(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 101854625 B
(45)授权公告日 2014.12.03

(21)申请号 200910081161.7
(22)申请日 2009.04.03
(73)专利权人 华为技术有限公司
地址 518129 广东省深圳市龙岗区坂田华为总部办公楼
(72)发明人 张爱琴 陈璟 杨义
(74)专利代理机构 北京同立钧成知识产权代理有限公司 11205
代理人 刘芳
(51)Int.Cl.
H04W 12/02(2009.01)
H04W 28/06(2009.01)
H04W 28/18(2009.01)

(56)对比文件
CN 101378591 A,2009.03.04,
CN 101378591 A,2009.03.04,
CN 101170811 A,2008.04.30,
CN 101170811 A,2008.04.30,
EP 1729449 A1,2006.12.06,

审查员 王朝英

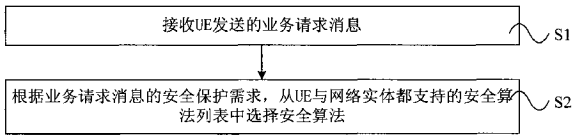
权利要求书7页 说明书21页 附图16页

(54)发明名称

安全算法选择处理方法与装置、网络实体及通信系统

(57)摘要

本发明实施例公开了一种安全算法选择处理方法与装置、网络实体及通信系统，其中，方法包括：接收用户终端发送的业务请求消息；根据业务请求消息的安全保护需求，从用户终端与网络实体都支持的安全算法列表中选择安全算法；用户终端和/或网络实体支持的安全算法列表基于不同的安全保护需求分别设置，或者，用户终端与网络实体支持的安全算法列表分别用于表示用户终端与网络实体的安全能力。本发明实施例可以根据不同业务请求消息的安全保护需求选择不同的安全算法，以对相应的业务进行不同的安全保护，提高了业务的安全性，综合考虑了通信系统中各算法的复杂度与占用的开销，在对业务进行有效安全保护的同时提高通信系统的性能。



CN 101854625 B

1. 一种安全算法选择处理方法，其特征在于，包括：

网络实体接收用户终端发送的业务请求消息；

所述网络实体根据所述业务请求消息的安全保护需求，从所述用户终端与网络实体都支持的安全算法列表中选择安全算法；

其中，所述用户终端和/或所述网络实体支持的安全算法列表基于不同的安全保护需求分别设置，或者，所述用户终端与所述网络实体支持的安全算法列表分别用于表示所述用户终端与所述网络实体的安全能力；

所述安全保护需求包括：数据类型、业务类型和用户需求中的任意一种或多种；

所述网络实体从所述用户终端与网络实体都支持的安全算法列表中选择安全算法包括：从所述用户终端与网络实体都支持的且应用服务器存储的安全算法列表中选择安全算法，所述应用服务器支持的安全算法列表基于不同的安全保护需求分别设置；或者，

所述网络实体接收用户终端发送的业务请求消息之后，所述网络实体向所述用户终端返回所述网络实体支持的安全算法列表、该安全算法列表中与所述安全保护需求对应的安全算法列表、所述网络实体支持的安全算法选择策略或安全算法选择策略标识，该安全算法选择策略基于所述网络实体支持的安全算法列表设置，以便所述用户终端根据所述业务请求消息的安全保护需求，从所述用户终端与网络实体都支持的安全算法列表中选择安全算法，具体包括：所述用户终端根据所述应用服务器存储的安全算法列表、所述安全保护需求对应的安全算法列表、安全算法选择策略或安全算法选择策略标识，与所述网络实体支持的安全算法列表、所述安全保护需求对应的安全算法列表、所述网络实体支持的安全算法选择策略或安全算法选择策略标识，从所述用户终端与所述网络实体都支持且所述应用服务器存储的安全算法列表中，选择所述安全保护需求对应的安全算法， 所述安全算法选择策略基于安全保护需求设置。

2. 根据权利要求 1 所述的方法，其特征在于，所述网络实体预先存储所述用户终端支持的且应用服务器存储的安全算法列表；相应的，所述网络实体根据所述业务请求消息的安全保护需求，从所述用户终端与网络实体都支持的安全算法列表中选择安全算法具体包括：所述网络实体从所述用户终端与所述网络实体都支持的安全算法列表中选择所述安全保护需求对应的安全算法。

3. 根据权利要求 1 所述的方法，其特征在于，所述业务请求消息中包括所述用户终端选择的安全算法列表，该安全算法列表由所述用户终端从所述用户终端支持的安全算法列表与所述应用服务器存储的安全算法列表、该安全算法列表中所述安全保护需求对应的安全算法列表、安全算法选择策略或安全算法选择策略标识选择，为所述用户终端支持且所述应用服务器存储的安全算法列表或所述用户终端支持且所述应用服务器存储的、所述安全保护需求对应的安全算法列表；

所述网络实体根据所述业务请求消息的安全保护需求，从所述用户终端与网络实体都支持的安全算法列表中选择安全算法具体包括：所述网络实体根据所述业务请求消息中的安全算法列表，从所述用户终端支持且所述应用服务器存储的安全算法列表以及所述网络实体支持的安全算法列表中，选择所述安全保护需求对应的安全算法；或者，所述网络实体根据所述业务请求消息中所述用户终端支持且所述应用服务器存储的、所述安全保护需求对应的安全算法列表与所述网络实体支持的、所述安全保护需求对应的安全算法列表中，

选择所述安全保护需求对应的安全算法。

4. 根据权利要求 1 所述的方法，其特征在于，所述业务请求消息中包括所述用户终端支持的安全算法列表或所述安全保护需求对应的安全算法列表，与所述应用服务器存储的安全算法列表、所述安全保护需求对应的安全算法列表、安全算法选择策略或安全算法选择策略标识；

所述网络实体根据所述业务请求消息的安全保护需求，从所述用户终端与网络实体都支持的安全算法列表中选择安全算法包括：所述网络实体根据所述业务请求消息中所述用户终端支持的安全算法列表或所述安全保护需求对应的安全算法列表，与所述应用服务器存储的安全算法列表、所述安全保护需求对应的安全算法列表、安全算法选择策略或安全算法选择策略标识，与所述网络实体支持的安全算法列表或所述安全保护需求对应的安全算法列表，选择所述安全保护需求对应的安全算法。

5. 根据权利要求 1 所述的方法，其特征在于，所述业务请求消息中包括所述用户终端支持的安全算法列表或该安全算法列表中与所述安全保护需求对应的安全算法列表；

所述接收用户终端发送的业务请求消息之后，还包括：所述网络实体获取所述应用服务器存储的安全算法列表、该安全算法列表中与所述安全保护需求对应的安全算法列表、安全算法选择策略或安全算法选择策略标识，该安全算法选择策略基于安全保护需求设置；

所述网络实体根据所述业务请求消息的安全保护需求，从所述用户终端与网络实体都支持的安全算法列表中选择安全算法包括：所述网络实体从所述用户终端与所述网络实体都支持且所述应用服务器存储的安全算法列表中，选择所述安全保护需求对应的安全算法；或者，所述网络实体根据所述应用服务器存储的安全算法选择策略、或所述安全算法选择策略标识所标识的安全算法选择策略，从所述用户终端与所述网络实体都支持且所述应用服务器存储的与所述安全保护需求对应的安全算法列表中，选择所述安全保护需求对应的安全算法。

6. 根据权利要求 1 至 5 任意一项所述的方法，其特征在于，所述安全保护需求包括：数据类型对应的安全保护级别需求或安全算法列表、业务类型对应的安全保护级别需求或安全算法列表或安全算法策略、与用户需求中的任意一种或多种，其中业务类型对应的安全算法策略用于表示所述业务 类型在不同条件下的安全保护级别需求。

7. 根据权利要求 1 至 5 任意一项所述的方法，其特征在于，所述网络实体为演进基站 eNB；所述业务请求消息为 RRC 请求消息或 UP 的用户数据；所述接收用户终端发送的业务请求消息包括：eNB 接收用户终端发送的 RRC 请求消息或 UP 的用户数据；或者

所述网络实体为移动性管理实体 MME；所述业务请求消息为 NAS 请求消息；所述接收用户终端发送的业务请求消息包括：MME 接收由 eNB 转发的、由所述用户终端发送的 NAS 请求消息。

8. 根据权利要求 1 至 5 任意一项所述的方法，其特征在于，所述用户终端的安全能力包括：为不同数据类型或者不同安全保护层次提供该用户终端支持的、不同的安全保护算法列表；

所述网络实体的安全能力包括：为不同数据类型或者不同安全保护层次提供该网络实体支持的、不同的安全保护算法列表。

9. 根据权利要求1至5任意一项所述的方法，其特征在于，从所述用户终端与网络实体都支持的且应用服务器存储的安全算法列表中选择安全算法包括：从所述用户终端与网络实体都支持的安全算法列表中，按照优先级顺序选择安全算法。

10. 一种安全算法选择处理装置，其特征在于，包括：

第一获取模块，用于获取用户终端发送的业务请求消息的安全保护需求；

第一选择模块，用于根据所述业务请求消息的安全保护需求，从所述用户终端与网络实体都支持的安全算法列表中选择安全算法；所述用户终端和/或所述网络实体支持的安全算法列表基于不同的安全保护需求分别设置，或者，所述用户终端与所述网络实体支持的安全算法列表分别用于表示所述用户终端与所述网络实体的安全能力；

所述安全保护需求包括：数据类型、业务类型和用户需求中的任意一 种或多种；

则所述第一选择模块包括：第一获取单元和第一选择单元；

所述第一获取单元还用于获取应用服务器存储的安全算法列表、所述安全保护需求对应的安全算法列表、安全算法选择策略或安全算法选择策略标识，该安全算法选择策略基于安全保护需求设置，所述应用服务器存储的安全算法列表基于不同的安全保护需求分别设置；

所述第一选择单元根据所述第一获取单元从所述用户终端获取的安全算法列表，与分别从所述网络实体和应用服务器获取的安全算法列表、安全算法选择策略或安全算法选择策略标识，选择所述安全保护需求对应的安全算法。

11. 根据权利要求10所述的装置，其特征在于，

所述第一获取单元还用于获取所述用户终端支持的安全算法列表或该安全算法列表中与所述安全保护需求对应的安全算法列表，与所述网络实体支持的安全算法列表、该安全算法列表中与所述安全保护需求对应的安全算法列表、安全算法选择策略、或安全算法选择策略标识，该安全算法选择策略基于所述网络实体支持的安全算法列表设置，所述用户终端和/或所述网络实体支持的安全算法列表基于不同的安全保护需求分别设置；

所述第一选择单元还用于根据所述第一获取单元从所述用户终端获取的安全算法列表，与从所述网络实体和应用服务器获取的安全算法列表、安全算法选择策略、或安全算法选择策略标识，选择所述安全保护需求对应的安全算法。

12. 一种通信系统，包括网络实体，其特征在于，还包括安全算法选择处理装置，用于获取用户终端发送的业务请求消息的安全保护需求，并根据所述业务请求消息对应的安全保护需求，从所述用户终端与所述网络实体都支持的且应用服务器存储的安全算法列表中选择安全算法；所述用户终端和/或所述网络实体支持的安全算法列表基于不同的安全保护需求 分别设置，或者，所述用户终端与所述网络实体支持的安全算法列表分别用于表示所述用户终端与所述网络实体的安全能力；所述安全保护需求包括：数据类型、业务类型和用户需求中的任意一种或多种；

