet data network is destined to the specified one of the plurality of wireless communication devices; select the stored set of traffic control rules associated with the determined identity; apply the selected traffic control rules to determine if the first packet is unsolicited by the user; and prevent the first packet from being sent to said specified one of the plurality of communication devices if the first packet is determined to be unsolicited, wherein the

UTC is resident in a wireless communications network and coupled to said packet data network and said plurality of wireless communication devices.

[0009] According to a third aspect of the present application there is provided a carrier wave embodying a computer data signal representing sequences of instructions which, when executed by a processor, cause the processor to: store a set of traffic control rules associated with a specified one of a plurality of wireless communication devices; determine an identify corresponding to a user of the specified one of the plurality of wireless communication devices; determine that a first packet received from a packet data network is destined to the specified one of the plurality of wireless communication devices; select the stored set of traffic control rules associated with the determined identify; apply the selected traffic control rules to determine if the first packet is unsolicited by the user; and prevent the first packet from being sent to the specified one of the plurality of communication devices if the first packet is determined to be unsolicited, wherein the processor is an unsolicited traffic controller (UTC), and wherein the UTC is resident in a wireless communications network and coupled to said packet data network and said plurality of wireless communication devices.

[0010] According to a fourth aspect of the application, there is provided in a wireless communication network, an apparatus for controlling unsolicited traffic destined to a specified one of a plurality wireless communication devices, the apparatus comprising: a first interface configured to receive traffic from a packet data network; a second interface configured to send traffic to the specified one of the plurality of wireless communication devices; a first storage medium having stored thereon computer executable instructions representing a set of traffic control rules; and an unsolicited traffic controller (UTC) communicating with the first and second

interfaces and the first storage medium, wherein the UTC determines an identity assigned to said specified one of said plurality of wireless communication devices, and executes the computer executable instructions to selectively block said unsolicited traffic received over the first interface from being sent over the second interface to the specified one of the plurality wireless communication devices.

[0011] Other aspects and features of the present application will be apparent to those ordinarily skilled in the art upon review of the following description of the specific embodiments of an apparatus and method of controlling unsolicited traffic destined to a wireless communication device.

BRIEF DESCRIPTION OF THE DRAWINGS

[0012] Embodiments of the present application will now be described, by way of example only, with reference to the attached figures, wherein:

FIG. 1 is a block diagram illustrating a wireless network including an embodiment of the unsolicited traffic controller (UTC), provided in accordance with the present application;

FIG. 2 is an interaction diagram illustrating the technique of implicit unsolicited traffic control, provided in accordance with the present application;

FIG. 3 is an interaction diagram illustrating the technique of explicit unsolicited traffic control, provided in accordance with the present application;

FIG. 4 is an interaction diagram illustrating the technique of dynamic unsolicited traffic control, provided in accordance with the present application;

FIGs. 5-8 are interaction diagrams illustrating the combination of the techniques shown in FIGs. 2-4.

FIG. 9 is an interaction diagram illustrating the technique of delegating unsolicited traffic control, provided in accordance with the present application;

FIG. 10 is a block diagram illustrating a wireless network including an embodiment of a UTC, provided in accordance with the present application.

FIG. 11 is an interaction diagram illustrating the UTC behaviour when a wireless communication device ceases operation, provided in accordance with the present application;

FIG. 12 is an interaction diagram illustrating the UTC behaviour when a previously active wireless communication device is becomes active again, provided in accordance with the present application;

FIG. 13 is an interaction diagram illustrating the interaction when an address assigned to a wireless communication device is devolved and re-assigned to another wireless communication device, provided in accordance with the present application;

FIG. 14 is an interaction diagram illustrating the interaction when a wireless communication does an inter-UTC handoff, provided in accordance with the present application;

FIG. 15 is a block diagram illustrating a wireless network including an embodiment of a UTC adapted to a 3rd Generation Partnership Project (3GPP) General Packet Radio Service (GPRS) environment, provided in accordance with the present application; and

FIG. 16 is a block diagram illustrating an exemplary embodiment of an unsolicited traffic controller apparatus provided in accordance with the present application.

[0013] Same reference numerals are used in different figures to denote similar elements.

DETAILED DESCRIPTION

[0014] Referring now to the drawings, FIG. 1 is a block diagram illustrating a wireless network including an embodiment of an unsolicited traffic controller (UTC), provided in accordance with the present application. The block diagram shows a wireless network **100** coupling a packet data network **120** with wireless communication devices **130A** ... **130N**, and coupling wireless communication devices to one another, thereby enabling traffic to flow to and from packet data network **120** from and to wireless communication devices **130A** ... **130N**, and enabling traffic to flow to and from one wireless communication device **130A** to and from another wireless communication device **130N**.

[0015] Wireless network **100** includes an unsolicited traffic controller **110**, provided in accordance with the present application, the purpose of which is to affect the manner that the coupling between wireless communication devices **130A** ... **130N** to each other and to packet data network **120** occurs, so as to limit unsolicited traffic destined to wireless communication devices **130A** ... **130N**. Specifically, unsolicited traffic controller **110** includes a set of firewall-like rules **140A** ... **140N**, each of which corresponds to a specific wireless communication device **130A** ... **130N**, so that their combined effect is that the over the air interfaces behave as if they were each substantially firewalled **150A** ... **150N**.

[0016] Various embodiments of an unsolicited traffic controller are envisaged, each adapted to the particular requirements of a specific wireless network. For example, in an embodiment adapted to a CDMA wireless network, the unsolicited traffic controller is preferably located in at least one Packet Data Serving Node (PDSN) of the wireless network. Alternatively, in an embodiment adapted to a GPRS wireless network, the unsolicited traffic controller is preferably located in at least one Serving

GPRS Support Node (SGSN), further preferably in at least one Gateway GPRS Support Node (GGSN). The choice of where to locate the unsolicited traffic controller is guided by the principle that it should have access to all traffic destined to the wireless devices so as to control the flow of unsolicited traffic. In this regard, an unsolicited traffic controller can be adapted to operate with any given wireless network in view of the present application.

[0017] The unsolicited traffic controller **110** of FIG. 1 can be configured for co-operation with GPRS. GPRS is specified for example by 3GPP. A push initiator is located within packet data network **120**. Wireless communication devices **130A** thru **130N** are user equipment, and each includes at least one user agent, and a push recipient. Wireless network **100** is a public land mobile network, and includes a push function as well as push subscription profiles corresponding to each of the users of the user equipments. The unsolicited traffic controller **110** in this embodiment operates as a user based firewall by controlling unsolicited traffic based on the push subscription profiles of the users of the user equipment: depending on configuration, it is envisaged that the unsolicited traffic controller **110** controls traffic based on IMSI, NAI, MSISDN or SIP url, for example.

[0018] The remainder of this description and drawings will use IP packets and IP addresses for exemplary purposes only, as the techniques shown herein can be applied to many alternative forms of communication. For example, the technique could be applied to voice, e-mail, hyper text transfer protocol (http), file transfer protocol (ftp), multimedia messaging service (MMS) and short messaging service (SMS).

[0019] FIGs 2 to 8 define various techniques for unsolicited traffic control. As those skilled in the art will appreciate, traffic can be controlled by implicit, explicit or dynamic rules or a combination of such rules. With respect to the physical structure of

an unsolicited traffic controller, Figure 16, which will be discussed later, describes an exemplary embodiment. Most notably, the unsolicited traffic controller stores the rules (see element **1670** in FIG. 16) which are used to selectively block packets.

[0020] Turning now to FIG. 2, an interaction diagram illustrating the technique of implicit unsolicited traffic control, provided in accordance with the present application is depicted. The interaction diagram shows the interactions between a wireless communication device **230A**, an implicit unsolicited traffic controller **210**, and a packet data network **220**.

[0021] Before describing this first interaction diagram further, it is important to describe some common aspects of notation that are used in this and other interaction diagrams of the present application. Time flows generally downwards in this interaction diagram, as well as in the other interaction diagrams of the present application. Furthermore, the tilde (~), as used in the drawings, in this description, is meant to be shorthand for "substantially like". Thus IP ~A is meant to denote all addresses which are substantially like IP A for some specific purpose. For example, the notation IP ~A when used to qualify IP addresses which can reach a wireless device having IP A, this includes IP A itself, as well as broadcast addresses, anycast addresses and multicast addresses which would normally reach IP A in the absence of the techniques of the present application. The same tilde (~) notation is used to denote packets. For example, if PKT1 has destination address IP A, source address IP B, and data, then ~PKT1 is meant to denote packets which are substantially like PKT1 for some specific purpose, e.g. where a substantial similarity can be found between the source, destination, and/or data between the two packets. For instance, in TCP/IP and UDP/IP packets, data in one packet can be considered to be substantially like data

in another packet if port numbers or socket numbers are substantially similar. As another example, for ICMP/IP packets, data can include protocol numbers.

[0022] Operationally, wireless communication device **230A** is currently assigned address IP A. Implicit UTC **210** keeps track of what kind of traffic is considered solicited for IP A. This is shown at two times in the IP A Solicited blocks. Initially, IP A Solicited **225** does not contain any information with respect to the packets illustrated in FIG. 2. Consequently, when PKT1 **237** is destined to an address like IP A, i.e. IP ~A, implicit UTC **210** advantageously blocks **235** PKT1 **237**. Further advantageously, implicit UTC **210** recognizes that wireless communication device **230A** sent out PKT2 (~PKT1) **240**, and consequently updates the list IP A Solicited **245** to include ~PKT1 **250,** so that when PKT3 (~PKT1) **260** is destined to wireless communication device **230A**, it is not blocked.

[0023] FIG. 3 is an interaction diagram illustrating the technique of explicit unsolicited traffic control, provided in accordance with the present application. Turning now to FIG. 3. similarly to FIG. 2, wireless communication device **330A** is currently assigned address IP A. Explicit UTC **310** keeps track of what kind of traffic is considered unsolicited for wireless communication device **330A**. This is shown at an initial time prior to explicit block **340,** in the list IP A unsolicited block **325** and at a time subsequent to explicit block **340,** in the list IP A unsolicited block **345**. Initially, the list IP A Unsolicited **325** does not contain any information with respect to the packets illustrated in FIG. 3, and in particular PKT3 **337**. Consequently, when PKT3 **337** is destined to an address like IP A, i.e. ~IP A, Explicit UTC **310** advantageously allows PKT3 **337** to go through. After wireless communication device **230A** receives PKT3 **337**, it sends an Explicit Block ~PKT3 message **340** to Explicit UTC **310**. Consequently, explicit UTC **310** updates the list IP A Unsolicited **345** so as

to include ~PKT3 **350**, so that when a packet like PKT3, i.e. ~PKT3 **360**, is destined to wireless communication device **330A**, it is blocked **335**.

[0024] In an alternate embodiment, wireless communication device **330A** may also send an explicit unblock ~PKT3 message to Explicit UTC **310** at a later time so that Explicit UTC **310** updates IP A unsolicited **345** to exclude ~PKT3 **350.** At any time subsequent to the unblock ~PKT3, if a packet like PKT3, i.e. ~PKT3, is destined to wireless communication device **330A**, it would be let through.

[0025] In yet another embodiment, the explicit UTC aspect of FIG. 3 can be combined with the implicit UTC aspect of FIG. 2. If wireless communication device **330A**sends a packet ~PKT3 to the Packet Data Network **320**, even though explicit UTC **310** accepts explicit blocks and unblocks, it can also interpret ~PKT3 as an implicit unblock and consequently updates the IP A Unsolicited **345** to remove ~PKT3 **350,** so that when an other packet ~PKT3 is destined to wireless communication device **330A**, it is no longer blocked.

[0026] FIG. 4 is an interaction diagram illustrating the technique of dynamic unsolicited traffic control, provided in accordance with the present application. Turning now to FIG. 4, similarly to FIGs. 2-3, wireless communication device **430A** is currently assigned address IP A. Dynamic UTC **410** keeps track of what kind of traffic is considered unknown for A. This is shown at two times in the A unsolicited blocks. Initially, the list IP A Unknown **425** does not contain any information with respect to the packets illustrated in FIG. 4, and in particular PKT4 **437**. Consequently, when PKT4 **437** is destined to an address like IP A, i.e. IP~A, Dynamic UTC **410** advantageously allows PKT4 **437** to go through once after which Dynamic UTC **410** updates A Unknown **445** to include ~PKT4, so that when a subsequent packet like PKT4, i.e. ~PKT4 **460** is destined to wireless communication device **430A**, it is

blocked **435**. In an alternative embodiment, it is envisaged that the blocking operation allow for a predetermined number of packets matching a listing in IP A unknown before blocking subsequent packets.

[0027] In other alternative embodiments, wireless communication device **430A** can also send either an explicit or implicitly unblock to Dynamic UTC **410** at a later time so that Dynamic UTC **410** updates list IP A Unknown **445** to allow packets like PKT3, i.e. ~PKT4 **450. Thus,** when a packet like PKT, i.e. ~PKT4, is destined to wireless communication device **230A,** it is not blocked.

[0028] FIG. 5 shows an embodiment of an UTC **510** that combines the implicit aspect of the UTC **210** of FIG. 2 with the dynamic aspect of the UTC **410** of FIG. 4.

[0029] FIG. 6 shows an embodiment of an UTC **610** that combines the explicit aspect of UTC **310** of FIG. 3 with the dynamic aspect of the UTC **410** of FIG. 4.

[0030] FIGs. 7-8 shows an embodiment of an UTC **710** that combines the implicit aspect of the UTC **210** of FIG. 2 with the explicit aspect of UTC **310** of FIG. 3.

[0031] The lists utilized to categorize the various nature of packets in relation to a particular wireless device have thus far been kept separate in order to enable the reader to better understand their operation. However, as FIGs 2-8 demonstrate that introducing the appropriate lists into the UTC and following the appropriate procedures for updating those lists can combine various aspects of these UTCs, such as the implicit, explicit, and dynamic aspects. Therefore, for the remainder of this document and in the appended claims, the term rules will be used as a generic for the various lists utilized by a UTC to keep track of a wireless device, such as but not limited to the solicited, unsolicited, and unknown lists used thus far.

[0032] FIG. 9 is an interaction diagram illustrating the technique of delegating unsolicited traffic control, provided in accordance with the present application.

Turning to FIG. 9. initially, a UTC **910** does not contain any IP L rules **901** for wireless communication device **930L**, which as illustrated in FIG. 9 currently has address IP L. When PKT11 **903** arrives, UTC **910** sends PKT11 in a regulation message **905** to wireless device delegate **911** and at substantially the same time stores a copy of the packet in storage **920**, which was initially empty **903**. After receiving PKT11, wireless device delegate **950** forms PKT11 rule **906** and sends it back to UTC **910** in response to the regulation message **905**. UTC **910** updates the rules **960** for wireless communication device **930L** accordingly. If the rule for PKT11 is such that PKT11 **903** would be allowed to go through to wireless communication device **930L**, UTC **910** forwards **970** a copy of stored PKT11 to wireless communication device **930L**. Conversely if the rule for PKT11 is such that PKT11 **903** is not allowed to go to wireless communication device **930L**, then it is not forwarded. In the drawing, the conditional aspect of the forwarding **970** is illustrated by using a doted line to represent the message **970**.

[0033] FIG. 10 is a block diagram illustrating a wireless network including an embodiment of an unsolicited traffic controller, provided in accordance with the present application. Compared with FIG. 1, FIG. 10 further details wireless network **1000** showing the cooperation between UTC **1010** and an Authentication, Authorization and Accounting server AAA **1020**. AAA **1020** manages subscriber information wireless devices **130A-130N** as illustrated by records W A Data **1060A** through W N Data **1060N**. An example of AAA is a RADIUS server.

