



(19) **United States**
(12) **Patent Application Publication**
Zhu

(10) **Pub. No.: US 2013/0227644 A1**
(43) **Pub. Date: Aug. 29, 2013**

(54) **SIPTO DECISION METHOD AND DEVICE FOR H(E)NB SYSTEM**

Publication Classification

(75) Inventor: **Li Zhu**, Shenzhen (CN)
(73) Assignee: **ZTE CORPORATION**, Shenzhen, Guangdong (CN)

(51) **Int. Cl.**
H04W 12/06 (2006.01)
(52) **U.S. Cl.**
CPC **H04W 12/06** (2013.01)
USPC **726/3**

(21) Appl. No.: **13/703,117**

(22) PCT Filed: **May 31, 2011**

(57) **ABSTRACT**

(86) PCT No.: **PCT/CN11/74995**

§ 371 (c)(1),
(2), (4) Date: **Jan. 10, 2013**

(30) **Foreign Application Priority Data**

Jun. 12, 2010 (CN) 201010206676.8

The disclosure claims a Selected Internet Protocol Traffic Offload (SIPTO) decision method and device for a Home (evolved) Node-B (H(e)NB) system, both the method and device can judge whether a H(e)NB has the SIPTO authority, and can allow the H(e)NB to implement the SIPTO if the H(e)NB has the SIPTO authority. The method and device of the disclosure can support the SIPTO of the H(e)NB.