应用服务器，用于存储安全算法列表、安全算法选择策略或安全算法选择策略标识，所述安全算法选择策略基于安全保护需求设置，所述应用服务器存储的安全算法列表基于不同的安全保护需求分别设置；

所述安全算法选择处理装置还用于获取应用服务器存储的安全算法列表、安全算法选择策略或安全算法选择策略标识，根据从所述用户终端获取的安全算法列表，与分别从所

述网络实体和应用服务器获取的安全算法列表、安全算法选择策略或安全算法选择策略标识，选择所述安全保护需求对应的安全算法，所述网络实体的安全算法选择策略基于所述网络实体支持的安全算法列表设置。

13. 一种用户终端，其特征在于，包括：

第一存储模块，用于存储所述用户终端支持的安全算法列表，该安全算法列表基于不同的安全保护需求分别设置或者用于表示所述用户终端的安全能力；

第二获取模块，用于从所述第一存储模块中获取安全算法列表，或查询业务请求消息的安全保护需求，从所述第一存储模块中获取该安全保护需求对应的安全算法列表；

第一发送模块，用于生成并向网络实体发送业务请求消息，所述业务请求消息中包括所述第二获取模块获取的安全算法列表；

第一接收模块，用于接收所述网络实体返回的安全算法，所述安全算法根据所述业务请求消息的安全保护需求，从所述用户终端与网络实体都支持的安全算法列表中选择；

所述安全保护需求包括：数据类型、业务类型和用户需求中的任意一 种或多种；

第三获取模块，用于获取应用服务器存储的安全算法列表、所述安全保护需求对应的安全算法列表、安全算法选择策略或安全算法选择策略标识，该安全算法选择策略基于安全保护需求设置；

所述第二获取模块包括：

第二获取单元，用于从所述第一存储模块中获取安全算法列表，或查询所述业务请求消息的安全保护需求，从所述第一存储模块中获取该安全保护需求对应的安全算法列表；

第二选择单元，用于根据所述第二获取单元从所述第一存储模块中存储的安全算法列表，与所述第三获取模块从所述应用服务器获取的安全算法列表、安全算法选择策略或安全算法选择策略标识，选择所述用户终端支持且所述应用服务器存储的安全算法列表，或所述用户终端支持且所述应用服务器存储的安全算法列表中与所述安全保护需求对应的安全算法列表；

所述业务请求消息的安全算法列表包括所述第二选择单元选择的安全算法列表。

14. 一种网络实体，其特征在于，包括：

第二存储模块，用于存储所述网络实体支持的安全算法列表或安全算法选择策略，所述安全算法列表基于不同的安全保护需求分别设置或者用于表示所述网络实体的安全能力，所述安全算法选择策略基于所述网络实体支持的安全算法列表设置；

第二接收模块，用于接收用户终端发送的业务请求消息，该业务请求消息中包括所述用户终端支持的安全算法列表；

第四获取模块，用于获取应用服务器存储的安全算法列表、该安全算法列表中所述安全保护需求对应的安全算法列表、安全算法选择策略或安全算法选择策略标识，该安全算法选择策略基于安全保护需求设置，所述 应用服务器支持的安全算法列表基于不同的安全保护需求分别设置；

第二选择模块，用于根据所述第二存储模块中存储的安全算法列表或安全算法选择策略，所述业务请求消息中的安全算法列表，与所述应用服务器存储的安全算法列表、所述安全保护需求对应的安全算法列表、安全算法选择策略或安全算法选择策略标识，选择所述安全保护需求对应的安全算法；

第二发送模块，用于将所述第二选择模块选择的安全算法发送给所述用户终端；

所述安全保护需求包括：数据类型、业务类型和用户需求中的任意一种或多种；

所述业务请求消息中的安全算法列表包括所述用户终端支持的、所述安全保护需求对应的安全算法列表。

15. 一种通信系统，包括网络实体，其特征在于，所述网络实体中存储有该网络实体支持的安全算法列表或安全算法选择策略，该安全算法列表基于不同的安全保护需求分别设置或用于表示该网络实体的安全能力，所述安全算法选择策略基于所述网络实体支持的安全算法列表设置；

所述网络实体用于接收用户终端发送的业务请求消息，该业务请求消息中包括所述用户终端支持的安全算法列表或所述业务请求消息的安全保护需求所对应的安全算法列表，所述网络实体根据所述网络实体支持的安全算法列表或安全算法选择策略，与所述业务请求消息中携带的安全算法列表，选择所述用户终端与所述网络实体都支持且应用服务器存储的、所述安全保护需求对应的安全算法，并将选择的安全算法发送给所述用户终端；其中，所述业务请求消息中携带的安全算法列表为所述用户终端从所述应用服务器获取的安全算法列表、该安全算法列表与所述安全保护需求对应的安全算法列表、安全算法选择策略或安全算法选择策略标识，或者，为所述用户终端支持且所述应用服务器存储的安全算法列表或 所述安全保护需求对应的安全算法列表；

所述安全保护需求包括：数据类型、业务类型和用户需求中的任意一种或多种；

应用服务器，用于存储该应用服务器的安全算法列表、安全算法选择策略或安全算法选择策略标识，所述安全算法选择策略基于安全保护需求设置，所述应用服务器存储的安全算法列表基于不同的安全保护需求分别设置，并根据所述用户终端发送的获取请求消息，向所述用户终端返回所述应用服务器存储的安全算法列表、安全算法选择策略或安全算法选择策略标识。

16. 一种用户终端，其特征在于，包括：

第一存储模块，用于存储所述用户终端支持的安全算法列表，该安全算法列表基于不同的安全保护需求分别设置或用于表示所述用户终端的安全能力；

第一发送模块，用于生成并向网络实体发送业务请求消息；

第一接收模块，用于接收所述网络实体返回的安全算法列表、安全算法选择策略或安全算法选择策略标识，所述安全算法列表为所述网络实体支持的安全算法列表或该安全算法列表中与所述业务请求消息的安全保护需求对应的安全算法列表，所述安全算法选择策略基于所述网络实体支持的安全算法列表设置；

第三获取模块，用于获取应用服务器存储的安全算法列表、该安全算法列表中与所述安全保护需求对应的安全算法列表、安全算法选择策略或安全算法选择策略标识，该安全算法选择策略基于安全保护需求设置；

第三选择模块，用于根据所述第一存储模块中存储的安全算法列表，与所述第三获取模块获取到的安全算法列表、安全算法选择策略或安全算法选择策略标识，与所述第一接收模块接收到的安全算法列表、安全算法选择策略或安全算法选择策略标识，选择所述用户终端与所述网络实体都 支持且所述应用服务器存储的、所述安全保护需求对应的安全算法；

所述安全保护需求包括：数据类型、业务类型和用户需求中的任意一种或多种。

17. 一种网络实体，其特征在于，包括：

第二存储模块，用于存储所述网络实体支持的安全算法列表、安全算法选择策略或安全算法选择策略标识，所述安全算法列表基于不同的安全保护需求分别设置或用于表示所述网络实体的安全能力，所述安全算法选择策略基于所述网络实体支持的安全算法列表设置；

第二接收模块，用于接收用户终端发送的业务请求消息；

第四获取模块，用于获取应用服务器存储的安全算法列表、该安全算法列表中与所述安全保护需求对应的安全算法列表、安全算法选择策略或安全算法选择策略标识，该安全算法选择策略基于安全保护需求设置，所述应用服务器支持的安全算法列表基于不同的安全保护需求分别设置；

第二选择模块，用于根据所述第二存储模块中存储的安全算法列表或安全算法选择策略，与所述第四获取模块获取的所述应用服务器的安全算法列表、所述安全保护需求对应的安全算法列表、安全算法选择策略或安全算法选择策略标识，选择所述网络实体支持且所述应用服务器存储的安全算法列表、所述安全保护需求对应的安全算法列表、安全算法选择策略或安全算法选择策略标识；

第四发送模块，用于将所述第二存储模块中存储的安全算法列表或安全算法选择策略，与所述第四获取模块获取的所述应用服务器存储的安全算法列表、所述安全保护需求对应的安全算法列表、安全算法选择策略或安全算法选择策略标识发送给所述用户终端，或者将所述第二选择模块选择的安全算法列表、所述安全保护需求对应的安全算法列表、安全算法选择策略或安全算法选择策略标识发送给所述用户终端；

所述安全保护需求包括：数据类型、业务类型和用户需求中的任意一 种或多种。

18. 一种通信系统，包括网络实体，其特征在于，所述网络实体中存储有该网络实体支持的安全算法列表、安全算法选择策略或安全算法选择策略标识，所述安全算法列表基于不同的安全保护需求分别设置相应表示用户终端或所述网络实体的安全能力，所述安全算法选择策略基于所述网络实体支持的安全算法列表设置；

应用服务器，用于存储安全算法列表、安全算法选择策略或安全算法选择策略标识，所述安全算法选择策略基于安全保护需求设置，并根据所述网络实体发送的获取请求消息，向所述网络实体返回所述应用服务器存储的安全算法列表、安全算法选择策略或安全算法选择策略标识；

所述网络实体用于接收所述用户终端发送的业务请求消息，或者将所述网络实体存储的安全算法列表、所述安全保护需求对应的安全算法列表、安全算法选择策略或安全算法选择策略标识，以及通过所述获取请求消息获取的所述应用服务器存储的安全算法列表、该安全算法列表中与所述安全保护需求对应的安全算法列表、安全算法选择策略或安全算法选择策略标识，发送给所述用户终端，或者选择所述网络实体支持且所述应用服务器存储的安全算法列表、所述安全保护需求对应的安全算法列表、安全算法选择策略或安全算法选择策略标识，并发送给所述用户终端，以便所述用户终端根据该用户终端存储的安全算法列表，与所述网络实体返回的安全算法列表、安全算法选择策略或安全算法选择策略标识，选择所述安全保护需求对应的安全算法；

所述安全保护需求包括：数据类型、业务类型和用户需求中的任意一种或多种。

安全算法选择处理方法与装置、网络实体及通信系统

技术领域

[0001] 本发明涉及通信技术，尤其是一种安全算法选择处理方法与装置、网络实体及通信系统。

背景技术

[0002] 长期演进 (Long Term Evolve，以下简称 :LTE) 是由第三代合作伙伴计划 (Third Generation Partnership Project，以下简称 :3GPP) 定义的移动宽带网络标准的下一个演进目标，支持在成对频谱和非成对频谱上的运行，可实现对现有和未来的无线频带的高效利用。如图 1 所示，为作为 LTE 系统中接入网部分的演进的通用移动电信系统陆地无线接入网 (Evolved UMTSTerrestrial Radio Access Network，以下简称 :E-UTRAN) 的结构示意图。演进基站 (Evolved NodeB，以下简称 :eNB) 之间通过 X2 接口实现数据和信令的交互。eNB 通过 S1 接口连接到演变分组核心 (Evolved Packet Core，以下简称 :EPC) 网络中的移动性管理实体 (Mobility Management Entity，以下简称 :MME)。eNB 通过 S1 接口连接到服务网关 (Serving Gateway，以下简称 :S-GW)。

[0003] 如图 2 所示，为 LTE 系统架构演进 (LTE System Architecture Evolution，以下简称 :LTE-SAE) 系统的安全架构示意图。该 LTE-SAE 系统中，具有如下两层安全保护 :一层是用户终端 (User Equipment，以下简称 :UE) 与 eNB 之间的接入层 (Access Stratum，以下简称 :AS)，主要用于对 UE 与 eNB 之间的无线资源控制 (Radio Resource Control，以下简称 :RRC) 信令和用户面 (User Plane，以下简称 :UP) 的用户数据进行安全保护，包括 RRC 信令的加密保护和完整性保护以及 UP 的用户数据的加密 ;另一层是 UE 和 MME 之间的非接入层 (Non Access Stratum，以下简称 :NAS)，主要用于对 UE 和 MME 之间的 NAS 信令进行安全保护，包括 :NAS 信令的加密保护和完整性保护。