[0034] FIG 11 is an interaction diagram illustrating the UTC behaviour when a wireless communication device ceases operation, provided in accordance with the present application. Turning now to FIG. 11. A wireless communication device A **1130A** with identifier WA is assigned address J. A device profile **1120** is created in

AAA **1125**. When the address J assigned to the wireless communication device A is devolved **1140**, AAA sends a message that substantially indicates that device A data is inactive, such as Accounting Stop message **1150** to storing UTC **1110**. UTC **1110** identifies the UTC rules **1160** associated with wireless communication device **1130A** according to the identifier WA and address J assigned to that wireless communication device. UTC **1110** then stores **1170** the firewall rules associated with wireless communication device **1130A** to a storage device **1180** for later retrieval.

[0035] FIG 12 is an interaction diagram illustrating the UTC behaviour when a previously inactive wireless communication device becomes active again, provided in accordance with the present application. Turning to FIG. 12. initially the wireless communication device **1230A** with identifier WA has no address, and then is assigned **1240** address K. AAA **1225** sends a message that substantially indicates that device A data is active, such as Accounting Start message **1250,** to retrieving UTC **1210**. UTC **1210** retrieves **1270** the stored UTC rules **1290** for device A from the storage **1280** and updates UTC data **1295** with rules **1290** to apply to address K and starts functioning on behalf of wireless communication device **1230A** with address K.

[0036] FIG 13 is an interaction diagram illustrating the technique of UTC rule inversion when an address assigned to a wireless communication device is re-assigned to another wireless communication device, provided in accordance with the present application. Turning to FIG. 13. a wireless communication device A **1330A** with identifier WA initially is assigned address J. UTC **1310** holds the UTC rules **1360** on behalf of wireless communication device A **1330A**. As shown in the drawing, according to the rules currently in effect for WA, PKT12 is allowed to go through and reach wireless communication device A **1330A**. However, at a later time wireless communication device A **1330A** devolves address J back to the AAA **1320.** Upon

devolution of IP J **1340**, AAA **1320** sends a message that substantially indicates that device A data is inactive , such as Accounting Stop **1350**, to UTC **1310**. UTC **1310** inverts the IP J solicited rules **1325** portion of the UTC rules **1360**. Since this portion of the rules was related to wireless communication device A **1330A**, the inversion **1322** ensures that when wireless communication device **1330B** becomes active, and is assigned **1370** IP address J, even before AAA **1320** sends a message substantially indicating that wireless device B data is active, such as Accounting Start message **1380** to UTC **1310**, UTC **1310** advantageously blocks all packets which were considered solicited by wireless device A **1330A**. The inverted rules **1325I** thus ensure that, if wireless device A was using VPN through packet data network **1390** for example, and did not terminate VPN before devolution of IP J **1340**, no unsolicited packets, such as ~PKT12, left over from the stale VPN session will ever reach wireless device B **1330B**. Preferably, the inversion is temporary, for example clearing inverted rules **1325I** after all stale sessions would be known to have timed out, or replacing maintaining inverted rules **1325I** until UTC **1310** substitutes the inverted rules **1325I** with rules on behalf of wireless device B **1330B**, or until a predetermined timeout period has expired.

[0037] FIG. 14 is an interaction diagram illustrating the technique of inter-UTC hand-off, provided in accordance with the present application. Turning to FIG. 14 a wireless communication device A **1430** with identifier WA is using address S assigned by AAA **1420**. AAA **1420** sends a message that substantially indicates that device A data is inactive, such as Accounting Stop **1460**, to source UTC **1410Q**. IP S devolution **1450**, could be as a result of mobility, for example. A hand-off of WA Rules **1440** from UTC Q **1410Q** to UTC R **1410R** occurs.

[0038] Initially source UTC Q **1410Q** holds the WA Rules **1440** on behalf of wireless communication device A **1430**. After the hand-off, WA Rules **1440** are held at destination UTC R **1410R**.When AAA **1420** assigns IP T **1470** to wireless device **1430A**, AAA **1420** sends a message that substantially indicates that device A data is active, such as Accounting Start **1480**, to UTC R **1410R**. Advantageously, UTC R **1410R** already has WA Rules **1440** as a result of the hand-off, so wireless device WA **1430A** is never left unprotected by its WA Rules **1440**.

Although not expressly shown in the drawing, other mechanisms than the devolution and re-assignment of addresses may cause the hand off. For example AAA 1420 may issue hand off direction orders to UTCs.

[0039] FIG. 15 shows the GPRS embodiment described in the above paragraph in greater detail. Turning now to FIG. 15 and referring both to FIG. 1 and FIG. 15, the Public Land Mobile Network (PLMN) **1500** (a wireless network **100)** is the 3GPP network that receives the push data from the push initiator **1570** (which is in the packet data network **120** or **1520**) and ensures the delivery of push data to the push recipient (which is in at least one of wireless communication devices **130A-130N** or user equipments (UE) **1530A-1530N**. The delivery of the push data may involve other networks not explicitly shown in FIG. 1 or FIG. 15. The push function **1505** is the function in the PLMN **1500** that receives the push data from the push initiator **1570**. The push function is responsible for delivering the push data to the push recipient **1590A-1590N**. The packet data network **1520** is an interface into the PLMN **1500** via IP. User Equipment **1530A-1530N** is any one of the wireless communication devices **130A-130N**. Operationally, User Based Firewall (UBF) rules or Subscription-Based Firewall (SBF) rules (such as **140A-140N** or **1540A-1540N**) are persistently stored firewall rules based on the user or subscription rather than the session, and

enforced by unsolicited traffic controller **1510** or **110**. For example, a subscription-based rule will persist for a particular user or subscription across many IP (or other) sessions, whereas an IP based rule will persist for the duration of the IP session. A subscription may include more than one user, such as for example all users in a corporation. The user (or subscription) based firewall rules may be explicitly defined by the user, the operator, or implicitly defined by UE behaviour (for example, solicitation of a service). UE based list of firewall rules operate so as to appear substantially as if each interface had an apparent firewall **1550A-1550N (150A-150N)** protecting each user equipment's bearer path **1560A-1560N** linking wireless network **1500** or **100** with wireless communication devices **1530A-1530N (130A-130N)**. It is envisaged that the bearer path may include either or all of: sms, sip, circuit switched, packet switched, trunk service, wlan, broadcast, multicast or any other bearer required to provide a communication service such as voice, push to talk, wap, email, html, chat and the like. The push initiator **1570** is the entity that originates push data and submits it to the push function **1505** for delivery to a push recipient **1590A-1590N**. A push initiator may be for example an application providing value added services, such as email or other timely communications. A push user agent **1580A-1580N** is any software or device associated with a push recipient that interprets push data to the user of wireless communication devices **130A-130N**. This may include textual browsers, voice browsers, search engines, machine or device interface software, and other push user agents, for example. A push recipient is the entity that receives the push data from the Push function and processes or uses it. This is the UE with which the PLMN communicates with and bills to, the user agent with the application level address, and the device, machine or person that uses the push data. An individual user or subscription controls a push recipient. A push subscription profile (PSP) **1595** for

each user or subscriber is preferably accessible to the user based firewall (UBF) integral to unsolicited traffic controller **1510** or **110.** The PSP is a set of parameters indicating the push recipient's settings and preferences for the push service. This may include an override capability for the wireless carrier to implement a standard set of UBF rules for all Push Recipients (subscribers). For example, this would allow for all users to get WAP push by default without the capability to block it. A similar example is for Broadcast/multicast service.

[0040] FIG. 16 shows an exemplary embodiment of an unsolicited traffic controller apparatus, provided in accordance with the present application. Packet data network **1610** sends unsolicited traffic destined to wireless communication device. Unsolicited traffic controller **1600** intercepts all traffic sent by packet data network **1610** that is destined for wireless communication device 1620, or other like devices for whom it is delegated authority to control unsolicited traffic. Unsolicited traffic controller **1600** includes a packet data network interface **1640** to receive packets from packet data network, as well as a wireless data network interface **1660** to send packets to the wireless communication device **1620**.

[0041] Operationally, unsolicited traffic control module **1650** applies rules **1670** on behalf of wireless communication device **1620** to selectively block packets from being sent over wireless data network interface **1660** to wireless communication device **1620** thereby providing an apparent firewall **1630** that substantially prevents packets which are considered unsolicited by wireless communication device **1620** from ever reaching the wireless communication device **1620**.

[0042] In alternate embodiments, the interfaces **1640** and **1660** may be one way so that they can only receive and transmit respectively, or can be two-way allowing packets to be both transmitted and received.

[0043] The embodiments described herein are examples of structures, systems or methods having elements corresponding to elements of this application. This written description may enable those skilled in the art to make and use embodiments having alternative elements that likewise correspond to the elements of this a. The intended scope of the application thus includes other structures, systems or methods that do not differ from the invention as described herein, and further includes other structures, systems or methods with insubstantial differences from the invention as described herein.

CLAIMS:

1. In a wireless communication network, said wireless communications network comprising an unsolicited traffic controller (UTC) coupled to a packet data network and a plurality of wireless communication devices, a method of controlling traffic destined to a first one of said plurality of wireless communication devices comprising the steps of:

storing a set of traffic control rules associated with said first one of said plurality of wireless communication devices;

determining a subscription identity corresponding to a user of said first one of said plurality of wireless communication devices;

determining that a first packet received from said packet data network is destined to said first one of said plurality of wireless communication devices;

selecting said stored traffic control rules associated with said determined subscription identity;

applying said selected traffic control rules to determine if said first packet is unsolicited by said user; and

preventing said first packet from being sent to said first one of said plurality of communication devices if said first packet is determined to be unsolicited,

wherein said traffic includes Internet Protocol traffic,

and wherein said set of traffic control rules correspond to said subscription identity,

and wherein said subscription identity persists across multiple Internet Protocol sessions of said user.

2. The method as recited in claim 1, wherein said wireless communication network is a CDMA wireless network and wherein said UTC is located in at least one PDSN.

3. The method as recited in claim 1, wherein said wireless communication network is a GPRS wireless network and wherein said UTC is located in one of a SGSN and GGSN.

4. The method as recited in claim 1, wherein said set of traffic control rules is implicit, explicit, dynamic or a combination thereof.

5. The method as recited in claim 4, wherein if said traffic control rule is implicit, said UTC, in response to solicited traffic by said first one of said plurality of wireless communication devices, updates a list of said solicited traffic and, upon reception of traffic substantially similar to said solicited traffic from said packet data network, releases said substantially similar traffic to said first one of said plurality of wireless communication devices.

6. The method as recited in claim 4, wherein if said traffic control rule is explicit, said UTC, in response to a message received from said first one of said plurality of wireless communication devices regarding a specified type of traffic, updates a list to include said specified type of traffic, and blocks said specified type of traffic if received from said packet data network.

7. The method as recited in claim 4, wherein if said traffic control rule is dynamic, upon a first reception of a specified type of traffic from said packet data network, releases said specified type of traffic to said first one of said plurality of wireless communication devices and updates a list with said specified type of traffic, and wherein upon a second reception of traffic substantially similar to said specified type of traffic, blocks said substantially similar traffic.

8. The method as recited in claim 1, wherein said subscription identity includes one of IMSI, NAI, MSISDN, and SIP url.

9. The method as recited in claim 1, wherein said first packet comprises at least one of Internet Protocol, voice, email, hyper text transfer protocol, file transfer protocol, multimedia messaging service, and short messaging service.

10. The method as recited in claim 1, wherein said UTC is a delegating UTC and wherein said method further comprises the steps of:

sending said first packet in a regulation message to a delegate to regulate said first packet on behalf of said first one of said plurality of communication devices;

storing said first packet in a said delegating UTC;

receiving in said delegating UTC a rule from said delegate; and

updating said stored set of traffic control rules with said received rule.

11. The method as recited in claim 1, wherein said wireless communication network further comprises a server communicating with said UTC, and wherein said method further comprises the steps of:

creating a device profile associated with said first one of said plurality of wireless communication devices in said server;

devolving a first IP address associated with said first one of said plurality of wireless communication devices and sending a stop message from said server to said UTC when said first one of said plurality of wireless communication devices becomes inactive;

identifying said stored set of traffic control rules associated with said first one of said plurality of wireless communication devices; and

storing said identified set of traffic control rules in a storage device for later retrieval.

12. The method as recited in claim 11 further comprising the steps of:

assigning a second IP address to said user of said first one of said plurality of wireless communication devices;

sending a start message from said server to said UTC when said first one of said plurality of wireless communication devices becomes active;

retrieving said stored set of traffic control rules from said storage device; and

associating said retrieved rules with said second IP address.

13. The method as recited in claim 11 further comprising the steps of:

assigning said devolved first IP address to a second one of said plurality of wireless communication devices;

inverting said identified set of traffic rules associated with said first IP address;

sending a start message from said server to said UTC when said second one of said plurality of wireless communication devices becomes active; and

applying said inverted set of traffic control rules to said second one of said plurality of wireless communication devices.

14. The method as recited in claim 11, wherein said UTC is a source UTC, and wherein said method further comprises the steps of:

devolving said first IP address and sending an accounting stop message from said server to said source UTC indicating that said first one of said plurality of wireless communication devices has become inactive;

transferring said identified set of traffic control rules to a destination UTC;

assigning a second IP address corresponding to said user of said first one of said plurality of wireless communication devices;

sending a start message from said server to said destination UTC indicating that said first one of said plurality of wireless communication devices has become active; and

applying said transferred set of traffic control rules to said first one of said plurality of wireless communication devices.

15. A computer readable medium having stored thereon, computer executable instructions which when executed by a processor in an unsolicited traffic controller (UTC), cause said UTC to:

store a set of traffic control rules associated with a specified one of a plurality of wireless communication devices;

determine an identity corresponding to a user of said specified one of said plurality of wireless communication devices;

determine that a first packet received from a packet data network is destined to said specified one of said plurality of wireless communication devices;

select said stored set of traffic control rules associated with said determined subscription identity;

apply said selected traffic control rules to determine if said first packet is unsolicited by said user; and

prevent said first packet from being sent to said specified one of said plurality of communication devices if said first packet is determined to be unsolicited,

wherein said UTC is resident in a wireless communications network and coupled to said packet data network and said plurality of wireless communication devices,

wherein said traffic includes Internet Protocol traffic,

and wherein said set traffic control rules correspond to said subscription identity,

and wherein said subscription identity persists across multiple Internet Protocol sessions of said user.

16. In a wireless communication network, said wireless communications network comprising an unsolicited traffic controller (UTC) coupled to a packet data network and a plurality of wireless communication devices, a method of controlling traffic destined to a specified one of said plurality of wireless communication devices comprising:

step for storing a set of traffic control rules associated with said specified one of said plurality of wireless communication devices;

step for determining a subscription identify corresponding to a user of said specified one of said plurality of wireless communication devices;

step for determining in said UTC that a first packet received from said packet data network is destined to said specified one of said plurality of wireless communication devices;

step for selecting said stored traffic control rules associated with said determined subscription identify;

step for applying said stored traffic control rules to determine if said first packet is unsolicited by said user; and

step for preventing said first packet from being sent to said specified one of said plurality of communication devices if said first packet is determined to be unsolicited,

wherein said traffic includes Internet Protocol traffic,

and wherein said set of traffic control rules correspond to said subscription identity,

and wherein said subscription identity persists across multiple Internet Protocol sessions of said user.

17. In a wireless communication network, said wireless communications network comprising an unsolicited traffic controller (UTC) coupled to a push initiator and a plurality of push recipients, a method of controlling push data transferred to a push function for delivery to said plurality of push recipients comprising the steps of:

storing subscription based firewall (SBF) rules associated with a specified group of said plurality of push recipients, wherein said SBF rules are based on a subscription identity which persist across multiple Internet Protocol sessions of said specified group;

determining that push data received from said push initiator is destined for said specified group;

selecting said SBF rules,

applying said SBF rules to determine if said push data is unsolicited by said specified group, and

preventing said push data from being sent to said specified group, if said push data is determined to be unsolicited,

wherein said push data includes Internet Protocol traffic,

and wherein said SBF rules correspond to said subscription identity.