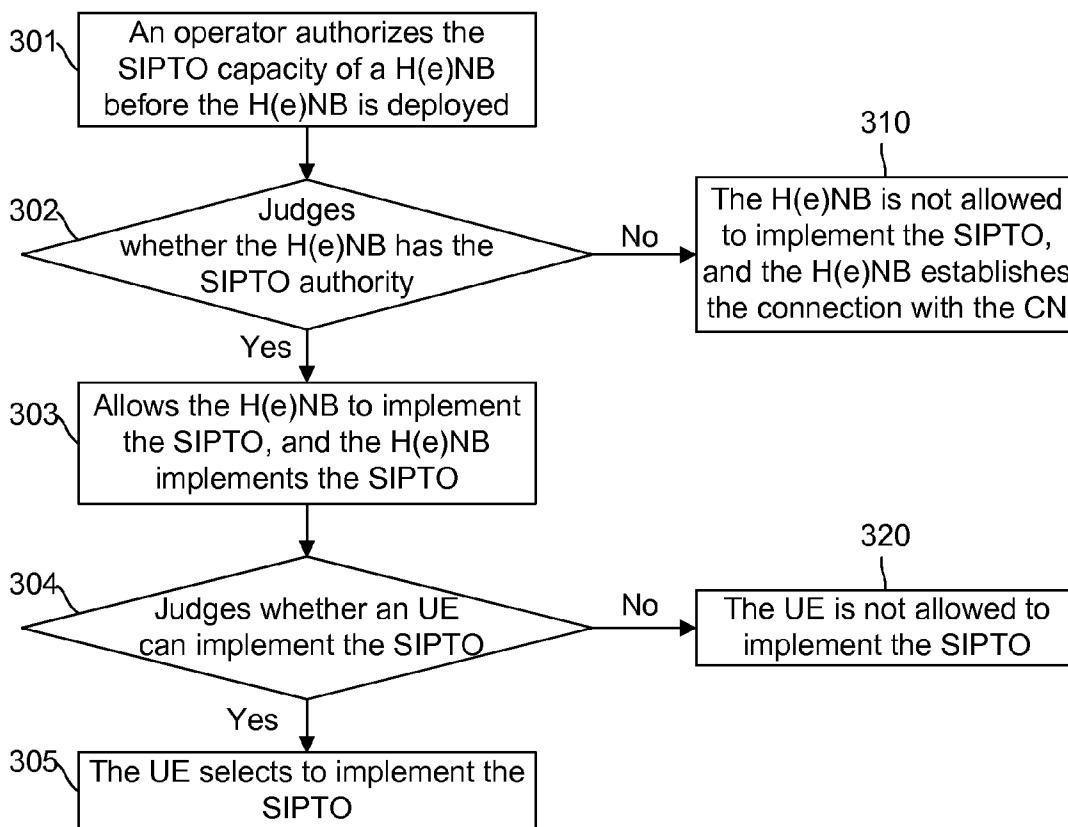


Fig. 1

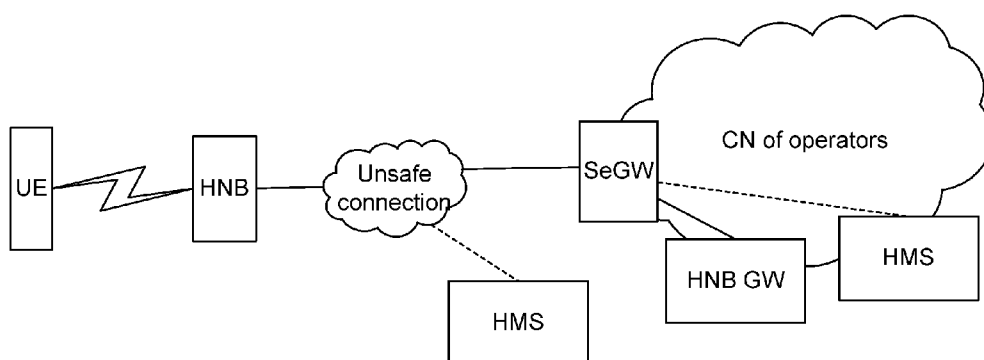


Fig. 2

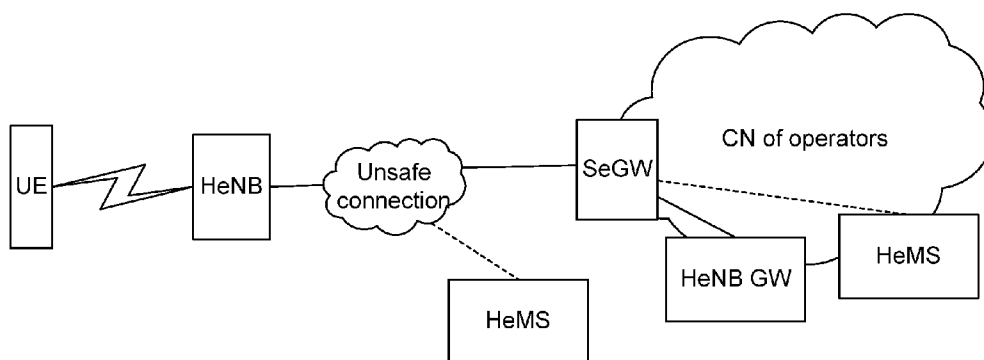


Fig. 3

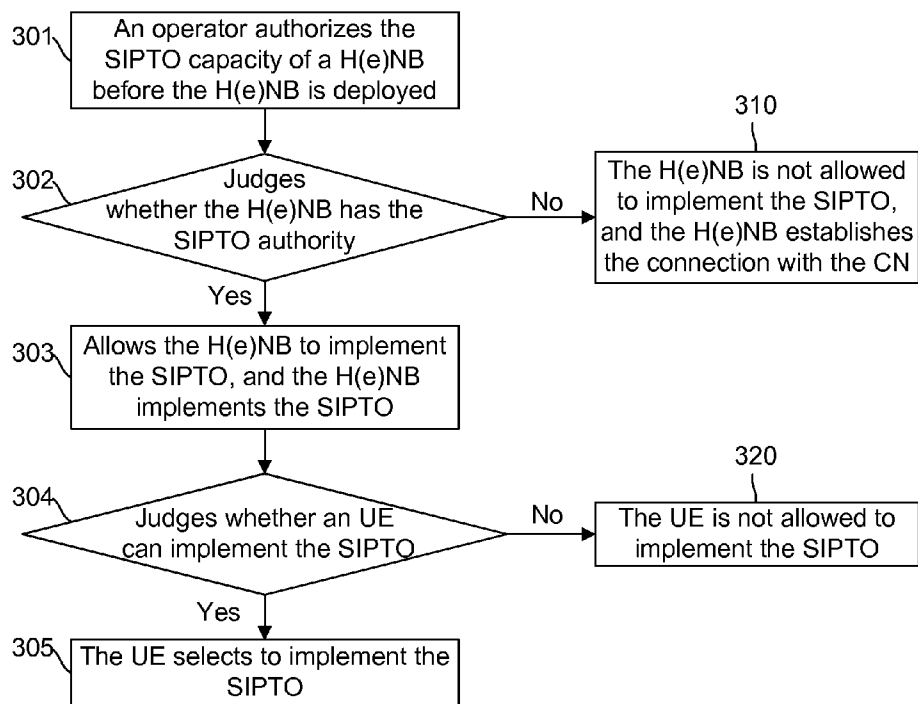


Fig. 4

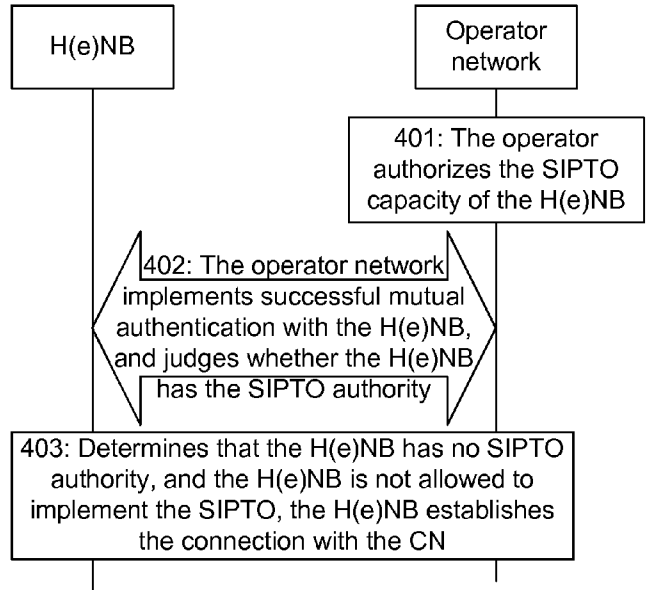


Fig. 5

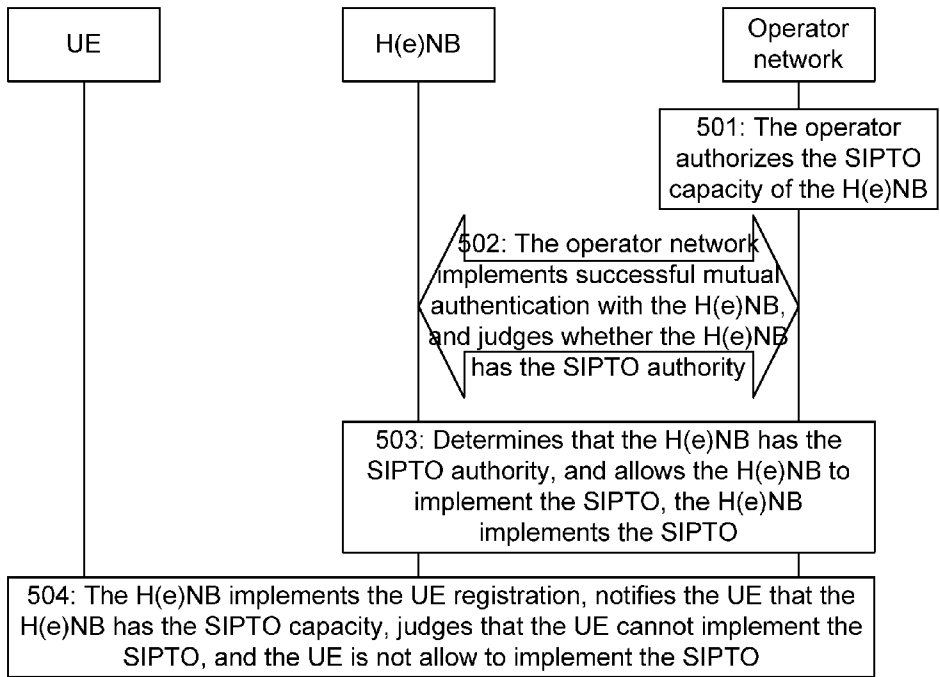


Fig. 6

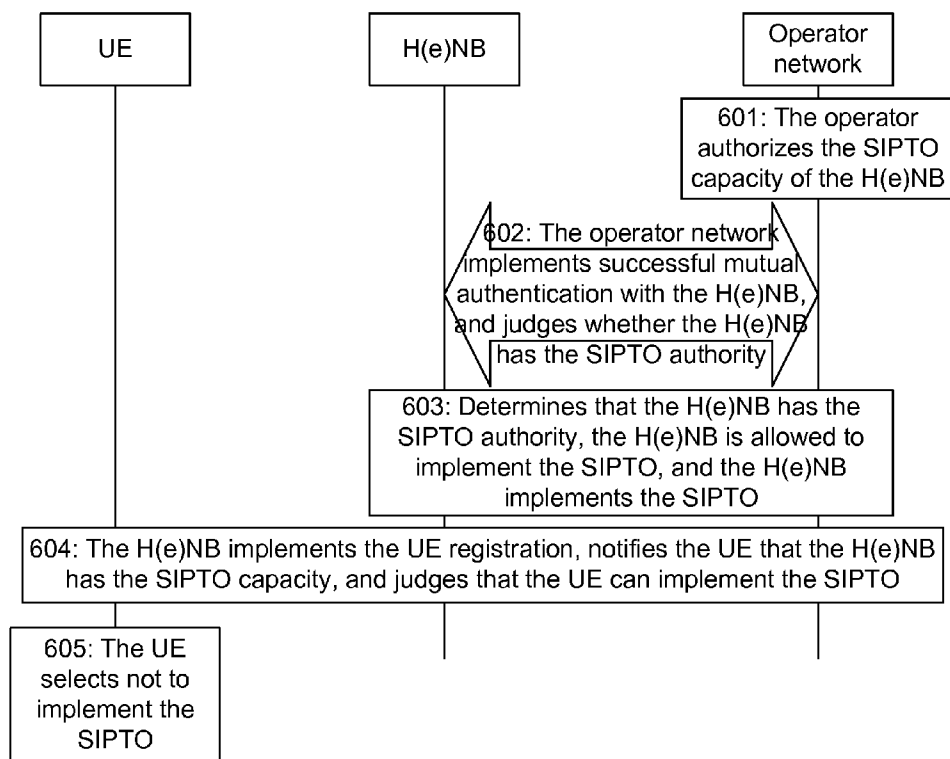


Fig. 7

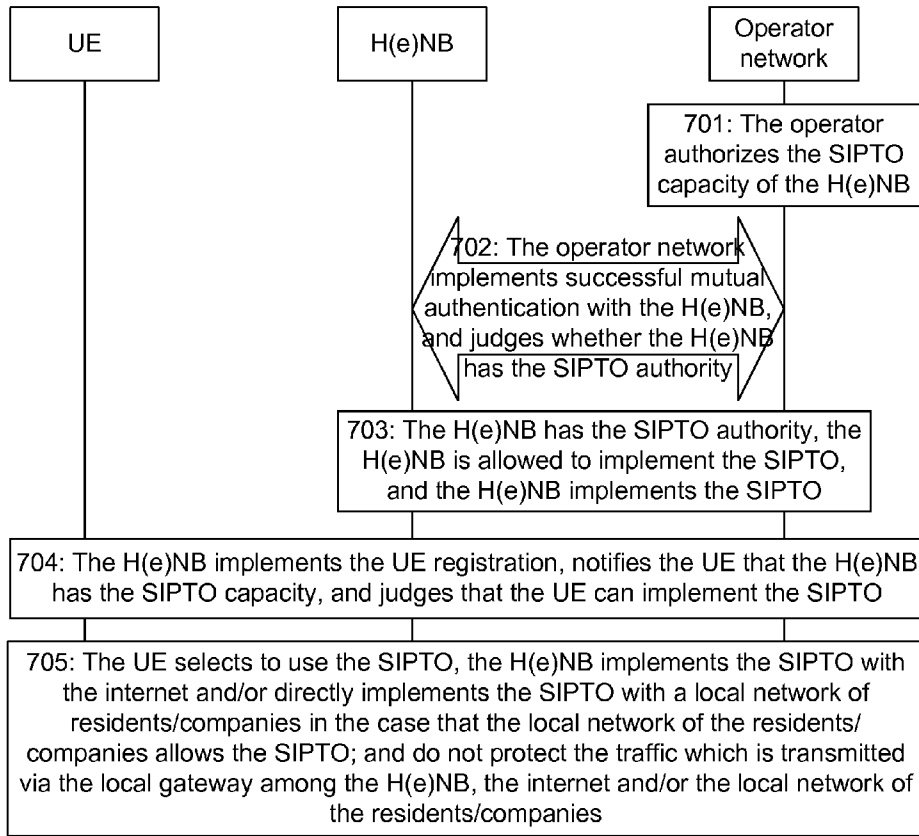


Fig. 8

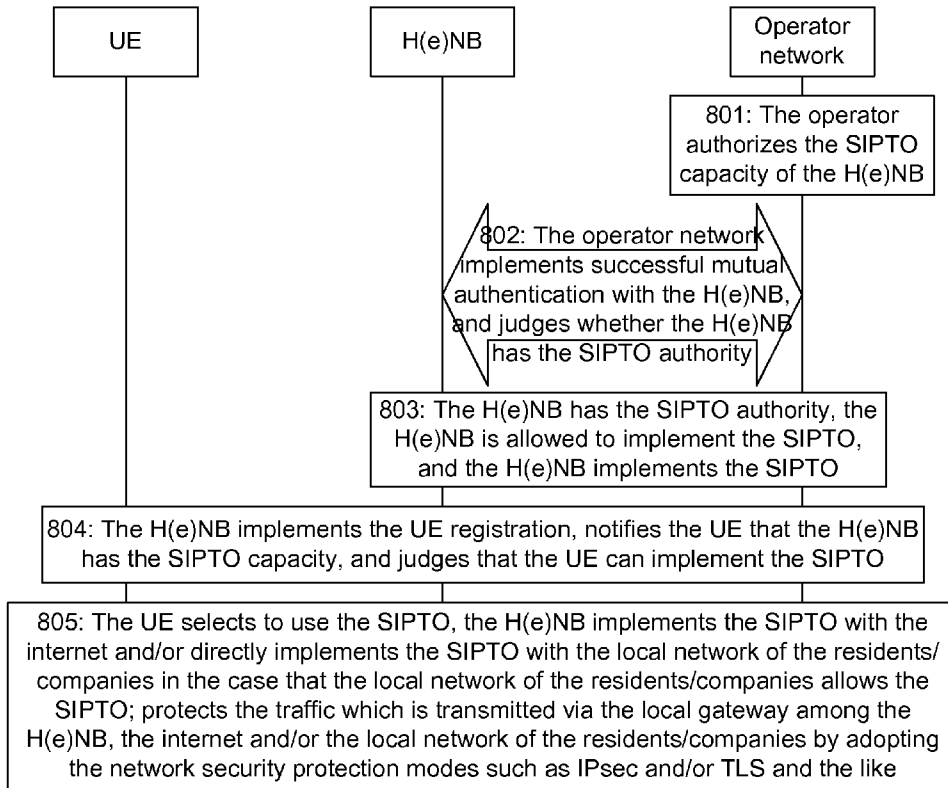


Fig. 9

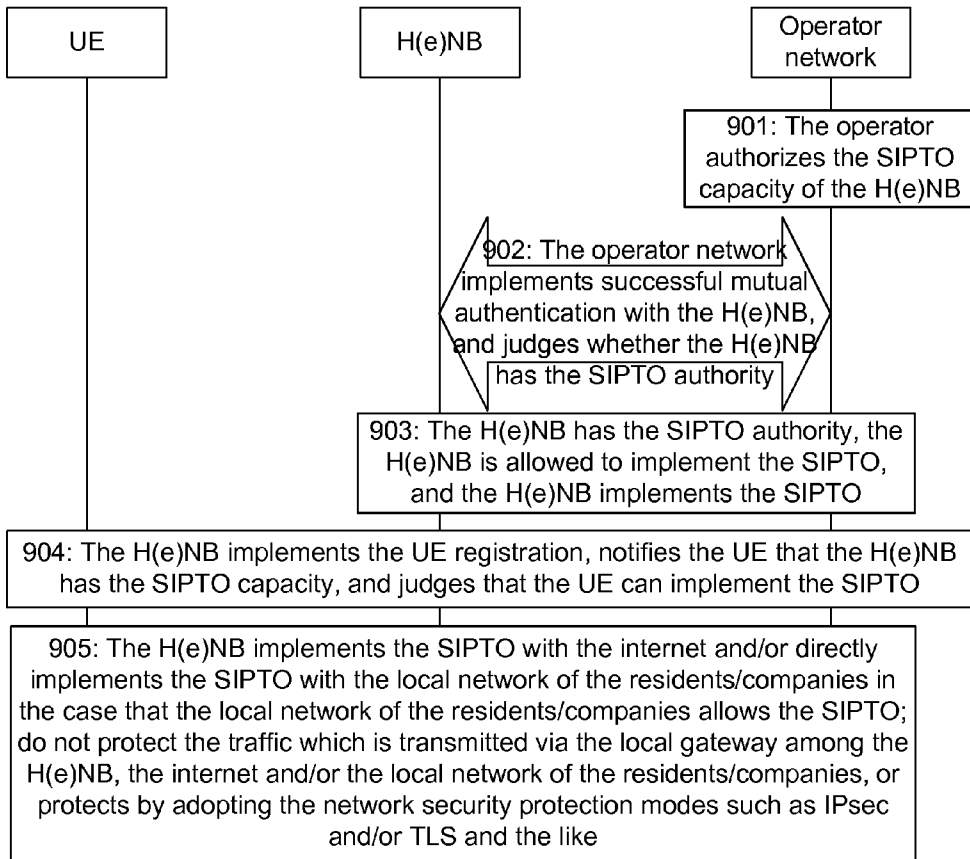
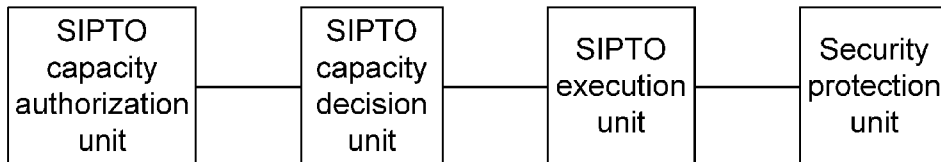


Fig. 10



SIPTO DECISION METHOD AND DEVICE FOR H(e)NB SYSTEM

TECHNICAL FIELD

[0001] The disclosure relates to the communication field, and in particular to a Selected Internet Protocol Traffic Offload (SIPTO) decision method and device of a Home (evolved) Node-B (H(e)NB) system which includes a Home Node-B (HNB) and a Home evolved Node-B (HeNB).

BACKGROUND

[0002] The HNB is configured to provide wireless coverage of The 3rd Generation Telecommunication (3G) for 3G mobile phones in homes. The HNB generally includes the access functions of a standard 3G macro wireless access network, such as a Node B and the like, and the wireless resource management functions such as a standard Radio Network Controller (RNC) and the like.

[0003] FIG. 1 is a system structure diagram of the HNB; as shown in FIG. 1, the HNB is accessed to a Core Network (CN) of an operator via a Security Gateway (SeGW). The SeGW represents the CN of the operator and implements mutual authentication with the HNB. A HNB Gateway (HNB GW) and the SeGW are entities logically separated in the CN of the operator, and are used for the access control of the User Equipment (UE) of a non-Closed Subscriber Group (CSG).