[0004] 在 LTE-SAE 系统中，UE 的能力包括 UE 空口能力 (UE radio capability) 和 UE 网络能力 (UE network capability)。其中，UE 空口能力使用在 UE 与 eNB 之间，主要体现在 UE 对于 AS 所支持的 AS 安全算法列表，假设该 AS 安全算法列表中算法的集合表示为 {A}。UE 网络能力使用在 UE 与 MME 之间，包含了 UE 在 NAS 的安全能力，体现在对于 NAS 所支持的 NAS 安全算法的列表，假设该 NAS 安全算法列表中算法的集合表示为 {B}。从 AS 与 NAS 的安全模式启动成功后启动对数据和信令的安全保护。启动 AS 与 NAS 的安全模式时，UE 分别向网络实体 eNB、MME 上报 AS 安全算法 {A} 与 NAS 安全算法 {B} ;假设表示 eNB 自身安全算法支持能力的安全算法列表为 {a}，表示 MME 自身安全算法支持能力的安全算法列表为 {b}，eNB 从 {{A} ∩ {a}} 中选择 AS 的安全算法，包括 :RRC 加密算法，即 :演进的分组系统 (EvolvedPacket System，以下简称 :EPS)AS 信令加密算法 (EPS AS EncryptionAlgorithm，以下简称 :EAEA)，RRC 完整性保护算法，即 :EPS AS 信令完整性保护算法 (EPS AS Integrity Algorithm，以下简称 :EAIA)，和用户面加密算法，即 :EPS 用户面加密算法 (EPS User-plan Encryption Algorithm，以下简称 :EUEA)，MME 从 {{B} ∩ {b}} 中选择 NAS 的安全算法，包括 EPSNAS 加密算法 (EPS NAS Encryption Algorithm，以下简称 :ENEA)，和 EPSNAS 完整性

保护算法(EPS NAS Integrity Algorithm,以下简称:ENIA)。

[0005] 在实现本发明的过程中,发明人发现选择AS安全算法与NAS的安全算法的现有技术至少存在以下问题:

[0006] UE中的AS安全算法列表与NAS安全算法列表相同,也即:集合{A}=集合{B},当UE中的AS安全算法列表包含eNB的安全算法列表、UE中的NAS安全算法列表包含MME的安全算法列表时,也即:{a}包含于{A}、集合{b}包含于{B}时,eNB选择的AS的安全算法与MME选择的NAS的安全算法可能相同;并且,UE中的AS安全算法列表包括了RRC信令的安全算法和UP的安全算法,因此,根据现有技术选择的RRC信令的安全算法和UP的安全算法完全相同。在LTE-SAE系统中,UE与网络实体支持的安全算法可能会有多种,不同安全算法的复杂度与开销有所不同。一般而言,安全级别越高的算法其复杂度与开销越大。不同的数据类型、业务类型与用户需求可能需要不同的安全算法,甚至不需要进行安全保护,因此,没必要针对所有的业务均采用相同的安全算法。但是,现有技术中网络实体eNB、MME无法基于不同的数据类型、业务类型与用户需求来选择相应的AS的安全算法与NAS的安全算法,因此,无法根据不同的数据类型、业务类型与用户需求对相应的业务进行不同的安全保护。

发明内容

[0007] 本发明实施例的目的是:提供一种安全算法选择处理方法与装置、网络实体及通信系统,以针对不同的业务选择不同的安全算法进行安全保护。

[0008] 本发明实施例提供的一种安全算法选择处理方法,包括:

[0009] 接收用户终端发送的业务请求消息;

[0010] 根据该业务请求消息的安全保护需求,从该用户终端与网络实体都支持的安全算法列表中选择安全算法;

[0011] 其中,该用户终端和/或该网络实体支持的安全算法列表基于不同的安全保护需求分别设置,或者,该用户终端与该网络实体支持的安全算法列表分别用于表示该用户终端与该网络实体的安全能力。

[0012] 本发明实施例提供的一种安全算法选择处理装置,包括:

[0013] 第一获取模块,用于获取用户终端发送的业务请求消息的安全保护需求;

[0014] 第一选择模块,用于根据该业务请求消息的安全保护需求,从该用户终端与网络实体都支持的安全算法列表中选择安全算法;该用户终端和/或该网络实体支持的安全算法列表基于不同的安全保护需求分别设置,或者,该用户终端与该网络实体支持的安全算法列表分别用于表示该用户终端与该网络实体的安全能力。

[0015] 本发明实施例提供的一种通信系统,包括网络实体,还包括安全算法选择处理装置,用于获取该用户终端发送的业务请求消息的安全保护需求,并根据该业务请求消息对应的安全保护需求,从该用户终端与该网络实体都支持的安全算法列表中选择安全算法;该用户终端和/或该网络实体支持的安全算法列表基于不同的安全保护需求分别设置,或者,该用户终端与该网络实体支持的安全算法列表分别用于表示该用户终端与该网络实体的安全能力。

[0016] 基于本发明上述实施例提供的安全算法选择处理方法、安全算法选择处理装置与

通信系统，由于用户终端和 / 或网络实体，例如 :eNB、MME，支持的安全算法列表基于不同的安全保护需求分别设置，可以根据不同业务请求消息的安全保护需求选择不同的安全算法，以对相应的业务进行不同的安全保护，不但提高了业务的安全性，还可以综合考虑通信系统中各算法的复杂度与占用的开销，在对业务进行有效安全保护的同时提高通信系统的性能。

[0017] 本发明实施例提供的一种用户终端，包括 :

[0018] 第一存储模块，用于存储该用户终端支持的安全算法列表，该安全算法列表基于不同的安全保护需求分别设置或者用于表示该用户终端的安全能力 ;

[0019] 第二获取模块，用于从该第一存储模块中获取安全算法列表，或查询该业务请求消息的安全保护需求，从该第一存储模块中获取该安全保护需求对应的安全算法列表 ;

[0020] 第一发送模块，用于生成并向网络实体发送业务请求消息，该业务请求消息中包括该第二获取模块获取的安全算法列表 ;

[0021] 第一接收模块，用于接收该网络实体返回的安全算法，该安全算法根据该业务请求消息的安全保护需求，从该用户终端与网络实体都支持的安全算法列表中选择。

[0022] 本发明实施例提供的一种网络实体，包括 :

[0023] 第二存储模块，用于存储该网络实体支持的安全算法列表或安全算法选择策略，该安全算法列表基于不同的安全保护需求分别设置或者用于表示该网络实体的安全能力，该安全算法选择策略基于该网络实体支持的安全算法列表设置 ;

[0024] 第二接收模块，用于接收用户终端发送的业务请求消息，该业务请求消息中包括该用户终端支持的安全算法列表 ;

[0025] 第二选择模块，用于根据该第二存储模块中存储的安全算法列表或安全算法选择策略，与该业务请求消息中的安全算法列表，从该用户终端与该网络实体都支持的安全算法列表中选择该安全保护需求对应的安全算法 ;

[0026] 第二发送模块，用于将该第二选择模块选择的安全算法发送给该用户终端。

[0027] 本发明实施例提供的另一种通信系统，包括网络实体，该网络实体中存储有该网络实体支持的安全算法列表或安全算法选择策略，该安全算法列表基于不同的安全保护需求分别设置或用于表示该网络实体的安全能力，该安全算法选择策略基于该网络实体支持的安全算法列表设置 ;

[0028] 该网络实体用于接收该用户终端发送的业务请求消息，该业务请求消息中包括该用户终端支持的安全算法列表或该业务请求消息的安全保护需求所对应的安全算法列表，根据该网络实体支持的安全算法列表或安全算法选择策略，与该业务请求消息中携带的安全算法列表，从该用户终端与该网络实体都支持的安全算法列表中选择该安全保护需求对应的安全算法，并将选择的安全算法发送给该用户终端。

[0029] 基于本发明上述实施例提供的用户终端、网络实体与另一种通信系统，由于用户终端和 / 或网络实体，支持的安全算法列表基于不同的安全保护需求分别设置，用户终端将其支持的全部安全算法列表或与业务请求消息的安全保护需求相应的安全算法列表发送给网络实体后，网络实体就可以从用户终端与该网络实体支持的安全算法中选择业务请求消息的安全保护需求相应的安全算法，以便后续对该业务进行相应的安全保护，提高了业务的安全性 ;另外，还可以综合考虑通信系统中各算法的复杂度与占用的开销，在对业务

进行有效安全保护的同时提高通信系统的性能。

[0030] 本发明实施例提供的另一种用户终端，包括：

[0031] 第一存储模块，用于存储该用户终端支持的安全算法列表，该安全算法列表基于不同的安全保护需求分别设置或用于表示该用户终端的安全能力；

[0032] 第一发送模块，用于生成并向网络实体发送业务请求消息；

[0033] 第一接收模块，用于接收该网络实体返回的安全算法列表、安全算法选择策略或安全算法选择策略标识，该安全算法列表为该网络实体支持的安全算法列表或该安全算法列表中与该业务请求消息的安全保护需求对应的安全算法列表，该安全算法选择策略基于该网络实体支持的安全算法列表设置；

[0034] 第三选择模块，用于根据该第一存储模块中存储的安全算法列表，与该第一接收模块接收到的安全算法列表，从该用户终端与该网络实体都支持的安全算法列表中选择该安全保护需求对应的安全算法。

[0035] 本发明实施例提供的另一种网络实体，包括：

[0036] 第二存储模块，用于存储该网络实体支持的安全算法列表、安全算法选择策略或安全算法选择策略标识，该安全算法列表基于不同的安全保护需求分别设置或用于表示该网络实体的安全能力，该安全算法选择策略基于该网络实体支持的安全算法列表设置；

[0037] 第二接收模块，用于接收用户终端发送的业务请求消息；

[0038] 第四发送模块，用于将该第二存储模块中存储的安全算法列表、该业务请求消息的安全保护需求对应的安全算法列表、安全算法选择策略或安全算法选择策略标识发送给该用户终端。

[0039] 本发明实施例提供的又一种通信系统，包括网络实体，该网络实体中存储有该网络实体支持的安全算法列表、安全算法选择策略或安全算法选择策略标识，该安全算法列表基于不同的安全保护需求分别设置相应表示该用户终端或该网络实体的安全能力，该安全算法选择策略基于该网络实体支持的安全算法列表设置；

[0040] 该网络实体用于接收该用户终端发送的业务请求消息，将该网络实体存储的安全算法列表、该安全保护需求对应的安全算法列表、安全算法选择策略或安全算法选择策略标识发送给该用户终端，以便该用户终端根据该用户终端存储的安全算法列表，与该网络实体返回的安全算法列表、安全算法选择策略或安全算法选择策略标识，选择该安全保护需求对应的安全算法。

[0041] 基于本发明上述实施例提供的另一种用户终端、另一种网络实体与又一种通信系统，由于用户终端和/或网络实体，支持的安全算法列表基于不同的安全保护需求分别设置，网络实体接收到用户终端发送的业务请求消息后，可以将其支持的全部安全算法列表或与业务请求消息的安全保护需求相应的安全算法列表返回给用户终端，以便用户终端从该用户终端与网络实体支持的安全算法中选择业务请求消息的安全保护需求相应的安全算法，从而在后续对该业务进行相应的安全保护，提高了业务的安全性；另外，还可以综合考虑通信系统中各算法的复杂度与占用的开销，在对业务进行有效安全保护的同时提高通信系统的性能。