18. The method of claim 17 wherein said push initiator is a packet data network.

19. The method of claim 18 wherein said plurality of push recipients are respective wireless communication devices.

20. The method of claim 19 wherein the wireless communication network is a public land mobile network.

21. The method of claim 19 wherein each of said plurality of push recipients comprise a push user agent taken from the group comprising a text browser, a voice browser and a search engine.

22. The method of claim 19 wherein each of said plurality of push recipients is controlled by a push subscription profile (PSP) accessible by said UTC, and wherein said PSP defines a specified type of push data that can be received from said push initiator.

23. The method of claim 17 wherein said UTC is linked to said push recipient along a bearer path, and wherein said bearer path is taken from the group comprising an sms, sip, circuit switched, packet switched, trunk service, wlan, broadcast and multicast path.

24. In a wireless communication network, an apparatus for controlling unsolicited traffic destined to a specified one of a plurality wireless communication devices, the apparatus comprising:

a first interface configured to receive traffic from a packet data network;

a second interface configured to send traffic to said specified one of said plurality of wireless communication devices;

a first storage medium having stored thereon computer executable instructions representing a set of traffic control rules; and

an unsolicited traffic controller (UTC) communicating with said first and second interfaces and said first storage medium, wherein said UTC determines a subscription identity assigned to said specified one of said plurality of wireless communication devices, and executes said computer executable instructions to selectively block said unsolicited traffic received over said first interface from being sent over said second interface to said specified one of said plurality wireless communication devices,

wherein said traffic includes Internet Protocol Traffic;

and wherein said set of traffic control rules correspond to said subscription identity;

and wherein said subscription identity persists across multiple Internet Protocol sessions of said user.

25. The apparatus as recited in claim 24, wherein said wireless communication network is a GPRS wireless network and said UTC is located in one of a SGSN and GGSN.

26. The apparatus as recited in claim 24, wherein said wireless communication network is a CDMA wireless network and wherein said UTC is located in at least one PDSN.

27. The apparatus as recited in claim 24, wherein said set of traffic control rules is implicit, explicit, dynamic or a combination thereof.

28. The apparatus as recited in claim 24, wherein said subscription identity includes one of IMSI, NAI, MSISDN, and SIP url.

29. The apparatus as recited in claim 24, wherein said traffic comprises at least one of Internet Protocol, voice, email, hyper text transfer protocol, file transfer protocol, multimedia messaging service, and short messaging service.

30. The apparatus as recited in claim 24 further comprising a delegate communicating with said UTC for regulating said first packet on behalf of said specified one of said plurality of communication devices.

31. The apparatus of claim 24 further comprising a server communicating with said UTC for managing subscriber information associated with respective ones of said plurality of wireless communication devices.

32. The apparatus as recited in claim 31, further comprising a second storage medium communicating with said UTC for storing said set of traffic control rules when said specified one of said plurality of wireless communication devices becomes inactive.

33. In a wireless communication network, an apparatus for controlling unsolicited traffic destined to a specified one of a plurality of wireless communication devices, the apparatus comprising:

an unsolicited traffic controller (UTC) comprising a subscription based firewall (SBF) having subscription based firewall rules associated therewith, wherein said SBF rules persist across multiple Internet Protocol sessions;

a push initiator comprising a packet data network communicating with said UTC;

a push recipient comprising at least one wireless communication device communicating with said UTC,

wherein push data received by said UTC from said push initiator has applied thereto said SBF rules to determine if said push data is unsolicited;

and wherein said push data includes Internet Protocol push data;

and wherein said subscription based firewall rules correspond to a subscription identity.

34. In a wireless communication network, an apparatus for controlling unsolicited traffic destined to a specified one of a plurality of wireless communication devices, the apparatus comprising:

means for receiving traffic from a packet data network;

means for sending traffic to said specified one of said plurality of wireless communication devices;

means for storing computer executable instructions representing a set of traffic control rules, wherein said traffic control rules persist across multiple Internet Protocol sessions; and

means for executing said computer executable instructions to selectively block traffic received from said packet data network and destined for said specified one of said plurality wireless communication devices;

wherein said means for executing communicates with said means for receiving, said means for sending and said means for storing;

and wherein said traffic includes Internet Protocol push data;

and wherein said traffic control rules correspond to a subscription identity.

35. In a wireless communication network, said wireless communication network comprising an unsolicited traffic controller (UTC) coupled to a packet data network and a plurality of wireless communication devices, a method of controlling traffic destined to a first wireless communication device of said plurality of wireless communication devices, the method comprising the steps of:

storing a set of traffic control rules associated with said first wireless communication device;

determining a first identity corresponding to a user of said first wireless communication device;

in response to one of: an incoming packet flowing from said packet data network and destined for said first wireless communication device; and an outgoing packet flowing from said first wireless communication device and destined for said packet data network, selecting said stored traffic control rules associated with said determined first identity and updating automatically said selected traffic control rules;

determining that a subsequent packet received from said packet data network is destined to said first wireless communication device;

applying said selected traffic control rules to determine if said subsequent packet is unsolicited by said user; and

preventing said subsequent packet from being sent to said first wireless communication device if said subsequent packet is determined to be unsolicited.

36. The method as recited in claim 35, wherein said wireless communication network is a CDMA wireless network and wherein said UTC is located in at least one PDSN.

37. The method as recited in claim 35, wherein said wireless communication network is a GPRS wireless network and wherein said UTC is located in one of a SGSN and GGSN.

38. The method as recited in claim 35, wherein said set of traffic control rules is implicit, explicit, dynamic or a combination thereof.

39. The method as recited in claim 35, wherein said selected traffic control rules comprise implicit traffic control rules, wherein in response to said outgoing packet flowing from said first wireless communication device and destined for said packet data network, updating automatically said selected traffic control rules comprises updating a list of solicited traffic in said implicit traffic control rules with a definition of traffic substantially similar to said outgoing packet, and wherein the method further comprises:

applying said selected traffic control rules to determine if said subsequent packet is solicited by said user by determining with use of said definition if said subsequent packet is substantially similar to said outgoing packet; and

releasing said subsequent packet to said first wireless communication device if said subsequent packet is determined to be solicited.

40. The method as recited in claim 35, wherein said selected traffic control rules comprise explicit traffic control rules, wherein in response to said incoming packet flowing from said packet data network and destined for said first wireless communication device, updating automatically said selected traffic control rules comprises:

releasing said incoming packet to said first wireless communication device;

sending from said first wireless communication device to said UTC a message regarding said incoming packet; and

with use of said message updating a list of unsolicited traffic in said explicit traffic control rules with a definition of traffic substantially similar to said incoming packet,

wherein applying said selected traffic control rules to determine if said subsequent packet is unsolicited by said user comprises determining with use of said definition if said subsequent packet is substantially similar to said incoming packet.

41. The method as recited in claim 35, wherein said selected traffic control rules comprise dynamic traffic control rules, wherein in response to said incoming packet flowing from said packet data network and destined for said first wireless communication device, updating automatically said selected traffic control rules comprises:

releasing said incoming packet to said first wireless communication device; and

updating a list of unknown traffic in said dynamic traffic control rules with a definition of traffic substantially similar to said incoming packet,

wherein applying said selected traffic control rules to determine if said subsequent packet is unsolicited by said user comprises determining with use of said definition if said subsequent packet is substantially similar to said incoming packet.

42. The method as recited in claim 35, wherein said first identity is selected from a group consisting of: IMSI, NAI, MSIDSN, and SIP url.

43. The method as recited in claim 35, wherein said incoming packet and said outgoing packet are selected from a group comprising Internet Protocol, voice, email, hyper text transfer protocol, file transfer protocol, multimedia messaging service, and short messaging service.

44. The method as recited in claim 35, wherein said UTC is a delegating UTC and wherein in response to said incoming packet flowing from said packet data network and destined for said first wireless communication device, updating automatically said selected traffic control rules comprises:

sending said incoming packet in a regulation message to a delegate to regulate said incoming packet on behalf of said first wireless communication device;

storing said incoming packet in said delegating UTC;

receiving in said delegating UTC a rule from said delegate; and

updating said selected traffic control rules with said received rule.

45. The method as recited in claim 35, wherein said wireless communication network further comprises an authentication, authorization and accounting (AAA) server communicating with said UTC, and wherein said method further comprises the steps of:

creating a profile associated with said first wireless communication device in said AAA;

devolving said first identity and sending an accounting stop message from said AAA to said UTC when said first wireless communication device becomes inactive;

identifying said stored set of traffic control rules associated with said first wireless communication device; and

storing said identified set of traffic control rules in a storage device for later retrieval.

46. The method as recited in claim 45 further comprising the steps of:

assigning a second identity corresponding to said user of said first wireless communication device;

sending an accounting start message from said AAA to said UTC when said first wireless communication device becomes active;

retrieving said stored set of traffic control rules from said storage device; and

associating said retrieved rules with said second identity.

47. The method as recited in claim 45 further comprising the steps of:

assigning said devolved first identity to a second wireless communication device of said plurality of wireless communication devices;

inverting said identified set of traffic control rules associated with said first identity;

sending an accounting start message from said AAA to said UTC when said second wireless communication device becomes active; and

applying said inverted set of traffic control rules to said second wireless communication device.

48. The method as recited in claim 45, wherein said UTC is a source UTC, and wherein said method further comprises the steps of:

devolving said first identity and sending an accounting stop message from said AAA to said source UTC indicating that said first wireless communication device has become inactive;

transferring said identified set of traffic control rules to a destination UTC;

assigning a second identity corresponding to said user of said first wireless communication device;

sending an accounting start message from said AAA to said destination UTC indicating that said first wireless communication device has become active; and

applying said transferred set of traffic control rules to said first wireless communication device.

49. A computer readable medium having stored thereon, computer executable instructions which when executed by a processor in an unsolicited traffic controller (UTC), cause said UTC to:

store a set of traffic control rules associated with a specified wireless communication device of a plurality of wireless communication devices;

determine an identity corresponding to a user of said specified wireless communication device;

in response to one of: an incoming packet flowing from a packet data network and destined for said specified wireless communication device; and an outgoing packet flowing from said specified wireless communication device and destined for said packet data network, select said stored traffic control rules associated with said determined identity and update automatically said selected traffic control rules;

determine that a subsequent packet received from a packet data network is destined to said specified wireless communication device;

apply said selected traffic control rules to determine if said subsequent packet is unsolicited by said user; and

prevent said subsequent packet from being sent to said specified wireless communication device if said subsequent packet is determined to be unsolicited,

wherein said UTC is resident in a wireless communication network and coupled to said packet data network and said plurality of wireless communication devices.

50. In a wireless communication network, said wireless communication network comprising an unsolicited traffic controller (UTC) coupled to a packet data network and a plurality of wireless communication devices, a method of controlling traffic destined to a specified wireless communication device of said plurality of wireless communication devices, the method comprising:

storing a set of traffic control rules associated with said specified wireless communication device;

determining an identity corresponding to a user of said specified wireless communication device;

in response to one of: an incoming packet flowing from a packet data network and destined for said specified wireless communication device; and an outgoing packet flowing from said specified wireless communication device and destined for said packet data network, selecting said stored traffic control rules associated with said determined identity and updating automatically said selected traffic control rules;

determining in said UTC that a subsequent packet received from said packet data network is destined to said specified wireless communication device;

applying said stored traffic control rules to determine if said subsequent packet is unsolicited by said user; and

preventing said first packet from being sent to said specified wireless communication device if said subsequent packet is determined to be unsolicited.

51. In a wireless communication network, said wireless communication network comprising an unsolicited traffic controller (UTC) coupled to a push initiator and a plurality of push recipients, a method of controlling push data transferred to a push function for delivery to said plurality of push recipients comprising the steps of:

storing subscription based firewall (SBF) rules associated with a specified group of push recipients of said plurality of push recipients, wherein said SBF rules are persistently stored rules based on a subscription;

in response to one of: push data received from said push initiator and destined for said specified group of push recipients; and data from said specified group of push recipients and destined for said push initiator, selecting said SBF rules and updating automatically said SBF rules;

determining that subsequent push data received from said push initiator is destined for said specified group of push recipients;

applying said selected SBF rules to determine if said subsequent push data is unsolicited by said specified group of push recipients;

preventing said subsequent push data from being sent to said specified group of push recipients, if said subsequent push data is determined to be unsolicited.

52. The method of claim 51 wherein said push initiator is a packet data network.

53. The method of claim 52 wherein said plurality of push recipients are respective wireless communication devices.

54. The method of claim 53 wherein the wireless communication network is a public land mobile network.

55. The method of claim 53 wherein each of said plurality of push recipients comprise a push user agent taken from the group comprising a text browser, a voice browser and a search engine.

56. The method of claim 53 wherein each of said plurality of push recipients is controlled by a push subscription profile (PSP) accessible by said UTC, and wherein said PSP defines a specified type of push data that can be received from said push initiator.

57. The method of claim 51 wherein said UTC is linked to said push recipient along a bearer path, and wherein said bearer path is taken from the group comprising an sms, sip, circuit switched, packet switched, trunk service, wlan, broadcast and multicast path.

58. In a wireless communication network, an apparatus for controlling unsolicited traffic destined to a specified wireless communication device of a plurality of wireless communication devices, the apparatus comprising:

a first interface configured to receive traffic from a packet data network;

a second interface configured to send traffic to said specified wireless communication device;

a first storage medium having stored thereon computer executable instructions representing a set of traffic control rules; and

an unsolicited traffic controller (UTC) communicating with said first and second interfaces and said first storage medium, wherein said UTC:

determines an identity assigned to said specified wireless communication device;

in response to one of: an incoming packet flowing from a packet data network and destined for said specified wireless communication device; and an outgoing packet flowing from said specified wireless communication device and destined for said packet data network, selects, of said set of traffic control rules, traffic control rules associated with said determined identity and updates automatically said selected traffic control rules;

determines that a subsequent packet received over said first interface from said packet data network is destined to said specified wireless communication device; and

executes said computer executable instructions to apply said selected traffic control rules to determine if said subsequent packet is unsolicited traffic and to selectively block said unsolicited traffic received over said first interface from being sent over said second interface to said specified wireless communication device.

59. The apparatus as recited in claim 58, wherein said wireless communication network is a GPRS wireless network and said UTC is located in one of a SGSN and GGSN.

60. The apparatus as recited in claim 58, wherein said wireless communication network is a CDMA wireless network and wherein said UTC is located in at least one PDSN.

61. The apparatus as recited in claim 58, wherein said set of traffic control rules is implicit, explicit, dynamic or a combination thereof.

62. The apparatus as recited in claim 58, wherein said identity is selected from a group consisting of: IMSI, NAI, MSISDN, and SIP url.

63. The apparatus as recited in claim 58, wherein said traffic is selected from a group comprising Internet Protocol, voice, email, hyper text transfer protocol, file transfer protocol, multimedia messaging service, and short messaging service.

64. The apparatus as recited in claim 58 further comprising a delegate communicating with said UTC for regulating said subsequent packet on behalf of said specified wireless communication device.

65. The apparatus of claim 58 further comprising an authentication, authorization and accounting (AAA) server communicating with said UTC for managing subscriber information associated with respective ones of said plurality of wireless communication devices.

66. The apparatus as recited in claim 65, further comprising a second storage medium communicating with said UTC for storing said set of traffic control rules when said specified wireless communication device becomes inactive.

67. In a wireless communication network, an apparatus for controlling unsolicited traffic destined to a specified wireless communication device of a plurality of wireless communication devices, the apparatus comprising:

an unsolicited traffic controller (UTC) comprising a subscription based firewall (SBF) having subscription based firewall rules associated therewith;

a push initiator comprising a packet data network communicating with said UTC; and

a push recipient comprising at least one wireless communication device communicating with said UTC,

wherein in response to one of: push data received from said push initiator and destined for said push recipient; and outgoing data from said push recipient and destined for said push initiator, said UTC selects said SBF rules, and automatically updates said SBF rules, wherein subsequent push data received by said UTC from said push initiator has applied thereto said SBF rules to determine if said push data is unsolicited.