[0004] FIG. 2 is a system structure diagram of the HeNB; as shown in FIG. 2, the difference between the HeNB and the HNB is that: the HeNB is an air interface for connecting The 3rd-Generation Partnership Project (3GPP) UE and an Evolved Universal Terrestrial Radio Access Network (EUTRAN). The H(e)NB includes the HNB and the HeNB, namely, is the joint name of the HNB and the HeNB.

[0005] As the existing wireless access technology makes the data transmission achieve higher rate, the operators have great requirement on reducing the network load and saving transmission cost by offloading the network traffic, but local IP accessing makes the UE with an IP address can directly access, via the H(e)NB, to the devices with IP addresses in other IP networks of the local residents or companies; thereby, reducing the network load and saving the transmission cost by offloading the selected traffic of a H(e)NB subsystem and a macro network (such as the internet traffic of the H(e)NB subsystem, the internet traffic, the company traffic of the macro network and the like) is increasingly concerned by the operators.

[0006] However, the current technical specifications have no description for the decision mechanism of the SIPTO of the H(e)NB, and have no corresponding protection measures for the transmission paths and transmission contents of the SIPTO of the H(e)NB either.

SUMMARY

[0007] In view of the above, the main purpose of the disclosure is to provide a SIPTO decision method and device of a H(e)NB system, so as to support the SIPTO of the H(e)NB.

[0008] In order to achieve the above purpose, the technical solutions of the disclosure are realized as follows:

[0009] a SIPTO decision method of a H(e)NB system, includes:

[0010] judges whether the H(e)NB has a SIPTO authority, and allows the H(e)NB to implement the SIPTO if the H(e)NB has the SIPTO authority.

[0011] The process of judges whether the H(e)NB has the SIPTO authority may include:

[0012] searching a H(e)NB identity stored in a decision point for judging whether the H(e)NB has the SIPTO authority, and confirming that the H(e)NB has the SIPTO authority if the H(e)NB identity is found, or the identity of the H(e)NB which is added with a SIPTO mark is found.

[0013] The method may further include:

[0014] the H(e)NB implements the SIPTO;

[0015] or, the H(e)NB implements the SIPTO, and establishes a connection with the CN.

[0016] The method may further include:

[0017] judges whether a UE can implement the SIPTO, and implements the SIPTO aiming at the data of the UE when the UE can implement the SIPTO.

[0018] The process of judges whether the UE can implement the SIPTO may include:

[0019] searches a UE identity which is stored in a related network element for authenticating the UE, and determines that the UE can implement the SIPTO if the UE identity is found, or the identity of the UE which is added with a SIPTO mark is found.

[0020] The method may further include:

[0021] implements network security protection including the IP Security (IPsec) and/or Transport Layer Security (TLS) for the transmission data of the H(e)NB and/or the UE.

[0022] A SIPTO decision method of a H(e)NB system, includes: judges whether the UE can implement the SIPTO, and implementing the SIPTO aiming at the transmission data of the UE when the UE can implement the SIPTO.

[0023] The process of judges whether the UE can implement the SIPTO may include:

[0024] searching a UE identity which is stored in the related network element for authenticating the UE, and determining that the UE can implement the SIPTO if the UE identity is found, or the identity of the UE which is added with a SIPTO mark is found.

[0025] The method may further include:

[0026] the UE selects to implement the SIPTO, aiming at the transmission data of the UE, the H(e)NB accessed by the UE implements the SIPTO with the internet, and/or implements the SIPTO with the local network of residents/companies.

[0027] The SIPTO implemented by the H(e)NB may be implemented in the case that the local network of the residents/companies allows the SIPTO; or,

[0028] the SIPTO implemented by the H(e)NB may be directly implemented without allowing the SIPTO by the local network of the residents/companies.

[0029] The method may further include: not protecting the transmission data of the UE, or implements the network security protection including the IPsec and/or TLS.

[0030] A SIPTO decision device of a H(e)NB system, includes a SIPTO capacity decision unit and a SIPTO execution unit, wherein,

[0031] the SIPTO capacity decision unit is configured to judge whether the H(e)NB and/or the UE have/has the SIPTO authority, and to notify a judgment result to the SIPTO execution unit;

[0032] the SIPTO execution unit is configured to determine whether implementing corresponding SIPTO communication according to the received judgment result.

[0033] The SIPTO execution unit may be further configured to implement corresponding SIPTO and/or CN communication according to the judgment result.

[0034] The device may further include a SIPTO capacity authorization unit, which is configured to authorize the SIPTO capacity of the H(e)NB and/or the UE, in order to make the authorization information referred by the authorization support the SIPTO capacity decision unit to implement the judgment.

[0035] The device may further include a security protection unit, which is configured to acquire current communication condition from the SIPTO execution unit, so as to determine whether implementing security protection for the current communication and executing the security protection.

[0036] It can be seen that the method and device of the disclosure can support the SIPTO of the H(e)NB.

BRIEF DESCRIPTION OF THE DRAWINGS

[0037] FIG. 1 is a HNB system structure diagram of the prior art;

[0038] FIG. 2 is a HeNB system structure diagram of the prior art;

[0039] FIG. 3 is a SIPTO decision flow sketch of the disclosure;

[0040] FIG. 4 is a SIPTO decision flowchart of embodiment one of the disclosure;

[0041] FIG. 5 is a SIPTO decision flowchart of embodiment two of the disclosure;

[0042] FIG. 6 is a SIPTO decision flowchart of embodiment three of the disclosure;

[0043] FIG. 7 is a SIPTO decision flowchart of embodiment four of the disclosure;

[0044] FIG. 8 is a SIPTO decision flowchart of embodiment five of the disclosure;

[0045] FIG. 9 is a SIPTO decision flowchart of embodiment six of the disclosure;

[0046] FIG. 10 is a SIPTO decision device diagram of an embodiment of the disclosure.