[0042] 下面通过附图和实施例，对本发明的技术方案做进一步的详细描述。

附图说明

[0043] 图 1 为作为 LTE 系统中接入网部分的 E-UTRAN 的结构示意图；

[0044] 图 2 为 LTE-SAE 系统的安全架构示意图；

[0045] 图 3 为本发明实施例的一种安全算法选择处理方法流程图；

[0046] 图 4 为本发明安全算法选择处理方法一个实施例的流程图；

[0047] 图 5 为本发明安全算法选择处理方法另一个实施例的流程图；

[0048] 图 6 为本发明安全算法选择处理方法又一个实施例的流程图；

[0049] 图 7 为本发明安全算法选择处理方法再一个实施例的流程图；

[0050] 图 8 为本发明安全算法选择处理方法还一个实施例的流程图；

[0051] 图 9 为本发明安全算法选择处理方法又一个实施例的流程图；

[0052] 图 10 为本发明安全算法选择处理装置一个实施例的结构示意图；

[0053] 图 11 为本发明安全算法选择处理装置另一个实施例的结构示意图；

[0054] 图 12 为本发明通信系统一个实施例的结构示意图；

[0055] 图 13 为本发明 UE 一个实施例的结构示意图；

[0056] 图 14 为本发明 UE 另一个实施例的结构示意图；

[0057] 图 15 为本发明 UE 又一个实施例的结构示意图；

[0058] 图 16 为本发明网络实体一个实施例的结构示意图；

[0059] 图 17 为本发明网络实体另一个实施例的结构示意图；

[0060] 图 18 为本发明应用服务器一个实施例的结构示意图；

[0061] 图 19 为本发明通信系统另一个实施例的结构示意图；

[0062] 图 20 为本发明通信系统又一个实施例的结构示意图；

[0063] 图 21 为本发明 UE 再一个实施例的结构示意图；

[0064] 图 22 为本发明 UE 还一个实施例的结构示意图；

[0065] 图 23 为本发明网络实体又一个实施例的结构示意图；

[0066] 图 24 为本发明网络实体再一个实施例的结构示意图；

[0067] 图 25 为本发明通信系统再一个实施例的结构示意图；

[0068] 图 26 为本发明通信系统还一个实施例的结构示意图。

具体实施方式

[0069] 如图 3 所示，本发明实施例的一种安全算法选择处理方法，包括：S1，接收 UE 发送的业务请求消息；S2，根据业务请求消息的安全保护需求，从 UE 与网络实体都支持的安全算法列表中选择安全算法。其中，UE 和 / 或网络实体支持的安全算法列表基于不同的安全保护需求分别设置，或者，UE 与网络实体支持的安全算法列表分别用于表示 UE 与网络实体的安全能力。由于用户终端和 / 或网络实体，支持的安全算法列表基于不同的安全保护需求分别设置，可以根据不同业务请求消息的安全保护需求选择不同的安全算法，以对相应的业务进行不同的安全保护，不但提高了业务的安全性，还可以综合考虑通信系统中各算法的复杂度与占用的开销，在对业务进行有效安全保护的同时提高通信系统的性能。

[0070] 其中的安全保护需求可以包括数据类型、业务类型与用户需求中的任意一种或多种。例如：数据类型对应的安全保护级别需求或安全算法列表，业务类型对应的安全保护级

别需求或安全算法列表或安全算法策略，其中，业务类型对应的安全算法策略用于表示该业务类型在不同条件下的安全保护级别需求。具体地，数据类型可以是 RRC 信令、UP 的用户数据或 NAS 信令。安全算法可以是 RRC 加密算法、RRC 完整性保护算法、UP 加密算法、UP 完整性保护算法、NAS 加密算法或 NAS 完整性算法。

[0071] 作为本发明的一个实施例，UE 支持的安全算法列表包括该 UE 的空口安全能力 Radio Capability 算法列表与网络安全保护能力 NetworkCapability 算法列表。UE 发送的业务请求消息具体可以是服务请求消息 Service Request 或者附着请求消息 Attach Request。

[0072] 本发明的实施例中，UE 的安全能力，例如：算法能力集，可以按照不同数据类型安全保护需求的不同，例如：区分信令与用户面数据，来分别定义不同的算法能力集，为不同数据类型或者不同安全保护层次提供该用 UE 支持的、不同的安全保护算法列表。其中的安全保护层次包括 AS 与 NAS。网络实体的安全能力具体可以为不同数据类型或者不同安全保护层次提供该网络实体支持的、不同的安全保护算法列表。由于不同安全算法的复杂度不同，占用的开销与加解密、完整性验证码的计算和校验的效率也不同，不同数据类型的数据包以及流量的特点是不一样的，对于安全保护需求也不同，例如：信令和用户数据为不同的数据类型。本发明实施例中，UE 的安全能力基于不同的数据类型、业务类型或用户需求的安全保护需求，在 UE 和 / 或网络实体中设置不同的安全算法能力集，这样，UE 或网络实体就可以根据不同的安全保护需求选择不同的安全算法来相应的业务进行安全保护，不但提高了业务的安全性，还可以综合考虑通信系统中各算法的复杂度与占用的开销，在对业务进行有效安全保护的同时提高通信系统的性能。

[0073] 由于数据量大，完整性算法占用的开销太大，对于系统的性能影响太大，现有技术中，对于 UP 的用户数据，并没有进行完整性保护。但是在某些场合，例如：在安全级别要求较高的防篡改、需要准确保证数据正常传输的场合，也有实际的数据完整性保护的需求。或者，基于高安全级别安全算法性能的局限性，本发明实施例中可以根据安全算法本身的特点，例如：复杂度、占用的开销等，来根据用户订阅的安全保护需求预先设置相应的安全算法列表，从而可以采用较为适合和完整性保护算法，例如：采用较低计算量的完整性算法，或者特定部分数据完整性校验的方法，来对相应的 UP 的用户数据进行完整性保护。

[0074] 在本发明的实施例中，网络实体具体可以是 eNB，也可以是 MME。网络实体为演进基站 eNB 时，相应的业务请求消息为 RRC 请求消息或 UP 的用户数据，接收 UE 发送的业务请求消息具体为：eNB 接收 UE 发送的 RRC 请求消息或 UP 的用户数据。网络实体为 MME 时，相应的业务请求消息为 NAS 请求消息，接收 UE 发送的业务请求消息具体为：MME 接收由 eNB 转发的、由 UE 发送的 NAS 请求消息。

[0075] 具体从 UE 与网络实体都支持的安全算法列表中选择业务请求消息的安全保护需求对应的安全算法时，若 UE 与网络实体都支持的安全算法列表中与业务请求消息的安全保护需求对应的安全算法有多种，则可以根据预先设定的优先级顺序，从符合条件的算法中选择用于业务保护的安全算法。该预先设定的优先级顺序可以包含在安全算法列表本身中，也可以在安全算法列表以外的位置存储安全算法列表中各安全算法的优先级顺序。

[0076] 本发明实施例的安全算法选择处理方法之前，可以在 UE 和 / 或网络实体中，根据不同的安全保护需求分别设置不同的安全算法列表，并可以根据实际需求，对 UE 的和 / 或

网络实体中安全算法列表进行增加、删除或更新。

[0077] 通过本发明实施例，从 UE 与网络实体都支持的安全算法列表中选择业务请求消息的安全保护需求对应的安全算法后，UE 与网络实体之间，例如 :UE 与 eNB 之间，UE 与 MME 之间，就可以根据选择的安全算法对业务进行安全保护。

[0078] 具体地，在 LTE-SAE 系统中，eNB 从该 eNB 自身与 UE 都支持的安全算法列表中选择出 RRC 加密算法、RRC 完整性保护算法、UP 加密算法、UP 完整性保护算法后，eNB 向 UE 发送经过完整性保护的 AS 安全模式命令，其中携带有密钥标识 KSIasme、EAEA、EAIA、EUEA 和 AS 消息完整性保护的认证码 (AS Message Authentication Codes，以下简称 :AS-MAC)，UE 进入 AS 安全模式并向 eNB 返回经过完整性保护的 AS 安全模式响应，其中携带有 AS-MAC，从而启动 AS 的安全模式，从 AS 的安全模式启动成功后，通过 eNB 选择的安全保护算法对数据和信令进行安全保护。MME 从该 MME 自身与 UE 都支持的安全算法列表中选择出 ENEA 与 ENIA 后，向 UE 发送经过完整性保护的 NAS 安全模式命令，其中携带有密钥标识 KSIasme、ENEA、ENIA 与 NAS 消息完整性保护的认证码 (NAS Message Authentication Codes，以下简称 :NAS-MAC)，UE 进入 NAS 安全模式并向 MME 返回经过完整性保护的 NAS 安全模式响应，其中携带有 NAS-MAC，从而启动 NAS 的安全模式，从 NAS 的安全模式启动成功后，通过 MME 选择的安全保护算法对数据和信令进行安全保护。

[0079] 如图 4 所示，为本发明安全算法选择处理方法一个实施例的流程图，其包括以下步骤 :

[0080] 步骤 101，网络实体接收 UE 发送的业务请求消息，该业务请求消息中包括 UE 支持的安全算法列表。

[0081] 其中的网络实体可以是 eNB 或者 MME。若网络实体是 eNB，则 eNB 可以与 UE 进行信息交互，直接从 UE 获得 UE 支持的安全算法列表。另外，UE 也可以将其支持的安全算法列表发送给 MME，eNB 从 MME 获取 UE 支持的安全算法列表。若网络实体是 MME，由于 MME 通过 eNB 与 UE 进行信息交互，UE 先将业务请求消息发送给 eNB，再由 eNB 将该业务请求消息转发给 MME。其它实施例中的消息发送流程同理，不再赘述。

[0082] 另外，步骤 101 中的业务请求消息中也可以不包括 UE 支持的安全算法列表，而由网络实体预先存储 UE 支持的安全算法列表，或者由应用服务器中存储的关于 UE 的安全能力信息提供。

[0083] 步骤 102，网络实体根据预先设置的业务请求消息与安全保护需求之间的对应关系信息，获取 UE 发送的业务请求消息的安全保护需求。

[0084] 步骤 103，网络实体获取自己支持的安全算法列表中与安全保护需求对应的安全算法列表，以及获取 UE 支持的安全算法列表中与安全保护需求对应的安全算法列表。

[0085] 具体地，若网络实体与 UE 中只有一个安全算法列表基于不同的安全保护需求分别设置，则仅对基于不同的安全保护需求分别设置安全算法列表的 UE 或网络实体执行该步骤 103 的操作，而认为未基于不同的安全保护需求分别设置的安全算法列表中的安全算法适用于所有的安全保护需求，也就是说，不论安全保护需求是什么，针对该安全保护需求，从该未基于不同的安全保护需求分别设置安全算法列表的 UE 或网络实体中获取的安全算法都是该 UE 或网络实体中的所有安全算法列表。其它实施例同理。例如 :假设 UE 支持的安全算法列表包括 A、B、C 三种算法，且该安全算法列表未基于不同的安全保护需求分