68. In a wireless communication network, an apparatus for controlling unsolicited traffic destined to a specified wireless communication device of a plurality of wireless communication devices, the apparatus comprising:

means for receiving traffic from a packet data network;

means for sending traffic to said specified wireless communication device;

means for storing computer executable instructions representing a set of traffic control rules;

means for determining an identity assigned to said specified wireless communication device;

means for, in response to one of: an incoming packet flowing from a packet data network and destined for said specified wireless communication device; and an outgoing packet flowing from said specified wireless communication device and destined for said packet data network, selecting, of said set of traffic control rules, traffic control rules associated with said determined identity and automatically updating said selected traffic control rules;

means for determining that a subsequent packet received from said packet data network is destined to said specified wireless communication device; and

means for executing said computer executable instructions to apply said selected traffic control rules to determine if said subsequent packet is unsolicited traffic; and to selectively block traffic received from said packet data network and destined for said specified one of said plurality wireless communication devices, wherein said means for executing communicates with said means for receiving, said means for sending and said means for storing.

69. A method for controlling unsolicited traffic between a wireless communication device and a packet data network, the method comprising:

detecting an incoming data packet destined to the wireless communication device from the packet data network or an originating data packet originating from the wireless communication device destined to the packet data network;

automatically updating a set of traffic control rules associated with the wireless communication device in response to detection of the incoming data packet or in response to detection of the originating data packet;

applying the updated set of traffic control rules to subsequent incoming data packets destined to the wireless communication device from the packet data network to identify solicited or unsolicited incoming data packets; and

blocking transmission of the unsolicited incoming data packets destined to the wireless communication device from the packet data network.

70. The method of claim 69, wherein automatically updating the set of traffic control rules comprises updating a list of solicited traffic, in response to detection of the originating data packet, to include a solicited traffic definition of traffic substantially similar to the originating data packet; and

wherein applying the updated set of traffic control rules to subsequent incoming data packet comprises determining whether the subsequent data packet is solicited based on a comparison with the solicited traffic definition in the list of solicited traffic; and

transmitting the subsequent incoming data packet to the wireless communication device if the subsequent packet is determined to be solicited.

71. The method of claim 70, wherein the solicited traffic definition is at least one of an Internet Protocol (IP) address, a port number, and a socket number.

72. The method of claim 69, wherein in response to detection of the incoming data packet destined to the wireless communication device from the packet data network, transmitting the incoming data packet to the wireless communication device; and

wherein automatically updating the set of traffic control rules comprises updating a list of unsolicited traffic, in response to an explicit message from the wireless communication device, to include a unsolicited traffic definition of traffic substantially similar to the incoming data packet; and

wherein applying the updated set of traffic control rules to subsequent incoming data packet comprises determining whether the subsequent data packet is unsolicited based on a comparison with the unsolicited traffic definition in the list of unsolicited traffic; and

blocking transmission of the subsequent incoming data packet to the wireless communication device if the subsequent packet is determined to be unsolicited.

73. The method of claim 72, wherein the unsolicited traffic control definition is at least one of a IP address, a port number, and a socket number.

74. The method of claim 69, wherein in response to detection of the incoming data packet destined to the wireless communication device from the packet data network, transmitting the incoming data packet to the wireless communication device; and

wherein automatically updating the set of traffic control rules comprises updating a list of unknown traffic to include a unknown traffic definition of traffic substantially similar to the incoming data packet; and

wherein applying the updated set of traffic control rules to subsequent incoming data packet comprises determining whether the subsequent data packet is unsolicited based on a comparison with the list of unknown traffic; and

blocking transmission of the subsequent incoming data packet to the wireless communication device if the subsequent packet is determined to be unsolicited.

75. The method of claim 74, wherein the unknown traffic control definition is at least one of a IP address, a port number, and a socket number.

76. The method of claim 74, further comprising:

automatically updating a list of solicited traffic in the set of traffic control rules, in response to detection of a subsequent originating data packet substantially similar to the incoming data packet, to include a solicited traffic definition corresponding to the unknown traffic definition; and

automatically clearing the unknown traffic definition from the list of unknown traffic.

77. The method of claim 74, further comprising:

automatically updating a list of unsolicited traffic in the set of traffic control rules, in response to an explicit message from the wireless communication device, to include a unsolicited traffic definition corresponding to the unknown traffic definition; and

automatically clearing the unknown traffic definition from the list of unknown traffic.

78. The method of claim 69, wherein in response to detection of the incoming data packet destined to the wireless communication device from the packet data network, automatically updating the set of traffic control rules comprises:

sending the incoming data packet to a delegate of the wireless communication device to regulate the incoming data packet on behalf of the wireless communication device;

storing the incoming data packet in a store;

automatically updating the traffic control rules based on a rule from the delegate;

applying the updated set of traffic control rules to the stored incoming data packet to

determine whether the stored incoming data packet is solicited or unsolicited based on the rule from the delegate.

79. The method of claim 69, further comprising:

associating the traffic control rules to a first identity of the wireless communication device;

creating a profile associated with the wireless communication device including the first identity of the wireless communication device in a authentication, authorization, and accounting (AAA) server;

devolving the first identity of the wireless communication device and sending an accounting stop message from the AAA server when the wireless communication device becomes inactive; and

storing the traffic control rules associated with the first identity of the wireless communication device in a storage device in the AAA server for later retrieval.

80. The method of claim 79, further comprising:

assigning a second identity to the wireless communication device;

sending an accounting start message from the AAA server when the wireless communication device becomes active;

retrieving the stored traffic control rules associated with the first identity of the wireless communication device based on the profile associated with the wireless communication device; and

associating the retrieved traffic control rules with the second identity of the wireless communication device.

81. The method of claim 79, further comprising:

assigning the devolved first identity to a second wireless communication device;

inverting the stored set of traffic control rules associated with first identity of the wireless communication device;

sending an accounting start message from the AAA server when the second wireless communication device becomes active; and

associating the inverted traffic control rules with the second wireless communication device.

82. The method of claim 81, wherein the first identity and second identity are at least one of International Mobile Station Identity (IMSI), Network Access Identifier (NAI), Mobile Station Internet Services Digital Network Number (MSISDN), and Session Initiation Protocol (SIP) Universal Resource Locator (url).

83. The method of claim 69, wherein the incoming data packet and the originating data packet are at least one of Internet Protocol, voice, email, hyper text transfer protocol, file transfer protocol, multimedia messaging service, and short messaging service.

84. An unsolicited traffic controller (UTC) for controlling unsolicited traffic between a wireless communication device and a packet data network, the UTC comprising:

a packet data network interface for receiving incoming data packets from the packet data network destined to the wireless communication device and for transmitting originating data packets originating from the wireless communication device destined to the packet data network;

a wireless data network interface for transmitting incoming data packets destined to the wireless communication device from the packet data network and for receiving originating data packets originating from the wireless communication device destined to the packet data network;

an unsolicited traffic control module for detecting the incoming data packet and the originating data packet;

the unsolicited traffic control module automatically updating a set of traffic control rules associated with the wireless communication device in response to detection of the incoming data packet or in response to detection of the originating data packet; applying the updated set of traffic control rules to subsequent incoming data packets destined to the

wireless communication device from the packet data network to identify solicited or unsolicited incoming data packets; and

blocking transmission of the unsolicited incoming data packets destined to the wireless communication device from the packet data network.

85. A wireless communication system comprising:

a wireless communication network including a wireless communication device, a packet data network, and a unsolicited traffic controller (UTC) for controlling unsolicited traffic between the wireless communication device and the packet data network, the UTC comprising:

a packet data network interface for receiving incoming data packets from the packet data network destined to the wireless communication device and for transmitting originating data packets originating from the wireless communication device destined to the packet data network;

a wireless data network interface for transmitting incoming data packets destined to the wireless communication device from the packet data network and for receiving originating data packets originating from the wireless communication device destined to the packet data network;

an unsolicited traffic control module for detecting the incoming data packet and the originating data packet;

the unsolicited traffic control module automatically updating a set of traffic control rules associated with the wireless communication device in response to detection of the incoming data packet or in response to detection of the originating data packet; applying the updated set of traffic control rules to subsequent incoming data packets destined to the wireless communication device from the packet data network to identify solicited or unsolicited incoming data packets; and blocking transmission of the unsolicited incoming data packets destined to the wireless communication device from the packet data network.

86. The wireless communication system of claim 85, wherein the wireless communication network is a Code Division Multiple Access (CDMA) wireless network and wherein the UTC is located in at least one Packet Data Servicing Node (PDSN).

87. The wireless communication system of claim 85, wherein the wireless communication network is a General Packet Radio Service (GPRS) wireless network and wherein the UTC is located in one of a Serving GPRS Support Node (SGSN) and Gateway GPRS Support Node (GGSN).

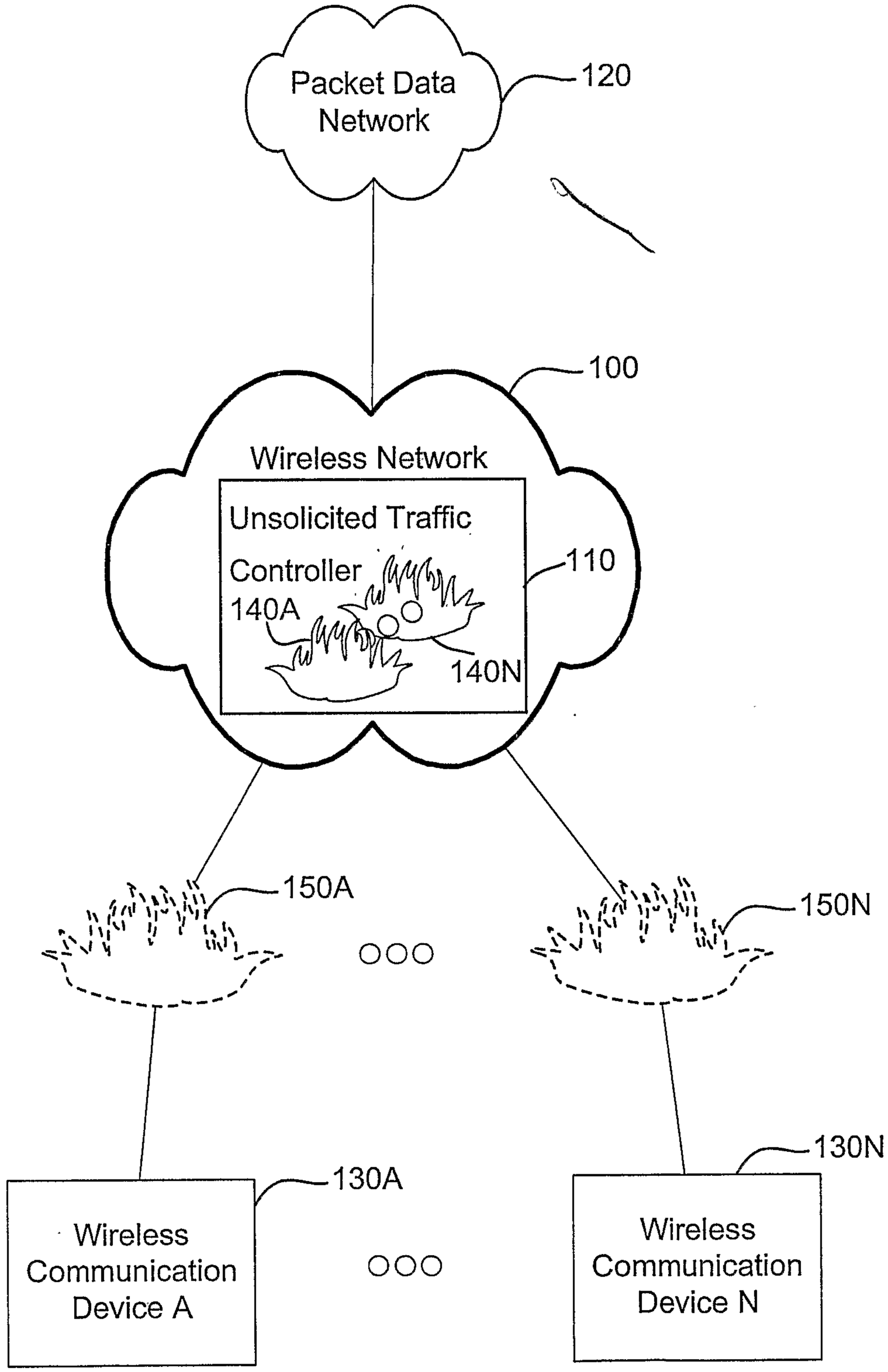

Packet Data Network
120
100
Wireless Network
Unsolicited Traffic Controller
110
140A
140N
150A
150N
130A
130N
Wireless Communication Device A
Wireless Communication Device N

FIG. 1

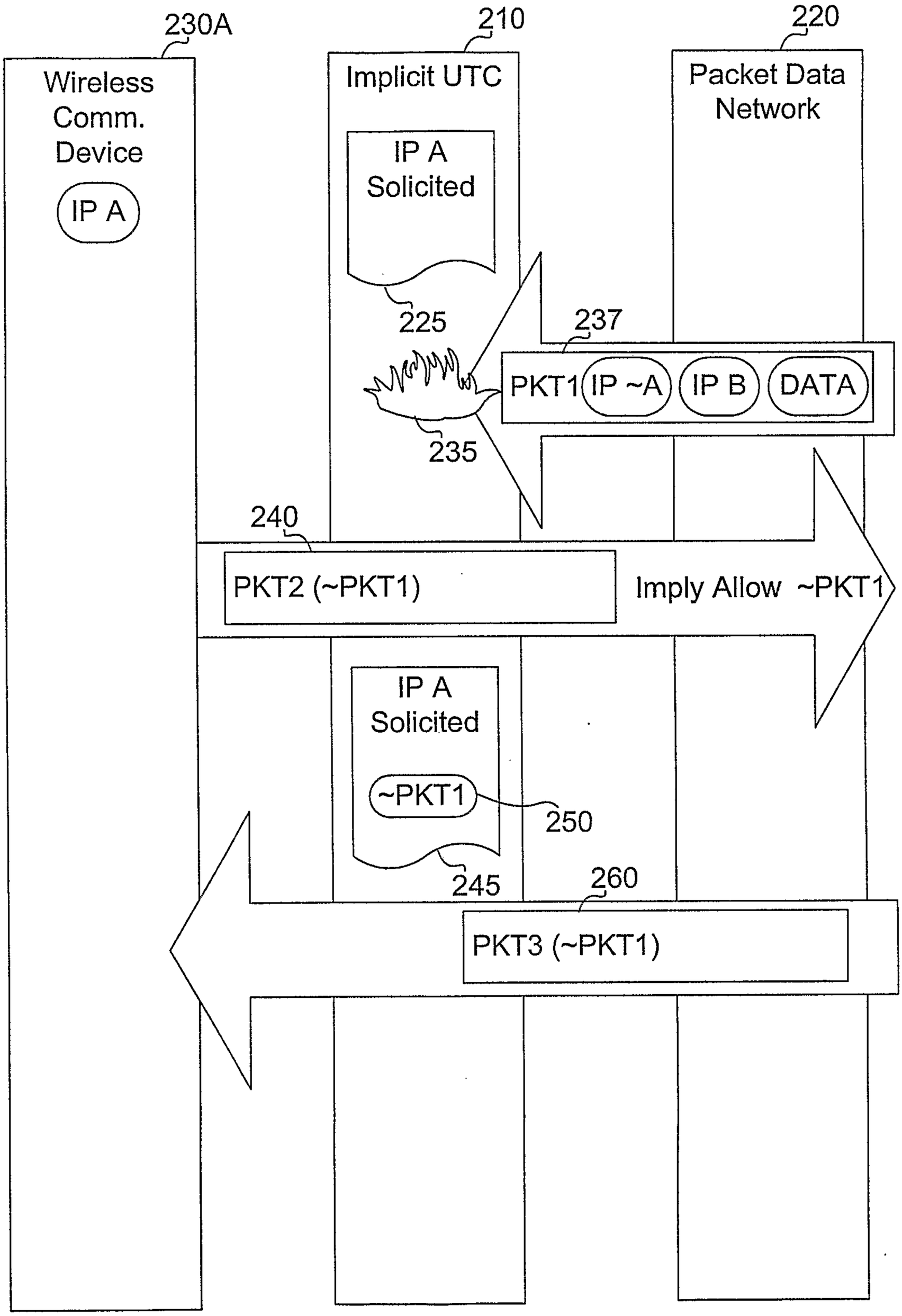

230A
Wireless Comm. Device
IP A
210
Implicit UTC
IP A Solicited
225
235
220
Packet Data Network
237
PKT1
IP ~A
IP B
DATA
240
PKT2 (~PKT1)
Imply Allow ~PKT1
IP A Solicited
~PKT1
250
245
260
PKT3 (~PKT1)