DETAILED DESCRIPTION

[0047] See FIG. 3, FIG. 3 is a SIPTO decision flow sketch of the disclosure, wherein the flow includes the steps as follows:

[0048] Step 301: an operator may authorize the SIPTO capacity of a H(e)NB before the H(e)NB is deployed.

[0049] For example, the operator can store the identity of the H(e)NB in the decision point which is used for judging whether the H(e)NB has the SIPTO authority, and add a SIPTO mark which is corresponding to the identity. The decision point which can be used for judging whether the H(e)NB has the SIPTO authority includes the SeGW, or a Service Gateway (SGW), or a Packet Data Gateway (PGW), or a Mobility Management Entity (MME), or a Mobile Switching Center (MSC), or a Serving General Packet Radio Service (GPRS) Support Node (SGSN), or a H(e)NB Gateway, or a Traffic Offload Function (TOF) entity, and the like.

[0050] Step 302: when the H(e)NB starts, the operator network implements successful mutual authentication with the H(e)NB, and judges whether the H(e)NB has the SIPTO authority; if yes, proceeds to Step 303; otherwise, proceeds to Step 310.

[0051] Specifically, when judging whether the H(e)NB has the SIPTO authority, the H(e)NB identity stored in the deci-

sion point which is used for judging whether the H(e)NB has the SIPTO authority can be searched; determines that the H(e)NB has the SIPTO authority if the found identity is added with the SIPTO mark; otherwise, determines that the H(e)NB has no SIPTO authority.

[0052] Step 303: the H(e)NB has the SIPTO authority, and the H(e)NB is allowed to implement the SIPTO, the H(e)NB implements the H(e)NB. Meanwhile, the H(e)NB can further establish a connection with the CN.

[0053] Step 304: judges whether the UE accessed to the H(e)NB can implement the SIPTO; if yes, proceeds to Step 305; otherwise, proceeds to Step 320.

[0054] Specifically, the H(e)NB firstly implements an UE registration, and notifies the UE that the H(e)NB has the SIPTO capacity, and can further authorize the SIPTO capacity of the UE; for example: stores the UE identity in a related network element for authenticating the UE, and adds the SIPTO mark which is corresponding to the identity. The UE identity stored in the related network element which is used for authenticating the UE can be searched when judging whether the UE can implement the SIPTO; determines that the UE can implement the SIPTO if the found identity is added with the SIPTO mark; otherwise, determines that the UE cannot implement the SIPTO.

[0055] Step 305: the UE implements the SIPTO or the UE can select whether implementing the SIPTO if the UE can implement the SIPTO. The UE does not implement the SIPTO if the UE selects not to implement the SIPTO. The UE can judge whether implementing the SIPTO according to the Quality of Service (QoS) and/or mobility requirements of the transmission data and the like.

[0056] When the UE selects to use the SIPTO, aiming at the data of the UE, the H(e)NB can implement a traffic transmission with the internet without passing through the CN, and/or directly implements the traffic transmission with the local network of the residents/companies without passing through the CN in the case that the local network of the residents/companies allows the SIPTO. The H(e)NB can judge whether implementing the SIPTO according to the QoS and/or mobility requirements of the transmission data and the like. And this flow ends.

[0057] Specifically, the traffic transmission without passing through the CN that implemented between the H(e)NB and internet and/or the local network of the residents/companies can be implemented via a local gateway; the local gateway can be combined with or separated from the H(e)NB. Additionally, the traffic among the H(e)NB, the internet and/or the local network of the residents/companies which is transmitted via the local gateway can be unprotected, or can be protected by adopting the network security protection modes such as IPsec and/or TLS and the like. Whether adopting the network security protection modes such as IPsec and/or TLS and the like is determined according to the operator requirements, or requirements such as the QoS and mobility requirements of the transmission data and the like.

[0058] Step 310: the H(e)NB is not allowed to implement the SIPTO, the H(e)NB establishes a connection with the CN. And this flow ends.

[0059] Step 320: the UE is not allowed to implement the SIPTO.

[0060] The above operation flow may perform different flows as shown in FIG. 4 to FIG. 9 under different application scenes.

[0061] See FIG. 4, FIG. 4 is a SIPTO decision flowchart of embodiment one of the disclosure; the flow includes the steps as follows:

[0062] Step 401: the operator authorizes the SIPTO capacity of the H(e)NB.

[0063] Step 402: the operator network implements successful mutual authentication with the H(e)NB, and judges whether the H(e)NB has the SIPTO authority.

[0064] Step 403: determines that the H(e)NB has no SIPTO authority, and the H(e)NB is not allowed to implement the SIPTO, the H(e)NB establishes a connection with the CN.

[0065] See FIG. 5, FIG. 5 is a SIPTO decision flowchart of embodiment two of the disclosure; the flow includes the steps as follows:

[0066] Step 501: the operator authorizes the SIPTO capacity of the H(e)NB.

[0067] Step 502: the operator network implements successful mutual authentication with the H(e)NB, and judges whether the H(e)NB has the SIPTO authority.

[0068] Step 503: determines that the H(e)NB has the SIPTO authority, and the H(e)NB is allowed to implement the SIPTO, the H(e)NB implements the SIPTO. Meanwhile, the H(e)NB can further establish a connection with the CN.

[0069] Step 504: the H(e)NB implements the UE registration, notifies the UE that the H(e)NB has the SIPTO capacity, judges that the UE cannot implement the SIPTO, and does not allow the UE to implement the SIPTO.

[0070] See FIG. 6, FIG. 6 is a SIPTO decision flowchart of embodiment three of the disclosure; the flow includes the steps as follows:

[0071] Step 601: the operator authorizes the SIPTO capacity of the H(e)NB.

[0072] Step 602: the operator network implements successful mutual authentication with the H(e)NB, and judges whether the H(e)NB has the SIPTO authority.

[0073] Step 603: determines that the H(e)NB has the SIPTO authority, and the H(e)NB is allowed to implement the SIPTO, the H(e)NB implements the SIPTO. Meanwhile, the H(e)NB can further establish a connection with the CN.