别设置，而网络实体支持的安全算法列表包括 A、B、D、E、F 五种算法，该安全算法列表中，与第一用户需求对应的安全算法为 A 与 B，与第二用户需求对应的安全算法为 D、E 与 F，则若用户终端发送的业务请求消息的安全保护需求为第一用户需求，则从 UE 获取的与该第一用户需求对应的安全算法 UE 支持的安全算法列表中的所有安全算法，即 :A、B 与 C，从网络实体获取的与该第一用户需求对应的安全算法为 A 与 B。

[0086] 步骤 104，网络实体从获取的安全算法列表中，UE 与网络实体都支持的安全算法列表中选择一种作为该业务请求消息所请求业务的安全保护算法。

[0087] 根据步骤 103 中的实例，可以选择 A 或 B 作为该业务请求消息所请求业务的安全保护算法。若预先设置了 A 安全算法与 B 安全算法的优先级顺序，则根据优先级顺序选择 A 或 B 作为该业务请求消息所请求业务的安全保护算法。否则，可以根据其它规则或随机选择 A 或 B 作为该业务请求消息所请求业务的安全保护算法。

[0088] 在上述图 4 所示的实施例中，由 UE 在发送给网络实体的业务请求消息时携带 UE 支持的安全算法列表，由网络实体直接根据 UE 支持的安全算法列表与网络实体支持的安全算法列表中选择相应的安全保护算法，对现有技术的流程改动较小，并且流程简单，易于实现。

[0089] 本发明实施例中的步骤 103 与步骤 104 可以没有时间顺序关系，例如 :步骤 104 也可以先于或同时与步骤 103 执行。例如 :可以先通过步骤 104 选择 UE 和网络实体都支持的安全算法，则从中选择出与业务请求消息的安全保护需求对应的安全算法。还是基于步骤 103 的实施例，从 UE 的安全算法列表和网络实体的安全算法列表中选择出二者都支持的安全算法为 A 与 B，再从 A 与 B 中选择出与第一用户需求对应的安全算法 :A 与 B，之后可以根据优先级顺序或随机选择 A 或 B 作为该业务请求消息所请求业务的安全保护算法。作为本发明实施例的一个具体应用，假设 UE 支持的安全算法列表如下表 1 所示。其中，在信令协议中的标识包括该安全算法支持的密钥长度 - 安全算法名称缩写，例如 :“128-EEA0”表示名称为 Null ciphering algorithm 的安全算法支持的密钥长度为 128，该安全算法名称缩写为 EEA0。“ √ ”表示该安全算法适用于某项业务，“ √ ”表示该安全算法不适用于某项业务，根据表 1，安全算法 Null ciphering 与 AES 适用于 RRC 加密业务，安全算法 SNOW 3G 不适用于 RRC 加密业务，也就是说 :对于 RRC 加密算法，UE 支持 Null ciphering 与 AES 安全算法。进一步地，可以按照安全算法被选择的优先级顺序来为安全算法分配安全算法编号，也就是说，在某一安全保护需求对应的各种算法中，可以优先选择编号较小或者编号较大的算法作为对相应业务进行安全保护的算法。

[0090] 表 1UE 支持的安全算法列表

[0091]

安全算法编号	在信令协议中的标识	安全算法名称	RRC 加密	.....	UP 加密
00002″	128-EEA0	Null ciphering algorithm	√	.....	×

″ 00012″	128-EEA1	SNOW 3G	×	.....	√
″ 00102″	128-EEA2	AES	√	.....	√

[0092] eNB 支持的安全算法列表如下表 2 所示，eNB 支持的安全算法适用于所有业务的安全保护需求，也就是说，eNB 支持的安全算法列表未基于不同的安全保护需求分别设置。

[0093] 表 2eNB 支持的安全算法列表

[0094]

安全算法编号	在信令协议中的标识	安全算法名称
00002″	128-EEA0	Null ciphering algorithm
″ 00012″	128-EEA1	SNOW 3G
″ 00102″	128-EEA2	AES

[0095] 表 1 与表 2 中的安全保护需求仅以数据类型为例。若网络实体接收到 UE 发送的业务请求消息为 RRC 请求消息，则确定其数据类型为 RRC 信令，根据步骤 103，从 RRC 请求消息中 UE 支持的安全算法列表中选择的安全算法列表包括安全算法 Null ciphering 与 AES，从 eNB 支持的安全算法列表中选择的安全算法列表包括安全算法 Null ciphering、SNOW 3G 与 AES，因此，eNB 可从 Null ciphering 与 AES 中选择一种安全算法作为 RRC 信令的加密算法。若表 1 与表 2 中的安全算法按照从高到低的优先级顺序排列，则 eNB 选择 Null ciphering 与 AES 中优先级较高的 Null ciphering 作为 RRC 信令的加密算法。而针对 UP 的用户数据选择 SNOW 3G 安全算法，这样，对 UP 的用户数据与 RRC 信令就选择了不同多个安全算法。在本发明的各实施例中，若网络实体与 UE 中对安全算法的优先级排列顺序冲突，可以根据预先设定，按照 UE 或网络实体中的优先级顺序选择，或者优先级顺序冲突的安全算法都不选择，或者直接结束本次安全算法选择。

[0096] 另外，在步骤 101 之前，UE 可以根据其将要发送的业务请求消息的安全保护需求，从该 UE 支持的安全算法列表中选择该安全保护需求对应的安全算法列表；相应的，步骤 101 中，业务请求消息中包括的是该 UE 支持的、安全保护需求对应的安全算法列表；步骤 103 中，仅需网络实体获取自己支持的安全算法列表中与获取的安全保护需求对应的安全算法即可，若网络实体中的安全算法列表未基于不同的安全保护需求分别设置，则网络实体获取自己支持的安全算法列表。

[0097] 如图 5 所示，为本发明安全算法选择处理方法另一个实施例的流程图，其包括以下步骤：

[0098] 步骤 201，网络实体接收 UE 发送的业务请求消息。

[0099] 步骤 202，网络实体获取自己支持的向安全算法列表，并发送给 UE。

[0100] 步骤 203，UE 根据预先设置的业务请求消息与安全保护需求之间的对应关系信息，获取 UE 发送的业务请求消息的安全保护需求。

[0101] 其中，步骤 203 与步骤 202 之间没有严格的时间关系限制，步骤 203 也可以与步骤 202 同时执行或先于步骤 202 执行。

[0102] 步骤 204，UE 从该 UE 与网络实体都支持的安全算法列表中选择安全保护需求对应的安全算法。

[0103] 具体地，UE 可以参考步骤 103-104 的方式选择从该 UE 与网络实体都支持的安全算法列表中选择安全保护需求对应的安全算法。

[0104] 在上述图 5 所示的实施例中，网络实体在接收到 UE 发送的业务请求消息后，向 UE 反馈该网络实体支持的安全算法列表，由 UE 直接根据 UE 支持的安全算法列表与网络实体支持的安全算法列表中选择相应的安全保护算法，不需要 UE 向网络实体上报其支持的安全算法列表，因此，可以较为快速的选择出安全保护需求对应的安全算法。

[0105] 或者，在步骤 201 之后，网络实体可以根据预先设置的业务请求消息与安全保护需求之间的对应关系信息，获取 UE 发送的业务请求消息的安全保护需求，并从自己支持的安全算法列表中与获取的安全保护需求对应的安全算法列表。相应的，步骤 202 中，网络实体仅将获取的安全保护需求对应的安全算法列表发送给 UE。步骤 204 中，UE 从网络实体发送的安全保护需求对应的安全算法列表与 UE 自身中与通过步骤 203 获取的安全保护需求对应的安全算法列表中，选择一种安全算法作为业务消息所请求业务的安全保护算法。

[0106] 若 UE 中的安全算法列表未基于不同的安全保护需求分别设置，则不需要执行步骤 203。相应的，步骤 204 中，UE 从网络实体发送的安全保护需求对应的安全算法列表与 UE 自身支持的安全算法列表中，选择一种安全算法作为业务消息所请求业务的安全保护算法。

[0107] 或者，在网络实体中存储有安全算法选择策略时，步骤 201 之后，向 UE 返回网络实体支持的安全算法选择策略，该安全算法选择策略基于网络实体支持的安全算法列表设置，例如：安全算法选择策略可以是在网络实体支持的安全算法列表中，各种数据类型、业务类型与用户需求具体对应的安全算法，或进一步包括安全算法的优先级顺序。相应的，步骤 204 中，UE 根据网络实体发送的安全算法选择策略，从 UE 与网络实体都支持的安全算法列表中选择安全保护需求对应的安全算法。

[0108] 网络实体中可以存储多个安全算法选择策略，这些安全算法选择策略的相关信息，例如：策略名称、策略标识 (identifier，以下简称：ID)、安全保护需求应用的安全算法在终端与网络实体都是同步的，或者，网络实体与 UE 对对方所能支持的安全算法选择策略是可知的。当网络实体启用安全算法的时候，可以将安全算法选择策略通过安全保护的消息传递给 UE，指示 UE 采用相应的安全算法保护后续的通信业务。如下表 3、表 4 所示，分别为网络实体中存储的安全算法策略一和安全算法策略二。安全算法策略给出了针对不同的数据类型、业务类型与用户需求具体应用的安全算法。

[0109] 表 3 安全算法策略一

[0110]

安全保护需求	应用的安全算法
数据类型一 / 业务类型一	算法 A
数据类型二 / 业务类型二	算法 B

数据类型三 / 业务类型三	算法 C
数据类型四 / 业务类型四	算法 D

[0111] 表 4 安全算法策略二

[0112]

安全保护需求	应用的安全算法
数据类型一 / 用户 AAAAAAA	算法 D
数据类型二 / 用户 CCCCCCC	算法 C

[0113]

数据类型三 / 用户 EEEEEEEE	算法 B
数据类型四 / 用户 XXXXXXX	算法 A

[0114] 进一步地，若 UE 中也存储有与网络实体中相同的安全算法选择策略，并且 UE 与网络实体都存储有安全算法选择策略与安全算法选择策略 ID 时，为了减少网络流量，尽可能少地占用有限的网络带宽资源，网络实体可以仅将与用户终端发送的业务请求消息对应的安全算法选择策略的安全算法选择策略 ID 发送给 UE。在步骤 204 中，UE 确定网络实体发送的安全算法选择策略 ID 所标识的安全算法选择策略，并根据该安全算法选择策略，从 UE 与网络实体都支持的安全算法列表中选择安全保护需求对应的安全算法。

[0115] 为了进一步对不同安全保护需求的安全算法进行限制，便于对安全算法的选择进行统一管理和更新，可以在通信网络中设置一个应用服务器，在其中基于不同的安全保护需求分别设置安全算法列表、安全算法选择策略或安全算法选择策略 ID，其中的安全算法选择策略基于安全保护需求设置，其设置方法可以参考网络实体中安全算法选择策略的设置方法。具体选择业务请求消息所请求业务的安全算法时，从 UE 与网络实体都支持且应用服务器存储的安全算法列表中选择安全算法。可以预先设定，在 UE 或网络实体选择的安全算法与应用服务器选择的安全算法冲突时，以应用服务器选择的安全算法为准。

[0116] 如图 6 所示，为本发明安全算法选择处理方法又一个实施例的流程图，其包括以下步骤：

[0117] 步骤 301，UE 向应用服务器发送获取请求消息，获取该应用服务器存储的安全算法列表，或该安全算法列表中与将要发送的业务请求消息的安全保护需求对应的安全算法列表，或安全算法选择策略，或安全算法选择策略 ID。

[0118] 步骤 302，UE 根据自身支持的安全算法列表，与从应用服务器获取的安全算法列表、安全算法选择策略或安全算法选择策略 ID，相应选择该 UE 支持且应用服务器存储的安全算法列表，或选择该 UE 支持且应用服务器存储的、业务请求消息的安全保护需求对应的安全算法列表。