FIG. 2

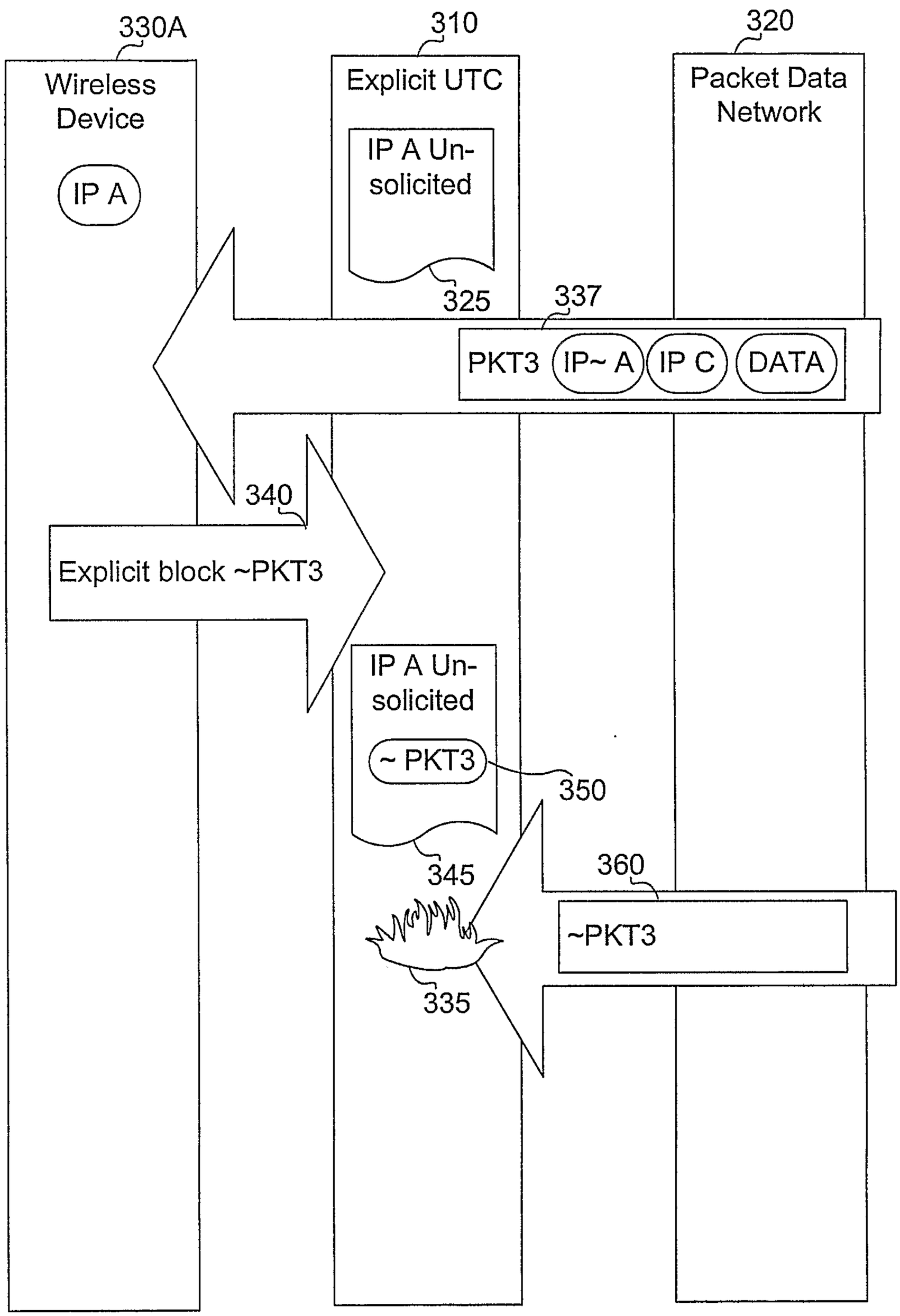

330A
Wireless Device
IP A
310
Explicit UTC
IP A Un-solicited
325
320
Packet Data Network
337
PKT3
IP~ A
IP C
DATA
340
Explicit block ~PKT3
IP A Un-solicited
~ PKT3
350
345
360
~PKT3
335

FIG. 3

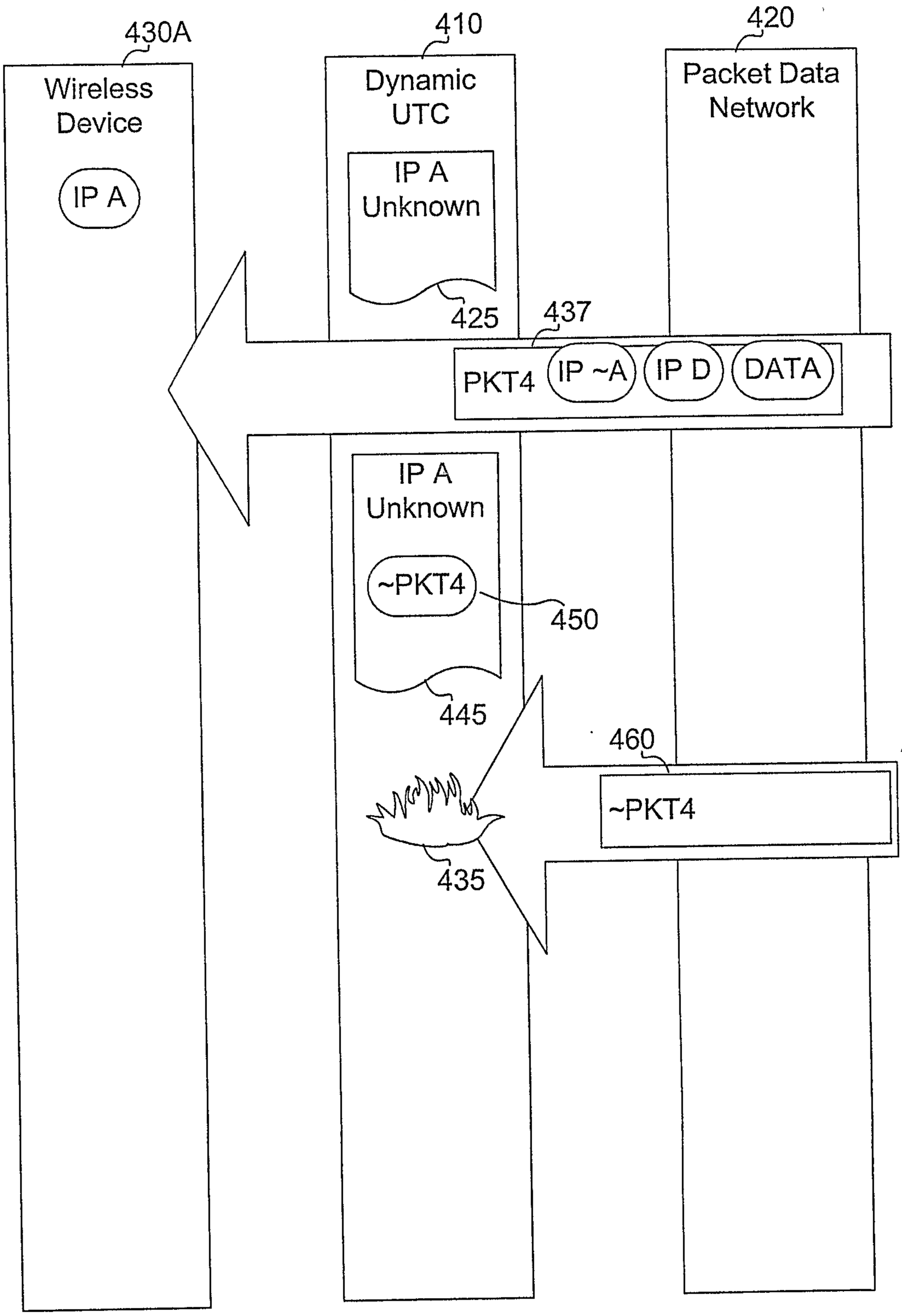

430A
Wireless Device
IP A
410
Dynamic UTC
IP A Unknown
425
420
Packet Data Network
437
PKT4
IP ~A
IP D
DATA
IP A Unknown
~PKT4
450
445
460
~PKT4
435

FIG. 4

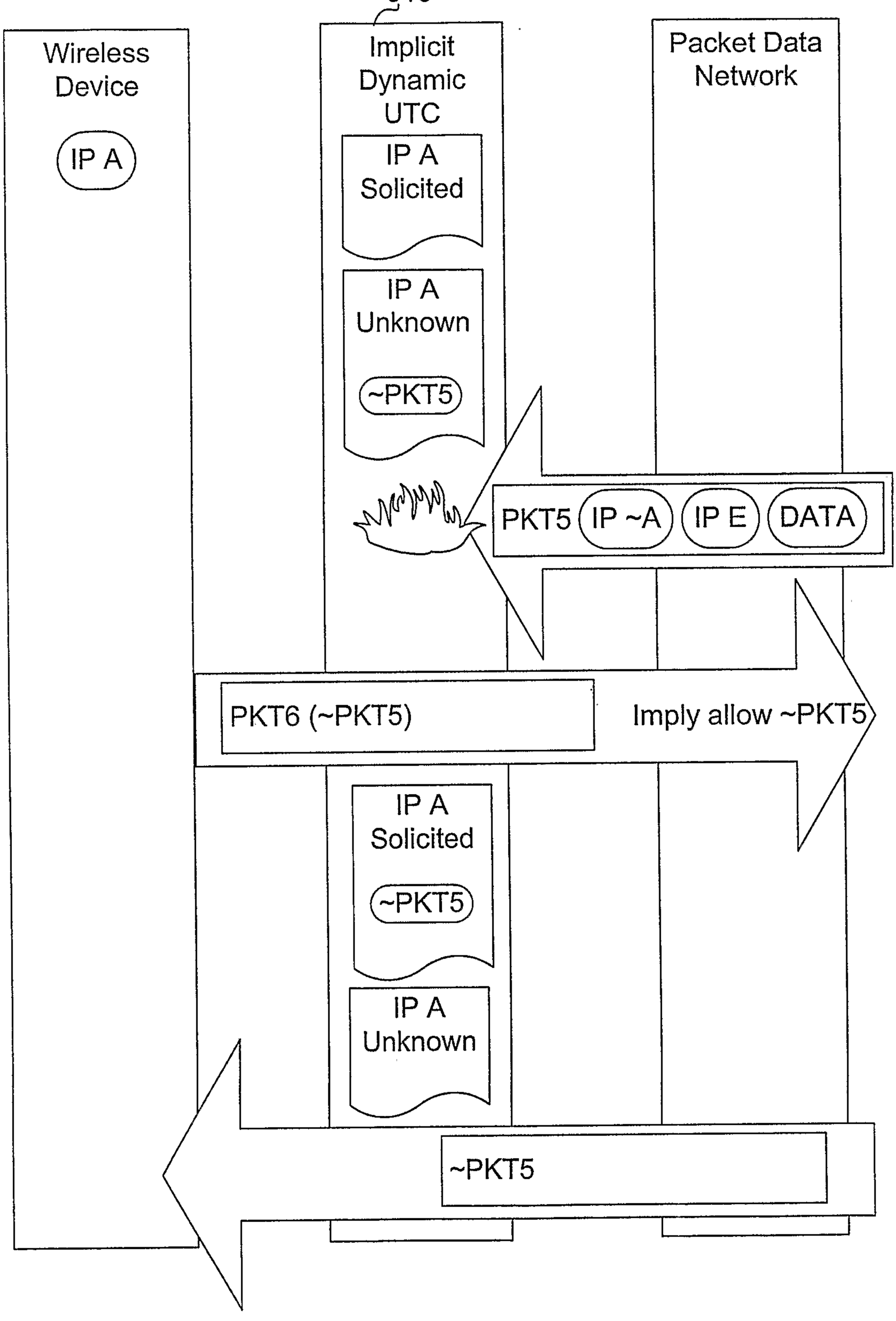

510
Wireless Device
IP A
Implicit Dynamic UTC
IP A Solicited
IP A Unknown
~PKT5
Packet Data Network
PKT5
IP ~A
IP E
DATA
PKT6 (~PKT5)
Imply allow ~PKT5
IP A Solicited
~PKT5
IP A Unknown
~PKT5

FIG. 5

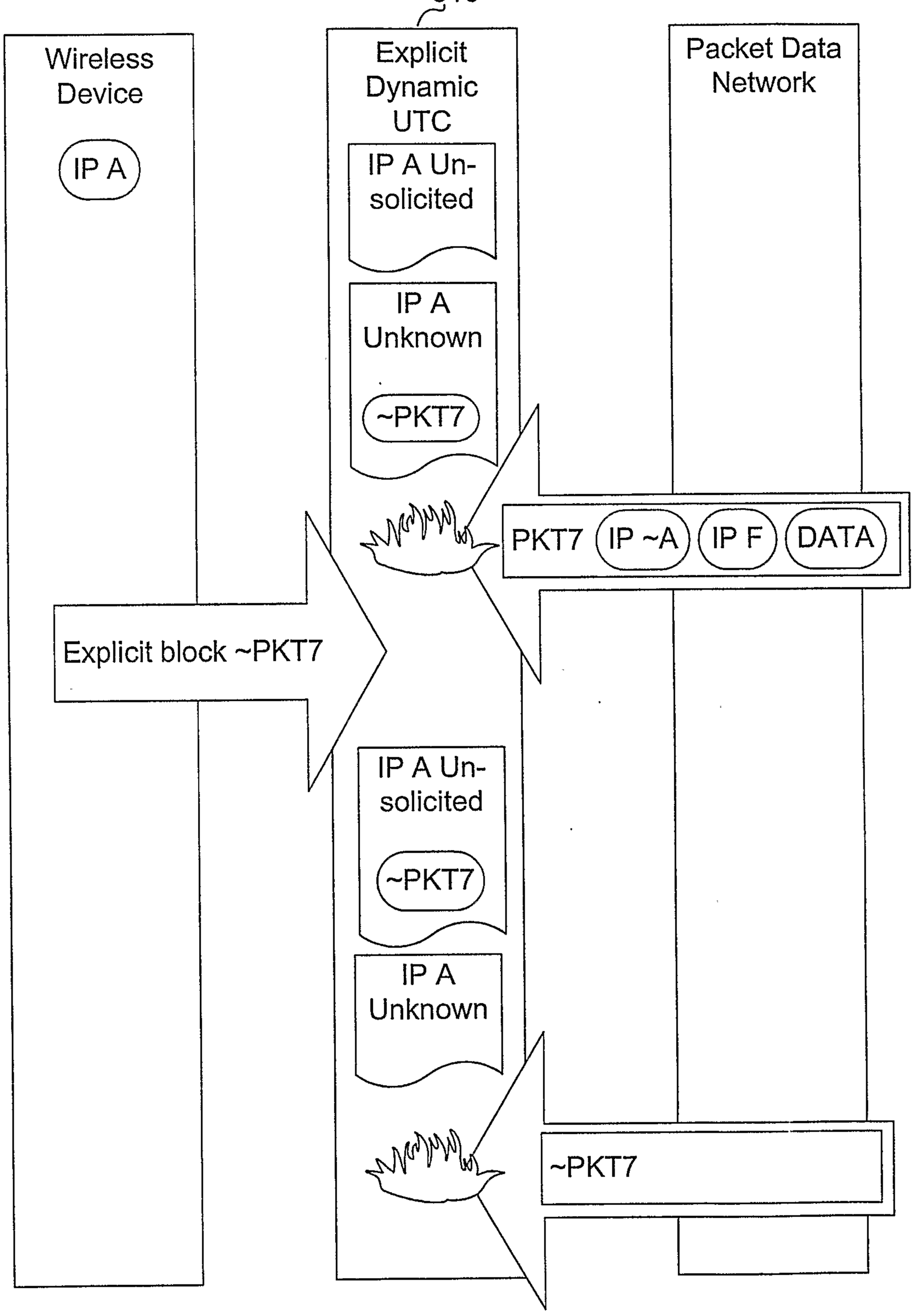

610
Wireless Device
IP A
Explicit Dynamic UTC
IP A Un-solicited
IP A Unknown
~PKT7
Packet Data Network
PKT7
IP ~A
IP F
DATA
Explicit block ~PKT7
IP A Un-solicited
~PKT7
IP A Unknown
~PKT7