[0074] Step 604: the H(e)NB implements the UE registration, notifies the UE that the H(e)NB has the SIPTO capacity, and judges that the UE can implement the SIPTO.

[0075] Step 605: the UE selects not to implement the SIPTO.

[0076] See FIG. 7, FIG. 7 is a SIPTO decision flowchart of embodiment four of the disclosure; the flow includes the steps as follows:

[0077] Step 701: the operator authorizes the SIPTO capacity of the H(e)NB.

[0078] Step 702: the operator network implements successful mutual authentication with the H(e)NB, and judges whether the H(e)NB has the SIPTO authority.

[0079] Step 703: the H(e)NB has the SIPTO authority, and the H(e)NB is allowed to implement the SIPTO, the H(e)NB implements the SIPTO. Meanwhile, the H(e)NB can further establish a connection with the CN.

[0080] Step 704: the H(e)NB implements the UE registration, notifies the UE that the H(e)NB has the SIPTO capacity, and judges that the UE can implement the SIPTO.

[0081] Step 705: the UE selects to use the SIPTO, aiming at the data of the UE, the H(e)NB implements the SIPTO with the internet and/or directly implements the SIPTO with the local network of the residents/companies in the case that the local network of the residents/companies allows the SIPTO;

and the traffic among the H(e)NB, the internet and/or the local network of the residents/companies which is transmitted via the local gateway is unprotected.

[0082] See FIG. 8, FIG. 8 is a SIPTO decision flowchart of embodiment five of the disclosure; the flow includes the steps as follows:

[0083] Step 801: the operator authorizes the SIPTO capacity of the H(e)NB.

[0084] Step 802: the operator network implements successful mutual authentication with the H(e)NB, and judges whether the H(e)NB has the SIPTO authority.

[0085] Step 803: the H(e)NB has the SIPTO authority, the H(e)NB is allowed to implement the SIPTO, the H(e)NB implements the SIPTO. Meanwhile, the H(e)NB can further establish a connection with the CN.

[0086] Step 804: the H(e)NB implements the UE registration, notifies the UE that the H(e)NB has the SIPTO capacity, and judges that the UE can implement the SIPTO.

[0087] Step 805: the UE selects to use the SIPTO, aiming at the data of the UE, the H(e)NB implements the SIPTO with the internet and/or directly implements the SIPTO with the local network of the residents/companies in the case that the local network of the residents/companies allows the SIPTO; and the traffic among the H(e)NB, the internet and/or the local network of the residents/companies which is transmitted via the local gateway is protected by adopting the network security protection modes such as IPsec and/or TLS and the like.

[0088] See FIG. 9, FIG. 9 is a SIPTO decision flowchart of embodiment six of the disclosure; the flow includes the steps as follows:

[0089] Step 901: the operator authorizes the SIPTO capacity of the H(e)NB.

[0090] Step 902: the operator network implements successful mutual authentication with the H(e)NB, and judges whether the H(e)NB has the SIPTO authority.

[0091] Step 903: the H(e)NB has the SIPTO authority, the H(e)NB is allowed to implement the SIPTO, the H(e)NB implements the SIPTO. Meanwhile, the H(e)NB can further establish a connection with the CN.

[0092] Step 904: the H(e)NB implements the UE registration, notifies the UE that the H(e)NB has the SIPTO capacity, and judges that the UE can implement the SIPTO.

[0093] Step 905: aiming at the data of the UE, the H(e)NB implements the SIPTO with the internet and/or directly implements the SIPTO with the local network of the residents/companies in the case that the local network of the residents/companies allows the SIPTO; and the traffic among the H(e)NB, the internet and/or the local network of the residents/companies which is transmitted via the local gateway is unprotected, or is protected by adopting the network security protection modes such as IPsec and/or TLS and the like.

[0094] In order to guarantee the smooth implementation of the above flows, the device as shown in FIG. 10 can be arranged. See FIG. 10, FIG. 10 is a SIPTO decision device diagram of an embodiment of the disclosure; the device includes a SIPTO capacity authorization unit, a SIPTO capacity decision unit, a SIPTO execution unit and a security protection unit which are connected.

[0095] During specific application, the SIPTO capacity authorization unit can authorize the SIPTO capacity of the H(e)NB and the UE. The SIPTO capacity decision unit can acquire the authorization information in the SIPTO capacity authorization unit, so as to judge whether the H(e)NB and the

UE have the SIPTO authority, and notify the judgment result to the SIPTO execution unit; the SIPTO execution unit implements corresponding SIPTO and/or CN communication according to the received judgment result.

[0096] In addition, the SIPTO execution unit can further notify the current communication condition to the security protection unit; the security protection unit determines whether implementing security protection for the current communication and implements the security protection, for example: the traffic among the H(e)NB, the internet and/or the local network of the residents/companies which is transmitted via the local gateway can be unprotected, or be protected by adopting the network security protection modes such as IPsec and/or TLS and the like.

[0097] Additionally, the SIPTO capacity authorization unit and the SIPTO execution unit can be configured in a functional entity such as the H(e)NB and the like, the SIPTO capacity decision unit can be configured in functional entities such as the SeGW, the SGW, the PGW, the MME, the MSC, the SGSN, the H(e)NB Gateway or the TOF entity and the like.

[0098] The specific functions which can be realized by each operation unit in FIG. 10 are described in details in the above flows, and are not described again.

[0099] In conclusion, with both the method and the device, the SIPTO decision technology of the H(e)NB system provided by the disclosure can support the SIPTO of the H(e)NB, and can further provide a security protection in a communication process.

[0100] The above is only the preferred embodiment of the disclosure and not intended to limit the disclosure. Any modifications, equivalent replacements, improvements and the like within the spirit and principle of the disclosure shall fall within the scope of protection of the disclosure.

1. A Selected Internet Protocol Traffic Offload (SIPTO) decision method for a Home (evolved) Node-B (H(e)NB) system, comprising:

judging whether the H(e)NB has a SIPTO authority, and allowing the H(e)NB to implement the SIPTO if the H(e)NB has the SIPTO authority.