[0119] 若 UE 从应用服务器获取的是安全算法选择策略 ID，UE 先根据安全算法选择策略与安全算法选择策略 ID 之间的对应关系获取相应的安全算法选择策略。

[0120] UE 选择的安全算法列表具体是 UE 支持且应用服务器存储的、且与业务请求消息

的安全保护需求对应的安全算法列表，还是 UE 支持且应用服务器存储的安全算法列表，可以根据通信需求预先设定。

[0121] 步骤 303，UE 向网络实体发送业务请求消息，该业务请求消息中包括 UE 选择的安全算法列表，具体为 UE 支持且应用服务器存储的安全算法列表，或 UE 支持且应用服务器存储的、且与业务请求消息的安全保护需求对应的安全算法列表。

[0122] 步骤 304，网络实体根据预先设置的业务请求消息与安全保护需求之间的对应关系信息，获取 UE 发送的业务请求消息的安全保护需求。

[0123] 步骤 305，若业务请求消息中包括的是 UE 支持且应用服务器存储的、且与业务请求消息的安全保护需求对应的安全算法列表，网络实体获取自己支持的安全算法列表中与获取的安全保护需求对应的安全算法列表。

[0124] 若业务请求消息中包括的是 UE 支持且应用服务器存储的安全算法列表，则该步骤 305 中，网络实体还从该安全算法列表中选择出安全保护需求对应的安全算法列表。

[0125] 具体业务请求消息中包括的安全算法列表是 UE 支持且应用服务器存储的、且与业务请求消息的安全保护需求对应的安全算法列表，还是 UE 支持且应用服务器存储的安全算法列表，可以根据通信需求预先设定。

[0126] 步骤 306，网络实体从自己支持的、且与业务请求消息的安全保护需求对应的安全算法列表，与业务请求消息中 UE 选择的安全算法列表中，选择一种作为该业务请求消息所请求业务的安全保护算法。

[0127] 在上述图 6 所示的实施例中，UE 先选择出该 UE 支持且应用服务器存储的安全算法列表，或选择该 UE 支持且应用服务器存储的、业务请求消息的安全保护需求对应的安全算法列表，再发送给网络实体，减少了 UE 发送全部该 UE 支持的全算法列表与应用服务器存储的全算法列表的网络流量。并且，网络实体选择安全算法列表时还考虑了应用服务器存储的安全算法列表，进一步限制了不同安全保护需求的安全算法，便于对安全算法的选择进行统一管理和更新。

[0128] 如图 7 所示，为本发明安全算法选择处理方法再一个实施例的流程图，其包括以下步骤：

[0129] 步骤 401，UE 向应用服务器发送获取请求消息，获取该应用服务器存储的安全算法列表，或该安全算法列表中与将要发送的业务请求消息的安全保护需求对应的安全算法列表，或安全算法选择策略，或安全算法选择策略 ID。

[0130] 步骤 402，UE 向网络实体发送业务请求消息，该业务请求消息中包括 UE 支持的安全算法列表，或该安全算法列表中与将要发送的业务请求消息的安全保护需求对应的安全算法列表，与获取的应用服务器存储的安全算法列表，或该安全算法列表中与安全保护需求对应的安全算法列表，或安全算法选择策略，或安全算法选择策略 ID。

[0131] 该业务请求消息中的安全算法列表具体是 UE 支持的安全算法列表，还是该安全算法列表中与将要发送的业务请求消息的安全保护需求对应的安全算法列表，是应用服务器存储的安全算法列表，还是该安全算法列表中与安全保护需求对应的安全算法列表，可以根据通信需求预先设定。

[0132] 步骤 403，网络实体根据预先设置的业务请求消息与安全保护需求之间的对应关系信息，获取 UE 发送的业务请求消息的安全保护需求。

[0133] 步骤 404，若业务请求消息中包括的是 UE 支持且应用服务器存储的、与该安全保护需求对应的安全算法列表，网络实体获取自己支持的安全算法列表中与获取的安全保护需求对应的安全算法列表。

[0134] 若业务请求消息中包括的是 UE 支持的安全算法列表，与应用服务器存储的安全算法列表、安全算法选择策略或安全算法选择策略 ID，则该步骤 404 中，网络实体还分别选择出 UE 支持且应用服务器存储的、与该安全保护需求对应的安全算法列表。

[0135] 如果业务请求消息中包括应用服务器的安全算法选择策略 ID，则需要预先在网络实体与应用服务器中设置相同的安全算法选择策略与安全算法选择策略 ID 之间的对应关系，网络实体根据安全算法选择策略 ID 获取相应的安全算法选择策略。

[0136] 具体业务请求消息中包括的安全算法列表是 UE 支持且应用服务器存储的、且与该安全保护需求对应的安全算法列表，还是 UE 支持且应用服务器存储的安全算法列表、安全算法选择策略或安全算法选择策略 ID，可以根据通信需求预先设定。

[0137] 步骤 405，网络实体从自己支持的、且与该安全保护需求对应的安全算法列表，和 UE 支持且应用服务器存储的、与该安全保护需求对应的安全算法列表中，选择一种作为该业务请求消息所请求业务的安全保护算法。

[0138] 在上述图 7 所示的实施例中，UE 将该 UE 支持的安全算法列表与应用服务器存储的安全算法列表，或该安全算法列表中与安全保护需求对应的安全算法列表，或安全算法选择策略，或安全算法选择策略 ID，发送给网络实体，网络实体选择安全算法列表时还考虑了应用服务器存储的安全算法列表，进一步限制了不同安全保护需求的安全算法，便于对安全算法的选择进行统一管理和更新。

[0139] 如图 8 所示，为本发明安全算法选择处理方法还一个实施例的流程图，其包括以下步骤：

[0140] 步骤 501，UE 向网络实体发送业务请求消息，该业务请求消息中包括 UE 支持的安全算法列表，或 UE 根据该业务请求消息的安全保护需求，从自己支持的安全算法列表选择出来的与安全保护需求对应的安全算法列表。

[0141] 业务请求消息中的安全算法列表具体是 UE 支持的、且与业务请求消息的安全保护需求对应的安全算法列表，还是 UE 支持的安全算法列表，可以根据通信需求预先设定。

[0142] 步骤 502，网络实体接收到 UE 发送的业务请求消息之后，获取应用服务器存储的安全算法列表、该应用服务器存储的且与该安全保护需求对应的安全算法列表、安全算法选择策略或安全算法选择策略 ID。

[0143] 步骤 503，网络实体根据预先设置的业务请求消息与安全保护需求之间的对应关系信息，获取 UE 发送的业务请求消息的安全保护需求。

[0144] 步骤 504，若网络实体通过步骤 501 与步骤 502 获得的是 UE 与应用服务器都支持的、业务请求消息的安全保护需求对应的安全算法列表，网络实体获取自己支持的安全算法列表中与获取的安全保护需求对应的安全算法列表。

[0145] 若网络实体通过步骤 501 与步骤 502 获得的是 UE 支持的安全算法列表，与应用服务器存储的安全算法列表、安全算法选择策略或安全算法选择策略 ID，则该步骤 504 中，网络实体还分别选择出 UE 支持且应用服务器存储的、与安全保护需求对应的安全算法列表。

[0146] 如果业务请求消息中包括应用服务器的安全算法选择策略 ID，则需要预先在网络

实体与应用服务器中设置相同的安全算法选择策略与安全算法选择策略 ID 之间的对应关系，网络实体根据安全算法选择策略 ID 获取相应的安全算法选择策略。

[0147] 步骤 505，网络实体从自己支持的、且与该安全保护需求对应的安全算法列表，与 UE 支持且应用服务器存储的、与该安全保护需求对应的安全算法列表中，选择一种作为该业务请求消息所请求业务的安全保护算法。

[0148] 在上述图 8 所示的实施例中，网络实体接收到 UE 发送的业务请求消息后，自己获取而不需要 UE 获取再发送应用服务器存储的安全算法列表，或该安全算法列表中与安全保护需求对应的安全算法列表，或安全算法选择策略，或安全算法选择策略 ID，减少了 UE 发送应用服务器的安全算法列表，或安全算法选择策略，或安全算法选择策略 ID 所占用的网络带宽；另外，网络实体选择安全算法列表时还考虑了应用服务器存储的安全算法列表，进一步限制了不同安全保护需求的安全算法，便于对安全算法的选择进行统一管理和更新。

[0149] 通过图 4 中的步骤 104，图 6 中的步骤 306，图 7 中的步骤 405，与图 8 中的步骤 505，网络实体选择出安全算法之后，可以通过安全模式命令将该选择的安全算法发送给 UE，以便于 UE 与网络实体通过该安全算法对相应的业务进行安全保护。具体地，若网络实体是 eNB，则 eNB 可以直接将选择的安全算法发送给 UE；若网络实体是 MME，则 MME 可以将选择的安全算法发送给 eNB，由 eNB 将该安全算法转发给 UE，网络实体向 UE 发送的其它消息流程类同，不再赘述。

[0150] 如图 9 所示，为本发明安全算法选择处理方法又一个实施例的流程图，其包括以下步骤：

[0151] 步骤 601，UE 向应用服务器发送获取请求消息，获取该应用服务器存储的安全算法列表，或该安全算法列表中与将要发送的业务请求消息的安全保护需求对应的安全算法列表，或安全算法选择策略，或安全算法选择策略 ID。

[0152] 若从应用服务器获取的是安全算法选择策略 ID，UE 需要根据安全算法选择策略与安全算法选择策略 ID 之间的对应关系获取相应的安全算法选择策略。

[0153] 步骤 602，UE 向网络实体发送业务请求消息。

[0154] 另外，步骤 602 也可以与步骤 601 同时执行或先于步骤 601 执行。

[0155] 步骤 603，网络实体接收到 UE 发送的业务请求消息之后，向 UE 返回该网络实体支持的安全算法列表，或其中与安全保护需求对应的安全算法列表，或安全算法选择策略，或安全算法选择策略 ID，该安全算法选择策略基于网络实体支持的安全算法列表设置。

[0156] 若网络实体返回的是安全算法选择策略 ID，UE 需要根据安全算法选择策略与安全算法选择策略 ID 之间的对应关系获取相应的安全算法选择策略。

[0157] 网络实体返回的具体是其支持的安全算法列表，还是其中安全保护需求对应的安全算法列表，还是安全算法选择策略，还安全算法选择策略 ID，可以根据通信需求预先设定。

[0158] 步骤 604，UE 根据自己支持的安全算法列表，与应用服务器存储的安全算法列表或安全算法选择策略，与网络实体的安全算法列表或安全算法选择策略，选择出与该业务请求消息的安全保护需求对应的安全算法。

[0159] 具体地，该步骤 604 中，UE 可以先分别选择出 UE 与网络实体都支持且应用服务器

存储的、与安全保护需求对应的安全算法列表，如果网络实体或应用服务器本身返回的就是其支持的、且与安全保护需求对应的安全算法列表，则无需执行该操作。然后，再进一步从三个安全算法列表中选择出一个共有的安全算法。具体实现可以参考图 4- 图 8 中的相应步骤。另外，如果网络实体或应用服务器本身返回的都是其支持的安全算法列表、安全算法选择策略或安全算法选择策略 ID，UE 也可以先选择出 UE 与网络实体都支持且应用服务器存储的安全算法列表，再从中选择出一个与安全保护需求对应的安全算法。