FIG. 6

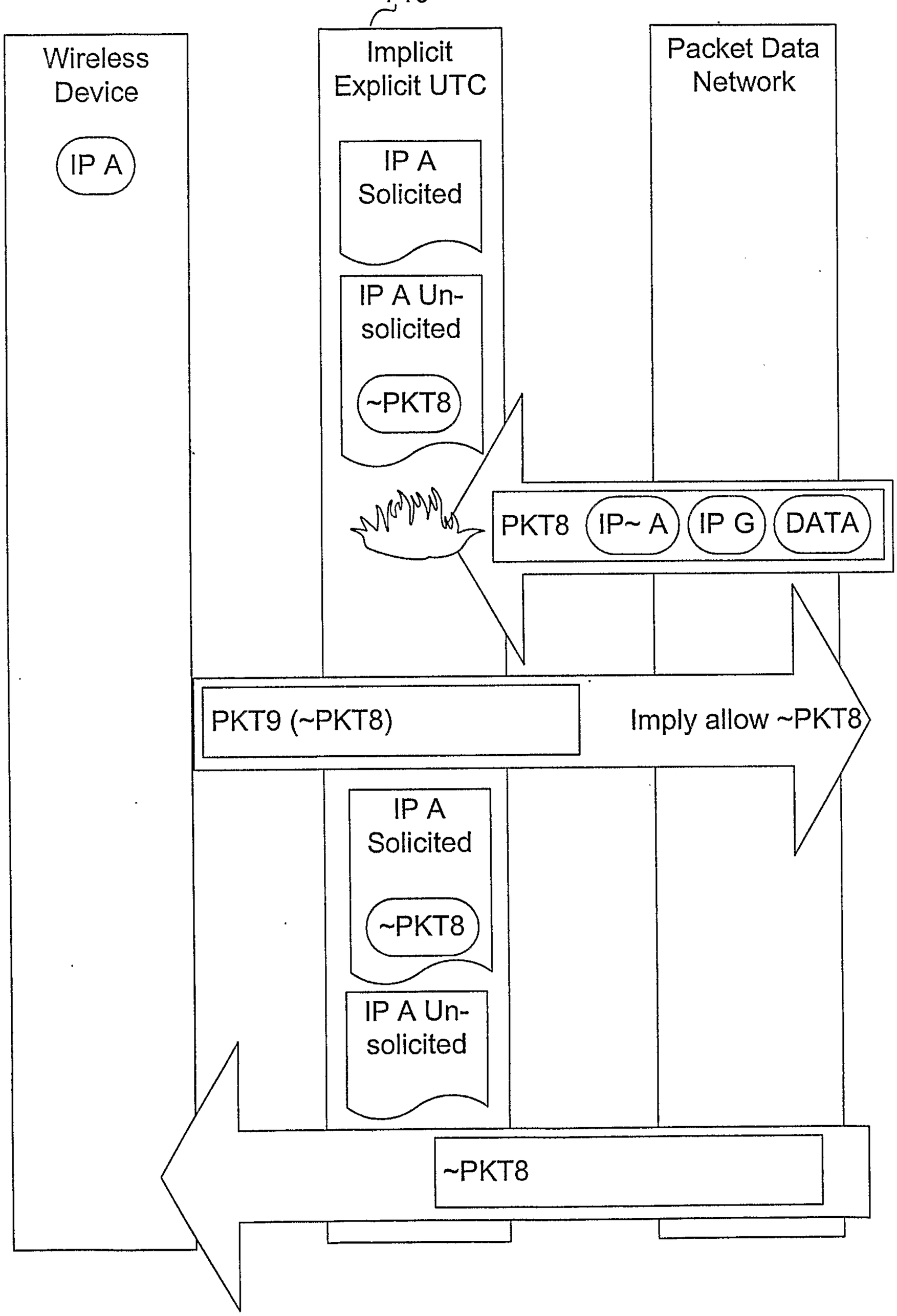

710
Wireless Device
IP A
Implicit Explicit UTC
IP A Solicited
IP A Un-solicited
~PKT8
Packet Data Network
PKT8
IP~ A
IP G
DATA
PKT9 (~PKT8)
Imply allow ~PKT8
IP A Solicited
~PKT8
IP A Un-solicited
~PKT8

FIG. 7

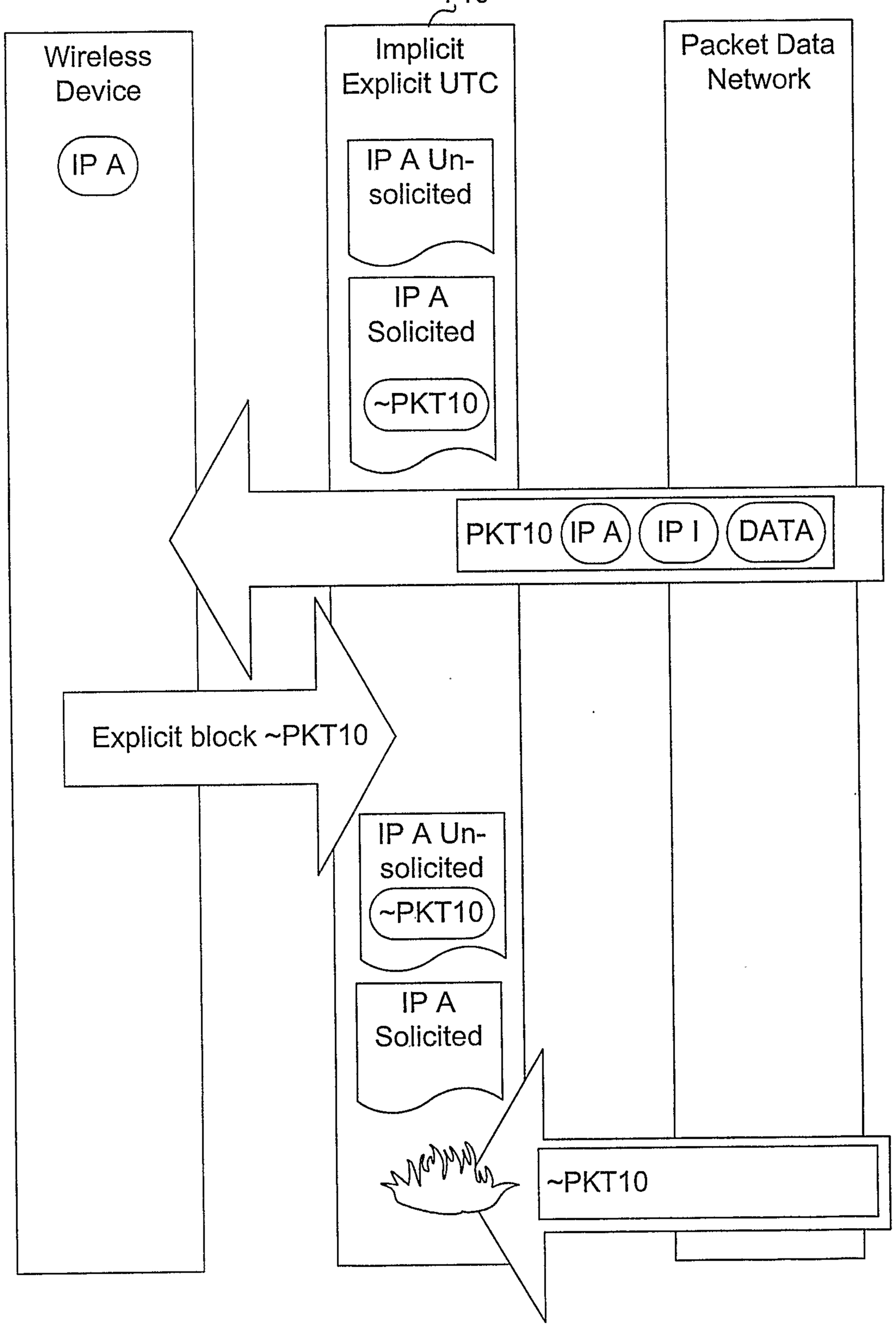

710
Wireless Device
IP A
Implicit Explicit UTC
IP A Un-solicited
IP A Solicited
~PKT10
Packet Data Network
PKT10
IP A
IP I
DATA
Explicit block ~PKT10
IP A Un-solicited
~PKT10
IP A Solicited
~PKT10

FIG. 8

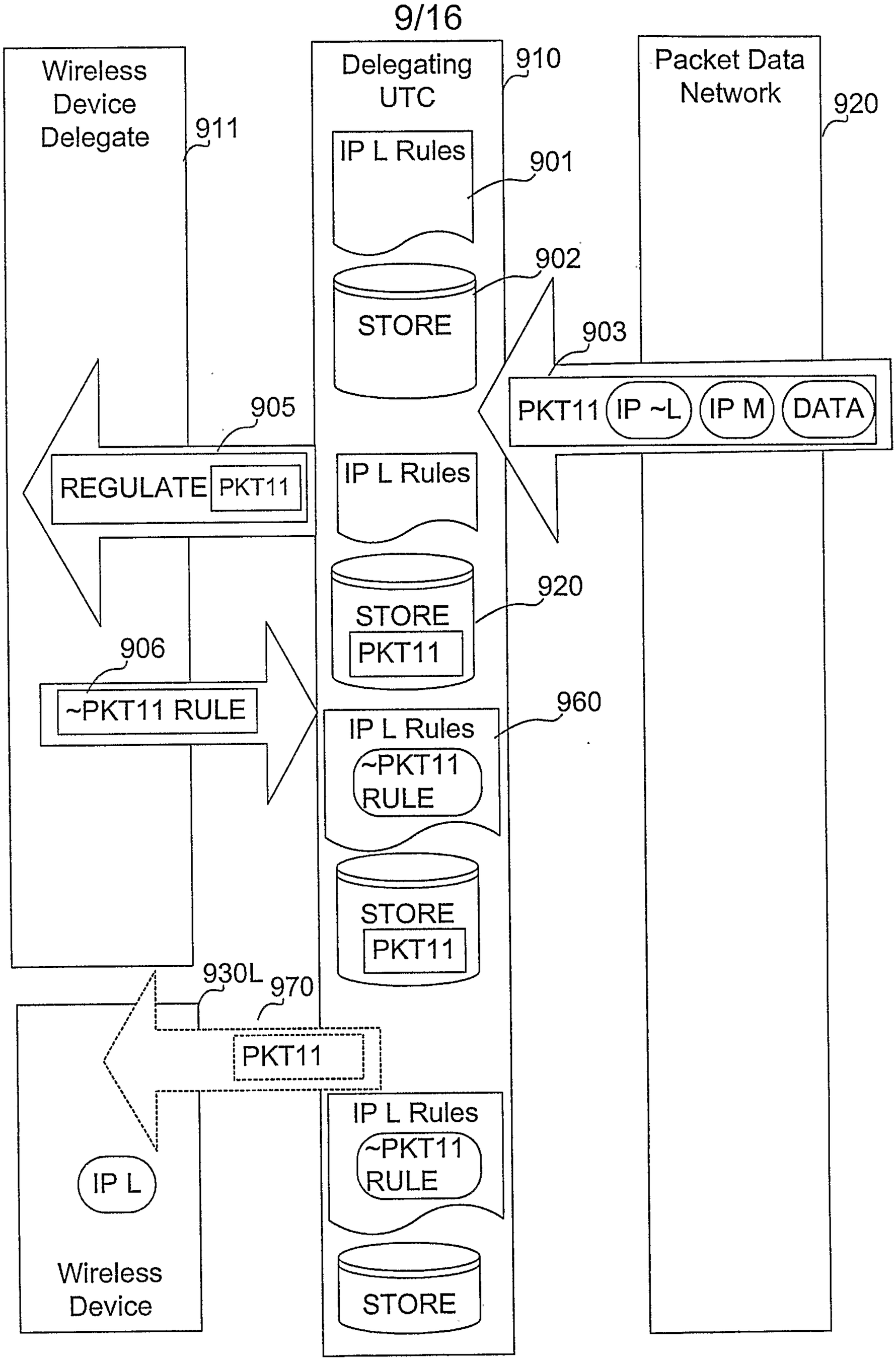

Wireless Device Delegate
911
Delegating UTC
910
Packet Data Network
920
IP L Rules
901
902
STORE
903
PKT11
IP ~L
IP M
DATA
905
REGULATE
PKT11
IP L Rules
STORE
PKT11
920
906
~PKT11 RULE
960
IP L Rules
~PKT11 RULE
STORE
PKT11
930L
970
PKT11
IP L Rules
~PKT11 RULE
IP L
Wireless Device
STORE

FIG. 9

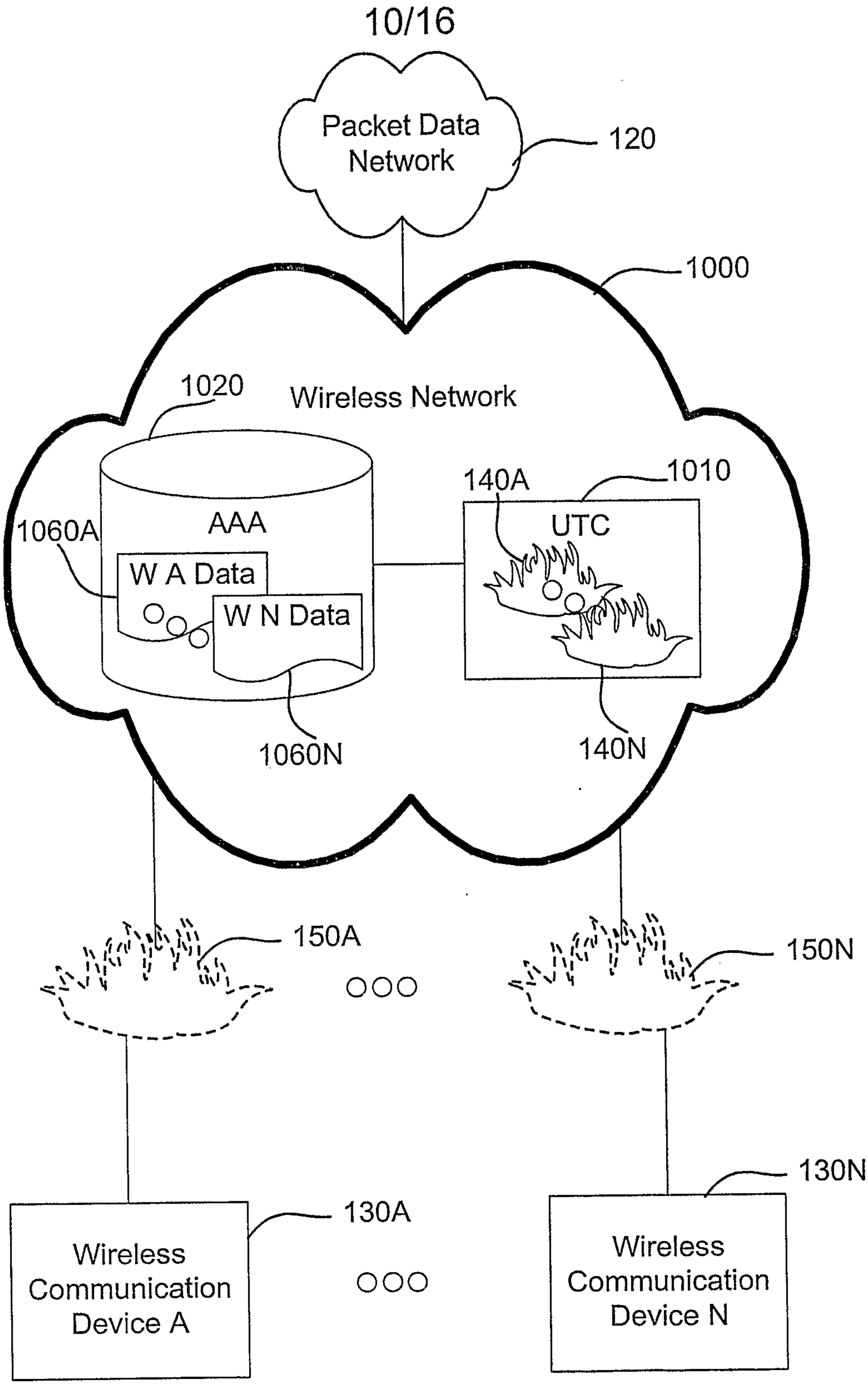

Packet Data Network
120
1000
1020
Wireless Network
AAA
1060A
W A Data
W N Data
1060N
140A
1010
UTC
140N
150A
150N
130A
Wireless Communication Device A
130N
Wireless Communication Device N