2. The method according to claim 1, wherein the process of judging whether the H(e)NB has the SIPTO authority comprises:

searching a H(e)NB identity stored in a decision point for judging whether the H(e)NB has the SIPTO authority, and confirming that the H(e)NB has the SIPTO authority if the H(e)NB identity is found, or the identity of the H(e)NB which is added with a SIPTO mark is found.

3. The method according to claim 2, wherein the method further comprises:

the H(e)NB implementing the SIPTO;
or, the H(e)NB implementing the SIPTO, and establishing a connection with a Core Network (CN).

4. The method according to claim 1, wherein the method further comprises:

judging whether a User Equipment (UE) can implement the SIPTO, and implementing the SIPTO aiming at the data of the UE when the UE can implement the SIPTO.

5. The method according to claim 4, wherein, the process of judging whether the UE can implement the SIPTO comprises:

searching a UE identity which is stored in a related network element for authenticating the UE, and determining that

the UE can implement the SIPTO if the UE identity is found, or the identity of the UE which is added with a SIPTO mark is found.

6. The method according to claim 4, wherein the method further comprises:

implementing network security protection comprising Internet Protocol (IP) Security (IPsec) and/or Transport Layer Security (TLS) for the transmission data of the H(e)NB and/or the UE.

7. A SIPTO decision method of a H(e)NB system, comprising: judging whether the UE can implement the SIPTO, and implementing the SIPTO aiming at the transmission data of the UE when the UE can implement the SIPTO.

8. The method according to claim 7, wherein, the process of judging whether the UE can implement the SIPTO comprises:

searching a UE identity which is stored in the related network element for authenticating the UE, and determining that the UE can implement the SIPTO if the UE identity is found, or the identity of the UE which is added with a SIPTO mark is found

9. The method according to claim 7, wherein, the method further comprises:

selecting, by the UE, to implement the SIPTO, aiming at the transmission data of the UE, implementing, by the H(e)NB accessed by the UE, the SIPTO with the internet, and/or implementing the SIPTO with the local network of residents/companies.

10. The method according to claim 9, wherein:

the SIPTO implemented by the H(e)NB is implemented in the case that the local network of the residents/companies allows the SIPTO; or,

the SIPTO implemented by the H(e)NB is directly implemented without allowing the SIPTO by the local network of the residents/companies.

11. The method according to claim 9, wherein the method further comprises:

not protecting the transmission data of the UE, or implementing the network security protection comprising the IPsec and/or TLS.

12. A SIPTO decision device of a H(e)NB system, comprising a SIPTO capacity decision unit and a SIPTO execution unit, wherein,

the SIPTO capacity decision unit is configured to judge whether the H(e)NB and/or the UE has the SIPTO authority, and to notify a judgment result to the SIPTO execution unit;

the SIPTO execution unit is configured to determine whether implementing corresponding SIPTO communication according to the received judgment result.

13. The device according to claim 12, wherein the SIPTO execution unit is further configured to implement corresponding SIPTO and/or CN communication according to the judgment result.

14. The device according to claim 12, wherein the device further comprises a SIPTO capacity authorization unit, which is configured to authorize the SIPTO capacity of the H(e)NB and/or the UE, in order to make the authorization information referred by the authorization support the SIPTO capacity decision unit to implement the judgment.

15. The device according to claim 12, wherein the device further comprises a security protection unit, which is configured to acquire current communication condition from the SIPTO execution unit, so as to determine whether implement-

ing security protection for the current communication and executing the security protection.

16. The method according to claim 2, wherein the method further comprises:

judging whether a User Equipment (UE) can implement the SIPTO, and implementing the SIPTO aiming at the data of the UE when the UE can implement the SIPTO.

17. The method according to claim 3, wherein the method further comprises:

judging whether a User Equipment (UE) can implement the SIPTO, and implementing the SIPTO aiming at the data of the UE when the UE can implement the SIPTO.

18. The method according to claim 16, wherein, the process of judging whether the UE can implement the SIPTO comprises:

searching a UE identity which is stored in a related network element for authenticating the UE, and determining that the UE can implement the SIPTO if the UE identity is found, or the identity of the UE which is added with a SIPTO mark is found.

19. The method according to claim 17, wherein, the process of judging whether the UE can implement the SIPTO comprises:

searching a UE identity which is stored in a related network element for authenticating the UE, and determining that the UE can implement the SIPTO if the UE identity is found, or the identity of the UE which is added with a SIPTO mark is found.

20. The method according to claim 16, wherein the method further comprises:

implementing network security protection comprising Internet Protocol (IP) Security (IPsec) and/or Transport Layer Security (TLS) for the transmission data of the H(e)NB and/or the UE.

21. The method according to claim 17, wherein the method further comprises:

implementing network security protection comprising Internet Protocol (IP) Security (IPsec) and/or Transport Layer Security (TLS) for the transmission data of the H(e)NB and/or the UE.

22. The method according to claim 8, wherein, the method further comprises:

selecting, by the UE, to implement the SIPTO, aiming at the transmission data of the UE, implementing, by the H(e)NB accessed by the UE, the SIPTO with the internet, and/or implementing the SIPTO with the local network of residents/companies.

23. The method according to claim 22, wherein: the SIPTO implemented by the H(e)NB is implemented in the case that the local network of the residents/companies allows the SIPTO; or,

the SIPTO implemented by the H(e)NB is directly implemented without allowing the SIPTO by the local network of the residents/companies.

24. The method according to claim 22, wherein the method further comprises:

not protecting the transmission data of the UE, or implementing the network security protection comprising the IPsec and/or TLS.

25. The device according to claim 13, wherein the device further comprises a SIPTO capacity authorization unit, which is configured to authorize the SIPTO capacity of the H(e)NB and/or the UE, in order to make the authorization information referred by the authorization support the SIPTO capacity decision unit to implement the judgment.

26. The device according to claim 13, wherein the device further comprises a security protection unit, which is configured to acquire current communication condition from the SIPTO execution unit, so as to determine whether implementing security protection for the current communication and executing the security protection.

* * * * *