[0160] 在上述图 9 所示的实施例中，由 UE 获取网络实体支持的安全算法列表与应用服务器存储的安全算法列表，或该安全算法列表中与安全保护需求对应的安全算法列表，或安全算法选择策略，或安全算法选择策略 ID，据此选择 UE 与网络实体都支持且应用服务器存储的与安全保护需求对应的安全算法列表，对现有技术的流程改动较小；另外，UE 选择安全算法列表时还考虑了应用服务器存储的安全算法列表，进一步限制了不同安全保护需求的安全算法，便于对安全算法的选择进行统一管理和更新。

[0161] 如图 10 所示，为本发明安全算法选择处理装置一个实施例的结构示意图，其包括第一获取模块 701 与第一选择模块 702。其中，第一获取模块 701 用于获取 UE 发送的业务请求消息的安全保护需求。第一选择模块 702 用于根据业务请求消息的安全保护需求，从 UE 与网络实体都支持的安全算法列表中选择安全算法。其中，UE 和 / 或网络实体支持的安全算法列表基于不同的安全保护需求分别设置，或者，UE 与网络实体支持的安全算法列表分别用于表示 UE 与网络实体的安全能力。

[0162] 如图 11 所示，为本发明安全算法选择处理装置另一个实施例的结构示意图，与图 10 所示的实施例相比，该实施例中的第一选择模块 702 包括第一获取单元 7021 与第一选择单元 7022。其中，第一获取单元 7021 用于获取 UE 支持的安全算法列表，或 UE 支持的、且与该 UE 发送的业务请求消息的安全保护需求对应的安全算法列表，与网络实体支持的安全算法列表、该安全算法列表中与该业务请求消息的安全保护需求对应的安全算法列表、安全算法选择策略或安全算法选择策略 ID，该安全算法选择策略基于网络实体支持的安全算法列表设置。第一选择单元 7022 用于根据第一获取单元 7021 从 UE 获取的安全算法列表，与从网络实体获取的安全算法列表、安全算法选择策略或安全算法选择策略 ID，选择该安全保护需求对应的安全算法。

[0163] 进一步地，在图 11 所示的实施例中，第一获取单元 7021 还可以获取应用服务器存储的安全算法列表、该安全算法列表中与该业务请求消息的安全保护需求对应的安全算法列表、安全算法选择策略或安全算法选择策略 ID，该安全算法选择策略基于安全保护需求设置，应用服务器存储的安全算法列表基于不同的安全保护需求分别设置。相应的，第一选择单元 7022 用于根据第一获取单元 7021 从 UE 获取的安全算法列表，与分别从网络实体和应用服务器获取的安全算法列表、安全算法选择策略或安全算法选择策略 ID，选择 UE、网络实体与应用服务器都支持的、且与该安全保护需求对应的安全算法。

[0164] 由于 UE、网络实体和 / 或应用服务器的安全算法列表基于不同的安全保护需求分别设置，本发明实施例的安全算法选择处理装置可以根据不同业务请求消息的安全保护需求选择不同的安全算法，以对 UE 与网络实体之间相应的业务进行不同的安全保护，不但提高了业务的安全性，还可以综合考虑通信系统中各算法的复杂度与占用的开销，在对业务进行有效安全保护的同时提高通信系统的性能。

[0165] 本发明上述各实施例提供的安全算法选择处理装置可用于实现本发明上述实施例中各安全算法选择处理的相应流程。

[0166] 本发明实施例提供的一种通信系统，包括网络实体 1 与安全算法选择处理装置 2。其中，安全算法选择处理装置 2 用于获取 UE 发送的业务请求消息的安全保护需求，并根据该业务请求消息对应的安全保护需求，从 UE 与网络实体 1 都支持的安全算法列表中选择安全算法。其中，UE 和 / 或网络实体 1 支持的安全算法列表基于不同的安全保护需求分别设置，或者，UE 与网络实体 1 支持的安全算法列表分别用于表示该 UE 与网络实体 1 的安全能力。该实施例中的安全算法选择处理装置 2 可基于图 10 或图 11 所示实施例的安全算法选择处理装置实现。

[0167] 进一步地，通信系统中还可以包括应用服务器 3，用于存储该应用服务器 3 存储的安全算法列表、安全算法选择策略或安全算法选择策略标识，其中的安全算法选择策略基于安全保护需求设置，应用服务器 3 存储的安全算法列表基于不同的安全保护需求分别设置。相应的，安全算法选择处理装置 2 还可以获取应用服务器 3 存储的安全算法列表、安全算法选择策略或安全算法选择策略 ID，根据从 UE 获取的安全算法列表，与分别从网络实体 1 和应用服务器 3 获取的安全算法列表、安全算法选择策略或安全算法选择策略 ID，选择与 UE 发送的业务请求消息的安全保护需求对应的安全算法。其中，网络实体 1 的安全算法选择策略基于该网络实体 1 支持的安全算法列表设置。该实施例中的安全算法选择处理装置 2 可基于图 11 所示实施例的安全算法选择处理装置实现。如图 12 所示，为本发明通信系统一个实施例的结构示意图，该实施例的安全算法选择处理装置 2 采用图 11 所示实施例的安全算法选择处理装置。

[0168] 如图 13 所示，为本发明 UE 一个实施例的结构示意图，该实施例的 UE 可以实现本发明图 4 与图 8 所示实施例中的相应流程，其包括第一存储模块 801、第二获取模块 802、第一发送模块 803 与第一接收模块 804。其中，第一存储模块 801 用于存储 UE 支持的安全算法列表，该安全算法列表基于不同的安全保护需求分别设置或者用于表示该 UE 的安全能力。第二获取模块 802 用于从第一存储模块 801 中获取安全算法列表，或查询业务请求消息的安全保护需求，从第一存储模块 801 中获取该安全保护需求对应的安全算法列表。第一发送模块 803 用于生成并向网络实体发送业务请求消息，业务请求消息中包括第二获取模块 802 获取的安全算法列表。第一接收模块 804 用于接收网络实体根据该业务请求消息返回的安全算法，该安全算法根据业务请求消息的安全保护需求，从 UE 与网络实体都支持的安全算法列表中选择。

[0169] 如图 14 所示，为本发明 UE 另一个实施例的结构示意图，该实施例的 UE 可以实现本发明图 7 所示实施例中的相应流程。与图 13 所示的实施例相比，该实施例的 UE 还包括第三获取模块 805，用于获取应用服务器存储的安全算法列表，或其中与安全保护需求对应的安全算法列表，或安全算法选择策略，或安全算法选择策略 ID，该安全算法选择策略基于安全保护需求设置，应用服务器存储的安全算法列表基于不同的安全保护需求分别设置。相应的，第一发送模块 803 向网络实体发送的业务请求消息中包括第二获取模块 802 从第一存储模块 801 中获取的安全算法列表和第三获取模块 805 从应用服务器获取的安全算法列表、安全算法选择策略、或安全算法选择策略 ID。

[0170] 如图 15 所示，为本发明 UE 又一个实施例的结构示意图，该实施例的 UE 可以实现

本发明图6所示实施例中的相应流程。与图13所示的实施例相比，该实施例的UE还包括第三获取模块805，用于获取应用服务器存储的安全算法列表，或其中与UE发送的业务请求消息的安全保护需求对应的安全算法列表，或安全算法选择策略，或安全算法选择策略ID，该安全算法选择策略基于安全保护需求设置。相应的，第二获取模块802包括第二获取单元8021与第二选择单元8022。其中，第二获取单元8021用于从第一存储模块801中获取安全算法列表，或查询业务请求消息的安全保护需求，从第一存储模块801中获取该安全保护需求对应的安全算法列表。第二选择单元8022用于根据第二获取单元8021从第一存储模块801中存储的安全算法列表，与第三获取模块805从应用服务器获取的安全算法列表、安全算法选择策略、或安全算法选择策略ID，选择UE支持且应用服务器存储的安全算法列表，或UE支持且应用服务器存储的、且与UE发送的业务请求消息的安全保护需求对应的安全算法列表。相应的，UE向网络实体发送的业务请求消息中的安全算法列表具体为第二选择单元8022选择的安全算法列表。

[0171] 如图16所示，为本发明网络实体一个实施例的结构示意图，该实施例的网络实体可用于实现本发明图4所示实施例中的相应流程，其包括第二存储模块901、第二接收模块902、第二选择模块903与第二发送模块904。其中，第二存储模块901用于存储网络实体支持的安全算法列表或安全算法选择策略，其中的安全算法列表基于不同的安全保护需求分别设置或者用于表示该网络实体的安全能力，安全算法选择策略基于网络实体支持的安全算法列表设置。第二接收模块902用于接收UE发送的业务请求消息，该业务请求消息中包括UE支持的安全算法列表。第二选择模块903用于根据第二存储模块901中存储的安全算法列表或安全算法选择策略，与第二接收模块902接收到的业务请求消息中的安全算法列表，从UE与网络实体都支持的安全算法列表中选择安全保护需求对应的安全算法。第二发送模块904用于将第二选择模块903选择的安全算法发送给UE。

[0172] 与图7所示实施例中的流程相应，在图16所示实施例的网络实体中，第二接收模块902接收到的业务请求消息中的安全算法列表具体可以是UE支持且应用服务器存储的安全算法列表，或UE支持且应用服务器存储的、且与业务请求消息的安全保护需求对应的安全算法列表。相应的，第二选择模块903从第二存储模块901中存储的安全算法列表或安全算法选择策略，与业务请求消息中的安全算法列表中，选择该安全保护需求对应的安全算法。

[0173] 与图6所示实施例中的流程相应，在图16所示实施例的网络实体中，第二接收模块902接收到的业务请求消息中还可以包括应用服务器存储的安全算法列表，或该安全算法列表中与业务请求消息的安全保护需求对应的安全算法列表，或安全算法选择策略，或安全算法选择策略ID，其中的安全算法选择策略基于安全保护需求设置，应用服务器存储的安全算法列表基于不同的安全保护需求分别设置。相应的，第二选择模块903根据第二存储模块901中存储的安全算法列表或安全算法选择策略，与业务请求消息中UE的安全算法列表，和应用服务器存储的安全算法列表、与安全保护需求对应的安全算法列表、安全算法选择策略或安全算法选择策略ID，选择安全保护需求对应的安全算法。

[0174] 如图17所示，为本发明网络实体另一个实施例的结构示意图。与图8所示实施例中的流程相应，与图16所示实施例的网络实体相比，第二接收模块902接收到的业务请求消息中的安全算法列表具体为UE支持的、且与UE发送的业务请求消息的安全保护需求对

应的安全算法列表。相应的，网络实体还包括第四获取模块 905，用于获取应用服务器存储的安全算法列表，或该安全算法列表中与安全保护需求对应的安全算法列表，或安全算法选择策略，或安全算法选择策略 ID，其中的安全算法选择策略基于安全保护需求设置，应用服务器存储的安全算法列表基于不同的安全保护需求分别设置。相应的，第二选择模块 903 根据第二存储模块 901 中存储的安全算法列表或安全算法选择策略，与第二接收模块 902 接收到的业务请求消息中的安全算法列表，与第四获取模块 905 获取到的应用服务器存储的安全算法列表、安全保护需求对应的安全算法列表、安全算法选择策略或安全算法选择策略 ID，选择安全保护需求对应的安全算法。