FIG. 10

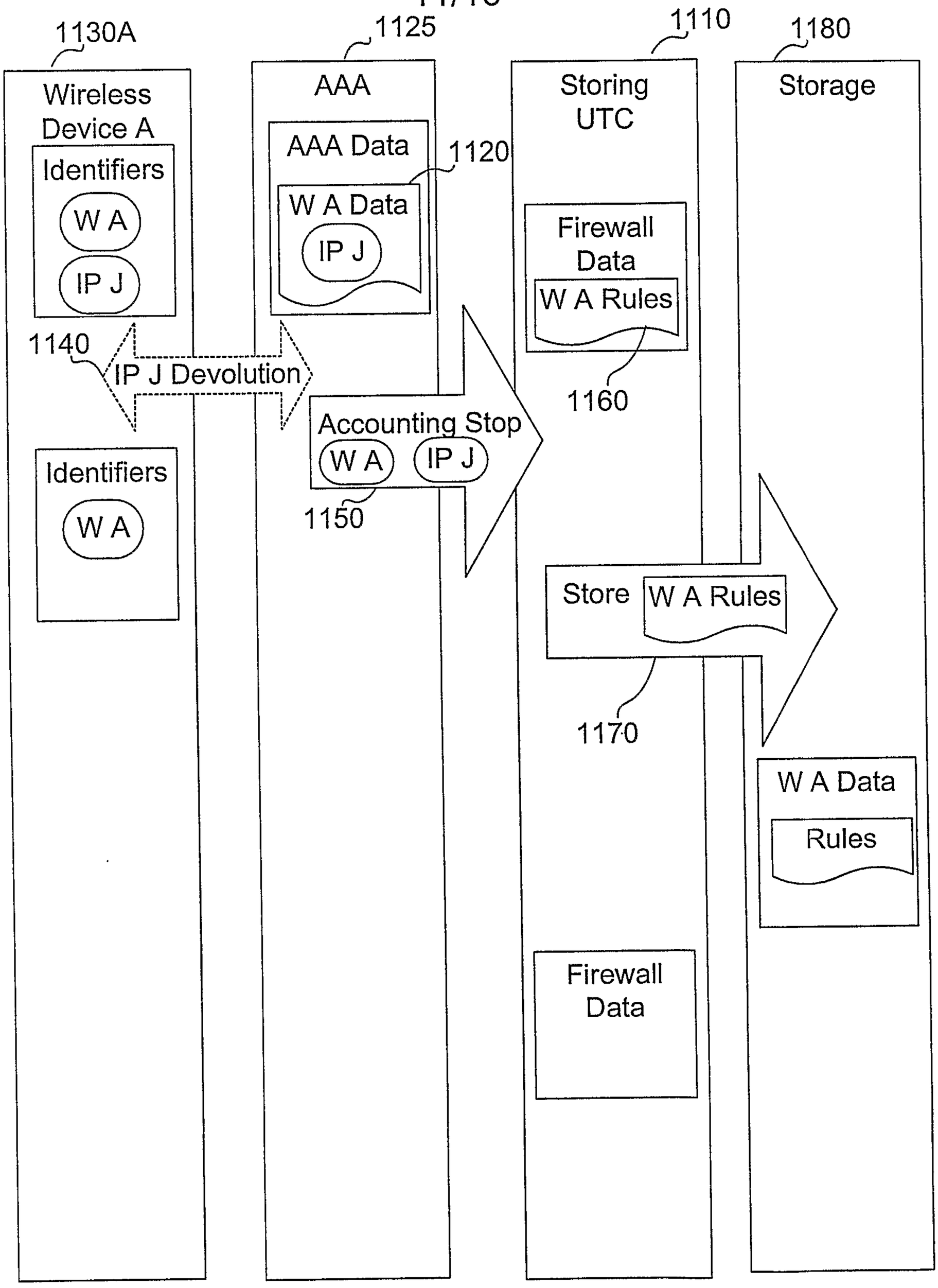

1130A
Wireless Device A
Identifiers
W A
IP J
1140
IP J Devolution
Identifiers
W A
1125
AAA
AAA Data
1120
W A Data
IP J
1150
Accounting Stop
W A
IP J
1110
Storing UTC
Firewall Data
W A Rules
1160
1180
Storage
Store
W A Rules
1170
W A Data
Rules
Firewall Data

FIG. 11

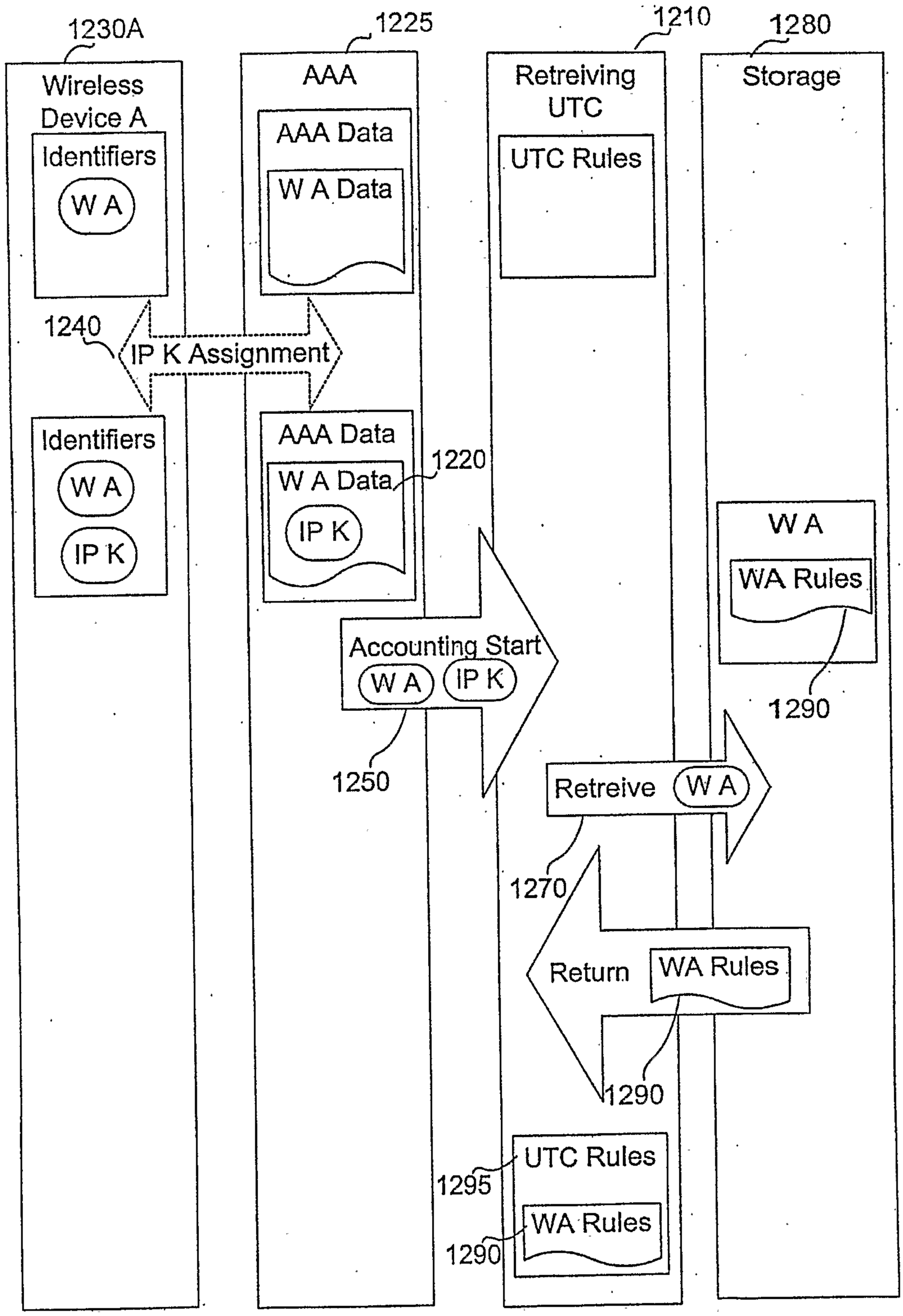

1230A
Wireless Device A
Identifiers
W A
1225
AAA
AAA Data
W A Data
1210
Retreiving UTC
UTC Rules
1280
Storage
1240
IP K Assignment
Identifiers
W A
IP K
AAA Data
W A Data
IP K
1220
W A
WA Rules
1290
Accounting Start
W A
IP K
1250
Retreive W A
1270
Return WA Rules
1290
1295
UTC Rules
WA Rules
1290

FIG. 12

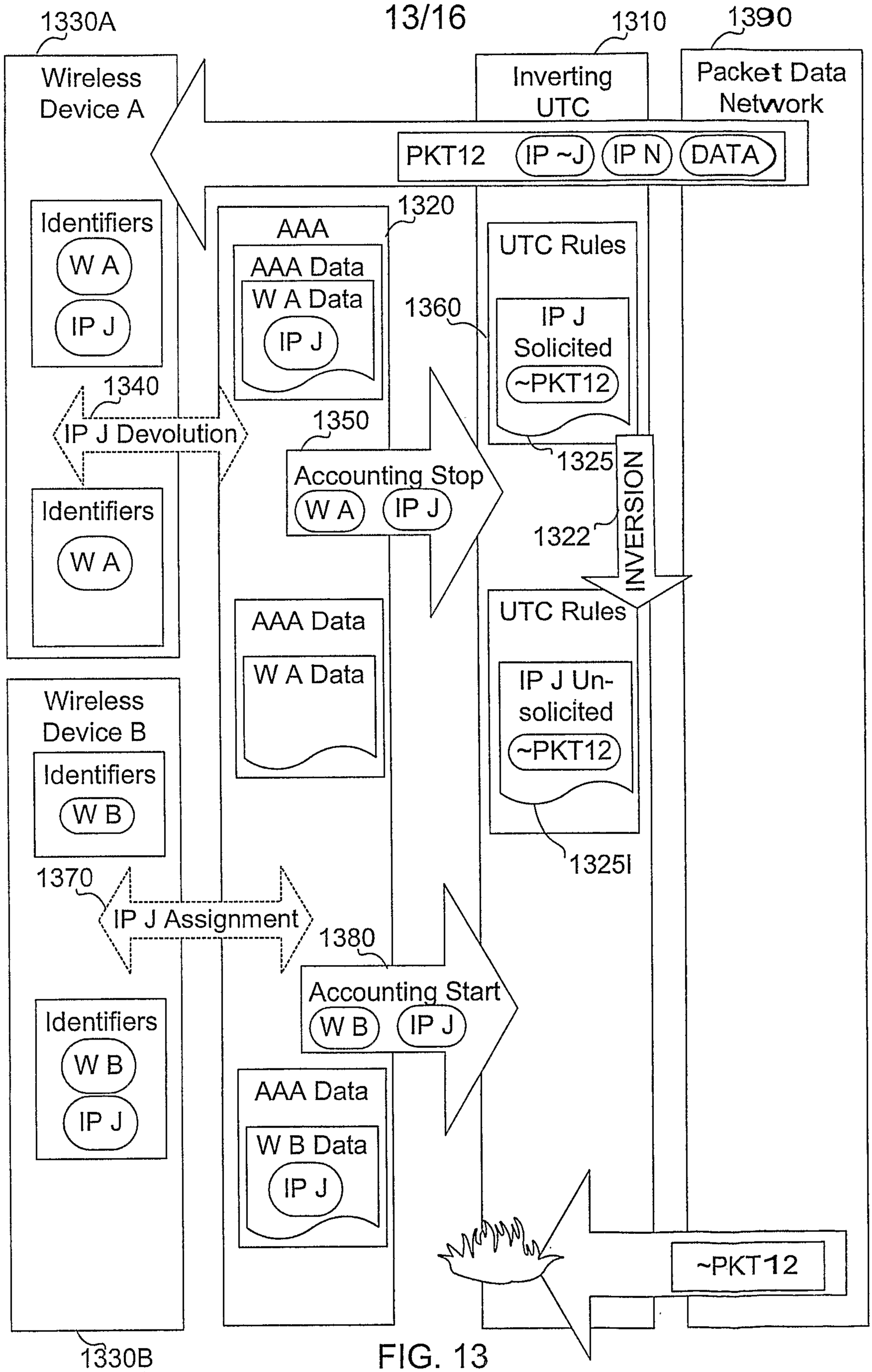

1330A
Wireless Device A
1310
Inverting UTC
1390
Packet Data Network
PKT12
IP ~J
IP N
DATA
Identifiers
W A
IP J
1320
AAA
AAA Data
W A Data
IP J
UTC Rules
1360
IP J Solicited
~PKT12
1340
IP J Devolution
1350
Accounting Stop
W A
IP J
1325
INVERSION
1322
Identifiers
W A
AAA Data
W A Data
UTC Rules
IP J Un-solicited
~PKT12
1325I
Wireless Device B
Identifiers
W B
1370
IP J Assignment
1380
Accounting Start
W B
IP J
Identifiers
W B
IP J
AAA Data
W B Data
IP J
~PKT12
1330B

FIG. 13

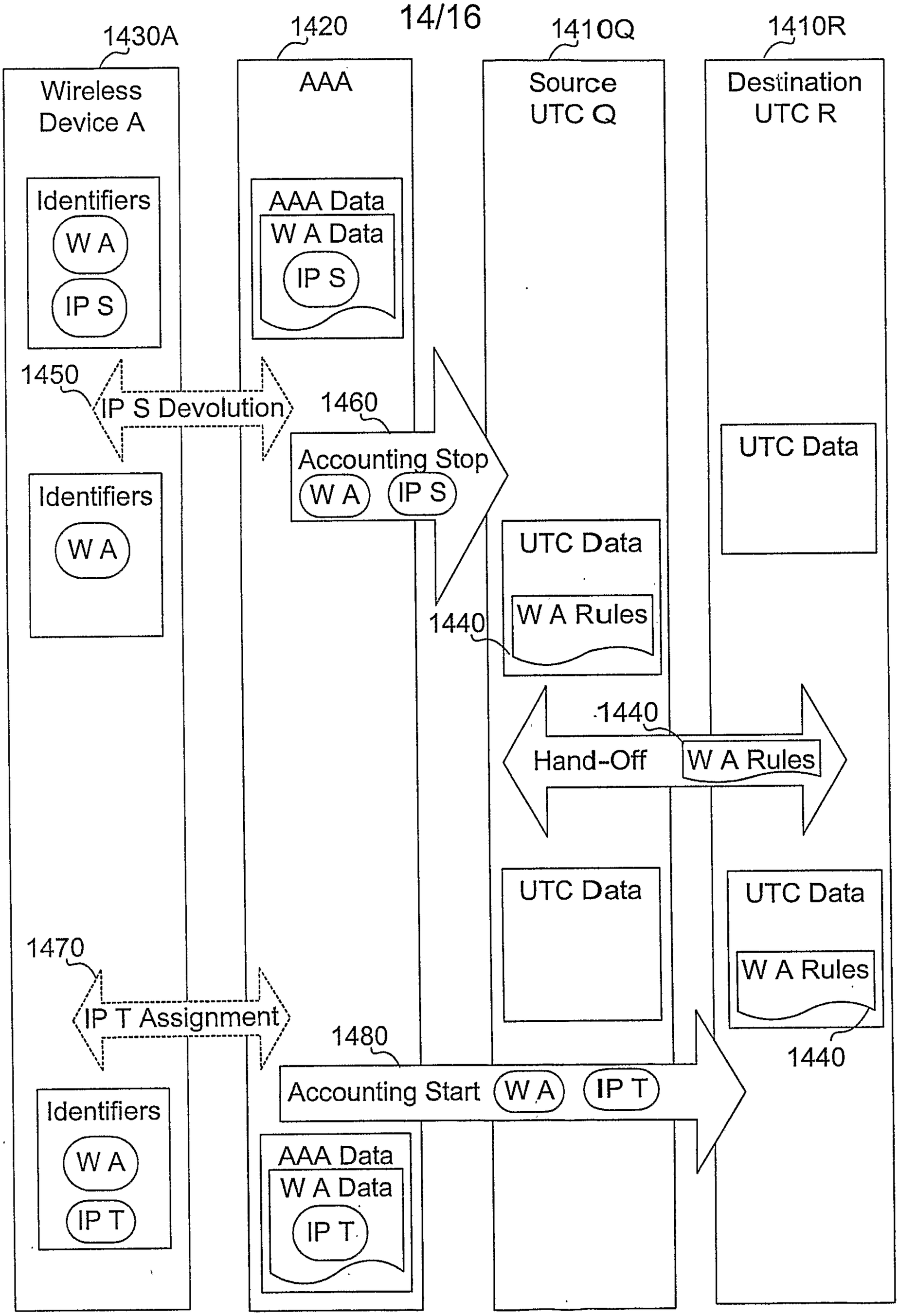

1430A
Wireless Device A
Identifiers
W A
IP S
1420
AAA
AAA Data
W A Data
IP S
1410Q
Source UTC Q
1410R
Destination UTC R
1450
IP S Devolution
Identifiers
W A
1460
Accounting Stop
W A
IP S
UTC Data
W A Rules
1440
UTC Data
1440
Hand-Off
W A Rules
UTC Data
UTC Data
W A Rules
1440
1470
IP T Assignment
1480
Accounting Start
W A
IP T
Identifiers
W A
IP T
AAA Data
W A Data
IP T

FIG. 14

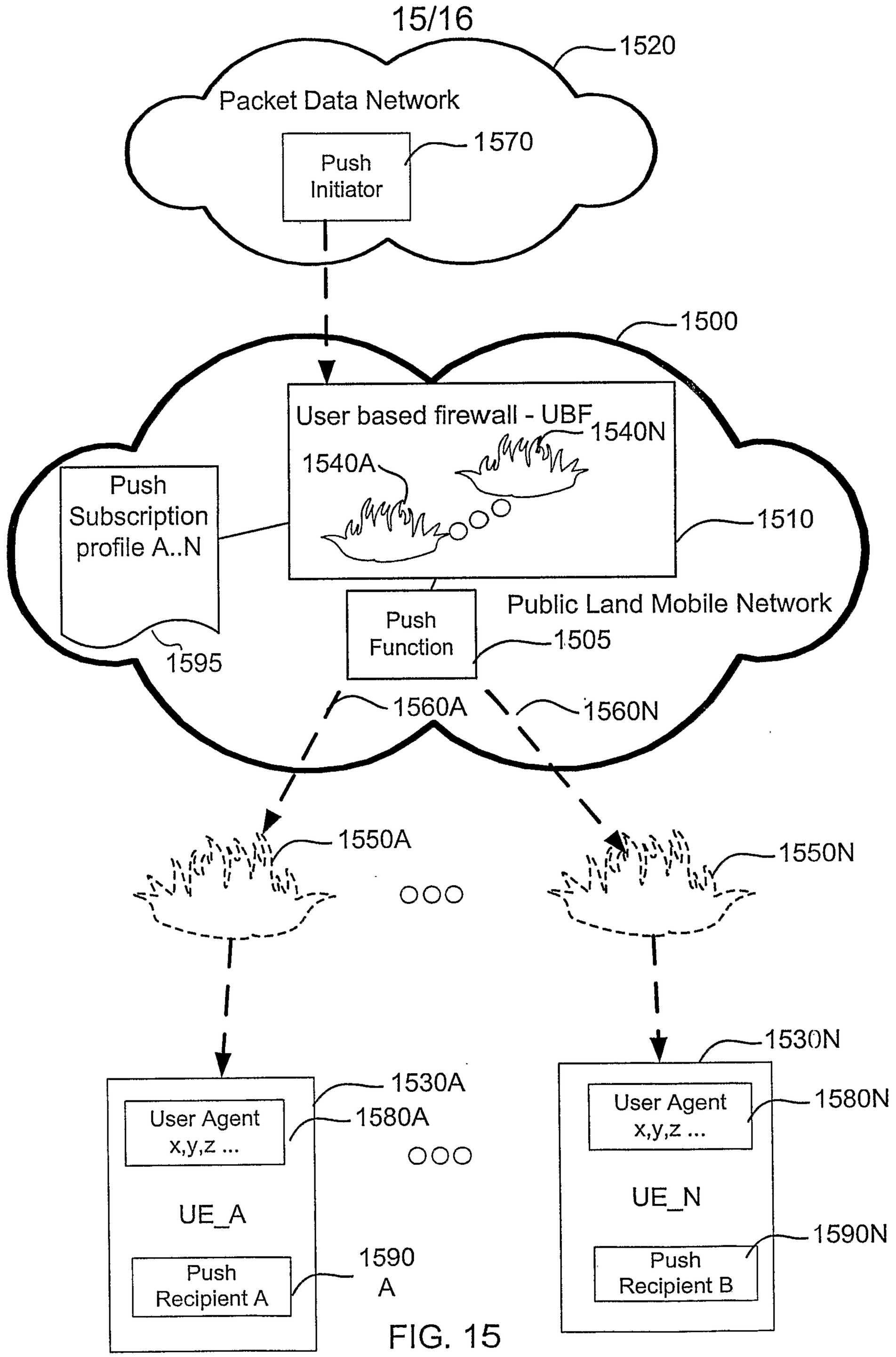

Packet Data Network
1520
Push Initiator
1570
1500
User based firewall - UBF
1540N
1540A
Push Subscription profile A..N
1510
Public Land Mobile Network
Push Function
1505
1595
1560A
1560N
1550A
1550N
1530A
User Agent x,y,z ...
1580A
UE_A
Push Recipient A
1590 A
1530N
User Agent x,y,z ...
1580N
UE_N
Push Recipient B
1590N

FIG. 15

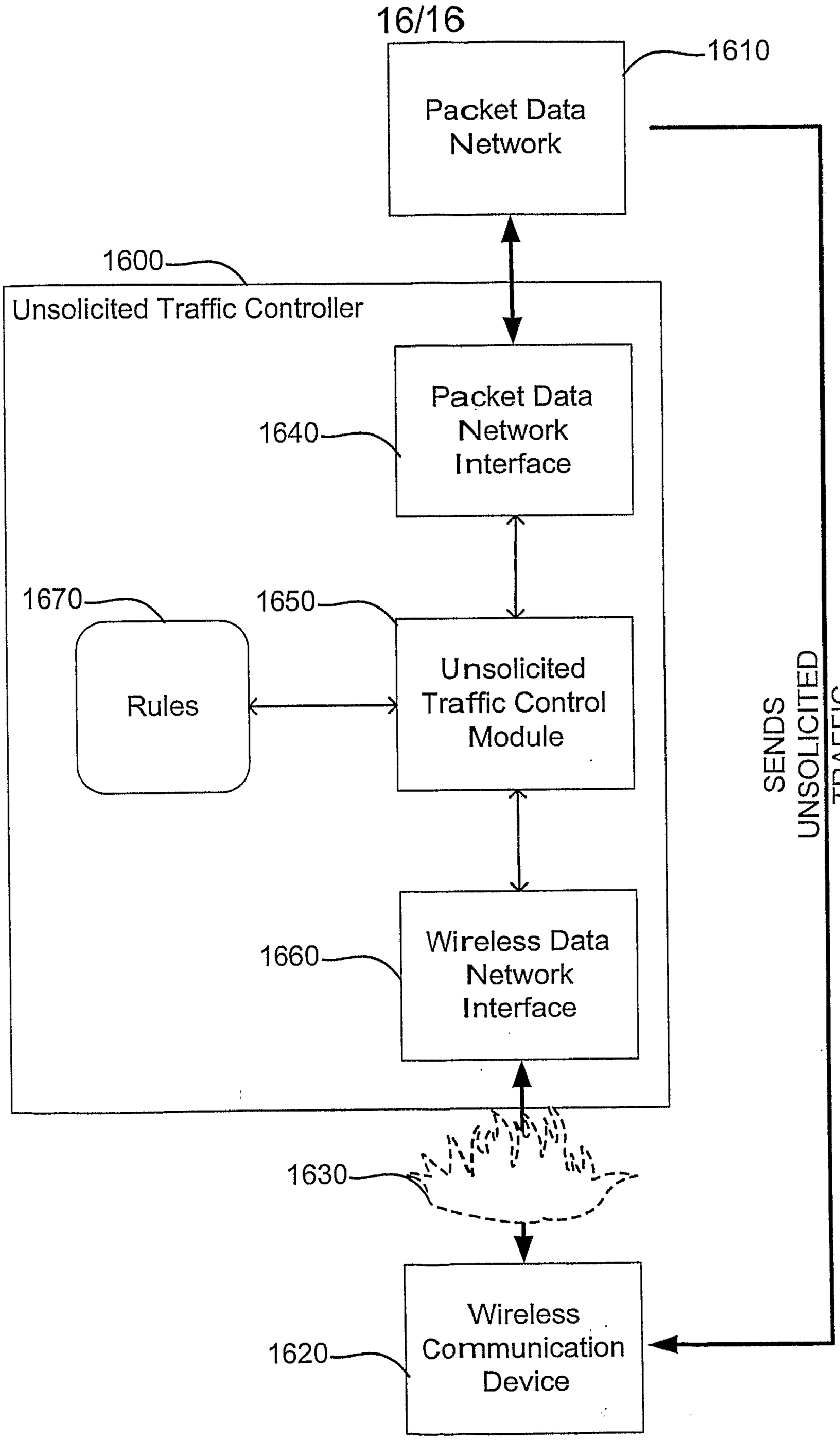
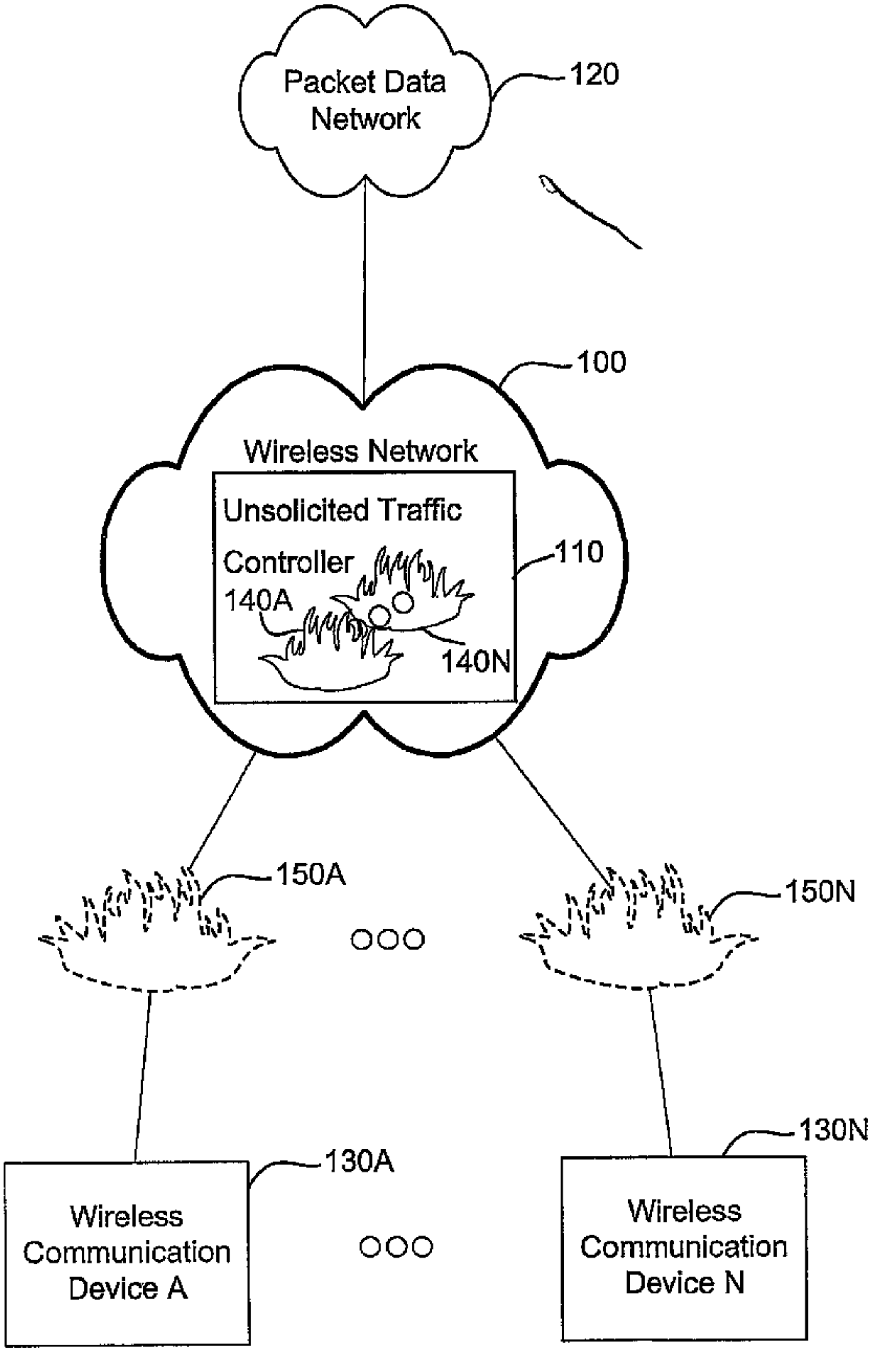

1610
Packet Data Network
1600
Unsolicited Traffic Controller
1640
Packet Data Network Interface
1670
Rules
1650
Unsolicited Traffic Control Module
1660
Wireless Data Network Interface
SENDS UNSOLICITED TRAFFIC
1630
1620
Wireless Communication Device

FIG. 16


Packet Data Network
120
100
Wireless Network
Unsolicited Traffic Controller
140A
140N
110
150A
150N
130A
130N
Wireless Communication Device A
Wireless Communication Device N