[0175] 如图 18 所示，为本发明应用服务器一个实施例的结构示意图，该实施例的应用服务器包括第三存储模块 1001、第三接收模块 1002 与第三发送模块 1003。其中，第三存储模块 1001 用于存储应用服务器的安全算法列表、安全算法选择策略或安全算法选择策略 ID，其中的安全算法选择策略基于安全保护需求设置。第三接收模块 1002 用于接收 UE 或网络实体发送的获取请求消息。第三发送模块 1003 用于向发送获取请求消息的相应 UE 返回第三存储模块 1001 中存储的安全算法列表、安全算法选择策略或安全算法选择策略 ID。

[0176] 本发明提供的另一个实施例的通信系统包括网络实体 1。该实施例的通信系统中，UE 中存储有该 UE 支持的安全算法列表，该安全算法列表基于不同的安全保护需求分别设置。网络实体 1 中存储有该网络实体 1 支持的安全算法列表或安全算法选择策略，其中的安全算法列表基于不同的安全保护需求分别设置，安全算法选择策略基于该网络实体 1 支持的安全算法列表设置。UE 生成并向网络实体 1 发送业务请求消息，该业务请求消息中包括 UE 支持的安全算法列表或其中与业务请求消息的安全保护需求对应的安全算法列表，以及接收网络实体 1 返回的安全算法，该安全算法由网络实体 1 根据业务请求消息的安全保护需求，从 UE 与网络实体 1 都支持的安全算法列表中选择得到。网络实体 1 接收 UE 发送的业务请求消息，根据网络实体 1 支持的安全算法列表或安全算法选择策略，与业务请求消息中携带的安全算法列表，从 UE 与网络实体 1 都支持的安全算法列表中选择与 UE 发送的业务请求消息的安全保护需求对应的安全算法，并将该选择的安全算法发送给 UE。该实施例的通信系统可用于实现如本发明图 4 所示实施例的流程，其中的 UE 可以采用图 13 所示实施例的 UE，网络实体 1 可以采用图 16 所示实施例的网络实体。如图 19 所示，为本发明通信系统另一个实施例的结构示意图。

[0177] 进一步地，本发明实施例的通信系统还可以包括应用服务器 3，用于存储该应用服务器 3 的安全算法列表、安全算法选择策略或安全算法选择策略 ID，其中的安全算法选择策略基于安全保护需求设置，应用服务器 3 存储的安全算法列表基于不同的安全保护需求分别设置，根据 UE 发送的获取请求消息，向 UE 返回该应用服务器 3 存储的安全算法列表、安全算法选择策略或安全算法选择策略标识。相应的，UE 还可以用于获取应用服务器 3 存储的安全算法列表、或其中与该安全保护需求对应的安全算法列表、安全算法选择策略或安全算法选择策略 ID，并通过业务请求消息发送给网络实体 1，或者，选择 UE 支持且应用服务器 3 存储的安全算法列表，或其中与安全保护需求对应的安全算法列表，并通过业务请求消息发送给网络实体 1。网络实体 1 根据该网络实体 1 支持的安全算法列表或安全算法选择策略，与业务请求消息中携带的安全算法列表，选择 UE 与网络实体 1 都支持且应用服务器 3 存储的、且与该安全保护需求对应的安全算法。该实施例的通信系统可用于实现如

本发明图 6 与图 7 所示实施例的流程，其中的 UE 可以采用图 15 与图 14 所示实施例的 UE，网络是实体 1 可以采用图 16 所示实施例中的相应网络实体。如图 20 所示，为本发明通信系统又一个实施例的结构示意图。

[0178] 如图 21 所示，为本发明 UE 再一个实施例的结构示意图，该实施例的 UE 可以实现本发明图 5 与图 8 所示实施例中的相应流程。其包括第一存储模块 801、第一发送模块 803、第一接收模块 804 与第三选择模块 806。其中，第一存储模块 801 用于存储该 UE 支持的安全算法列表，该安全算法列表基于不同的安全保护需求分别设置或用于表示该 UE 的安全能力。第一发送模块 803 用于生成并向网络实体发送业务请求消息。第一接收模块 804 用于接收网络实体返回的安全算法列表、安全算法选择策略或安全算法选择策略 ID，该安全算法列表为网络实体支持的安全算法列表，或其中与 UE 发送的业务请求消息的安全保护需求对应的安全算法列表，其中的安全算法选择策略基于网络实体支持的安全算法列表设置。第三选择模块 806 用于根据第一存储模块 801 中存储的安全算法列表，与第一接收模块 804 接收到的安全算法列表，从 UE 与网络实体都支持的安全算法列表中选择安全保护需求对应的安全算法。

[0179] 如图 22 所示，为本发明 UE 还一个实施例的结构示意图，该实施例的 UE 可以实现本发明图 9 所示实施例中的相应流程。与图 21 所示的实施例相比，该实施例的 UE 还包括第三获取模块 805，用于获取应用服务器存储的安全算法列表，或其中与 UE 发送的业务请求消息的安全保护需求对应的安全算法列表，或安全算法选择策略，或安全算法选择策略 ID，其中的安全算法选择策略基于安全保护需求设置。相应的，第三选择模块 806 根据第一存储模块 801 中存储的安全算法列表，与第三获取模块 805 从应用服务器获取到的安全算法列表、安全算法选择策略或安全算法选择策略 ID，与第一接收模块 804 接收到的网络实体的安全算法列表、安全算法选择策略或安全算法选择策略 ID，选择 UE 与网络实体都支持且应用服务器存储的、与 UE 发送的业务请求消息的安全保护需求对应的安全算法。

[0180] 如图 23 所示，为本发明网络实体又一个实施例的结构示意图，该实施例的网络实体可以实现本发明图 5 所示实施例中的相应流程。该实施例的网络实体包括第二存储模块 901、第二接收模块 902 与第四发送模块 907。其中，第二存储模块 901 用于存储网络实体支持的安全算法列表、安全算法选择策略或安全算法选择策略 ID，其中的安全算法列表基于不同的安全保护需求分别设置或用于表示该网络实体的安全能力，安全算法选择策略基于网络实体支持的安全算法列表设置。第二接收模块 902 用于接收 UE 发送的业务请求消息。第四发送模块 907 用于将第二存储模块 901 中存储的安全算法列表、其中与业务请求消息的安全保护需求对应的安全算法列表、安全算法选择策略或安全算法选择策略 ID 发送给 UE。

[0181] 如图 24 所示，为本发明网络实体再一个实施例的结构示意图，该实施例的网络实体可以实现本发明图 9 所示实施例中的相应流程。与图 23 所示的实施例相比，该实施例的网络实体还包括第四获取模块 905 与第二选择模块 903。其中，第四获取模块 905 用于获取应用服务器存储的安全算法列表、该安全算法列表中与安全保护需求对应的安全算法列表、安全算法选择策略或安全算法选择策略 ID，其中的安全算法选择策略基于安全保护需求设置，应用服务器存储的安全算法列表基于不同的安全保护需求分别设置。第二选择模块 903 用于根据第二存储模块 901 中存储的安全算法列表或安全算法选择策略，与第四获

取模块 905 获取的应用服务器存储的安全算法列表、安全保护需求对应的安全算法列表、安全算法选择策略或安全算法选择策略 ID，或者进一步选择网络实体支持且应用服务器存储的安全算法列表、安全保护需求对应的安全算法列表、安全算法选择策略或安全算法选择策略 ID。第四发送模块 907 将第二存储模块 901 中存储的安全算法列表或安全算法选择策略，与第四获取模块 905 获取的应用服务器存储的安全算法列表、安全保护需求对应的安全算法列表、安全算法选择策略或安全算法选择策略 ID 发送给 UE，或者将第二选择模块 903 选择的安全算法列表、安全保护需求对应的安全算法列表、安全算法选择策略或安全算法选择策略 ID 发送给 UE。

[0182] 本发明再一个实施例提供的通信系统中，UE 中存储有该 UE 支持的安全算法列表，该安全算法列表基于不同的安全保护需求分别设置。网络实体 1 中存储有该网络实体 1 支持的安全算法列表、安全算法选择策略或安全算法选择策略 ID，其中的安全算法列表基于不同的安全保护需求分别设置或相应表示 UE 或网络实体 1 的安全能力，安全算法选择策略基于网络实体 1 支持的安全算法列表设置。UE 生成并向网络实体 1 发送业务请求消息，以及接收网络实体 1 返回的安全算法列表、安全算法选择策略或安全算法选择策略 ID，其中的安全算法列表为网络实体 1 支持的安全算法列表或其中与业务请求消息的安全保护需求对应的安全算法列表，并根据 UE 存储的安全算法列表，与网络实体 1 返回的安全算法列表、安全算法选择策略或安全算法选择策略 ID，选择 UE 发送的业务请求消息的安全保护需求对应的安全算法。网络实体 1 用于接收 UE 发送的业务请求消息，将该网络实体 1 存储的安全算法列表、其中与业务请求消息的安全保护需求对应的安全算法列表、安全算法选择策略或安全算法选择策略 ID 发送给 UE。该实施例的通信系统可用于实现如本发明图 5 所示实施例的流程，其中的 UE 可以采用图 21 所示实施例的 UE，网络是实体 1 可以采用图 23 所示实施例中的相应网络实体。如图 25 所示，为本发明通信系统再一个实施例的结构示意图。

[0183] 进一步地，在上述通信系统中，还可以包括应用服务器 3，用于存储该应用服务器 3 的安全算法列表、安全算法选择策略或安全算法选择策略 ID，其中的安全算法选择策略基于安全保护需求设置，并根据 UE 发送的获取请求消息，向 UE 返回应用服务器 3 存储的安全算法列表、与 UE 发送的业务请求消息的安全保护需求对应的安全算法列表、安全算法选择策略或安全算法选择策略 ID，相应的，网络实体 1 还用于通过获取请求消息获取应用服务器 3 存储的安全算法列表、或其中与安全保护需求对应的安全算法列表、安全算法选择策略或安全算法选择策略 ID，并发送给 UE，或者选择网络实体 1 支持且应用服务器 3 存储的安全算法列表、安全保护需求对应的安全算法列表、安全算法选择策略或安全算法选择策略 ID，并发送给 UE。UE 根据 UE 存储的安全算法列表，和网络实体 1 返回的安全算法列表、安全算法选择策略或安全算法选择策略 ID，选择 UE 与网络实体 1 都支持且应用服务器 3 存储的、且与业务请求消息的安全保护需求对应的安全算法。该实施例的通信系统可用于实现如本发明图 9 所示实施例的流程，其中的 UE 可以采用图 22 所示实施例的 UE，网络实体 1 可以采用图 24 所示实施例中的相应网络实体。如图 26 所示，为本发明通信系统还一个实施例的结构示意图。

[0184] 本领域普通技术人员可以理解：实现上述方法实施例的全部或部分步骤可以通过程序指令相关的硬件来完成，前述的程序可以存储于一计算机可读取存储介质中，该程序

在执行时，执行包括上述方法实施例的步骤；而前述的存储介质包括：ROM、RAM、磁碟或者光盘等各种可以存储程序代码的介质。

[0185] 本发明实施例可以根据不同业务请求消息的安全保护需求选择不同的安全算法，以对相应的业务进行不同的安全保护，不但提高了业务的安全性，还可以综合考虑通信系统中各算法的复杂度与占用的开销，在对业务进行有效安全保护的同时提高通信系统的性能。

[0186] 最后所应说明的是：以上实施例仅用以说明本发明的技术方案，而非对本发明作限制性理解。尽管参照上述较佳实施例对本发明进行了详细说明，本领域的普通技术人员应当理解：其依然可以对本发明的技术方案进行修改或者等同替换，而这种修改或者等同替换并不脱离本发明技术方案的精神和范围。

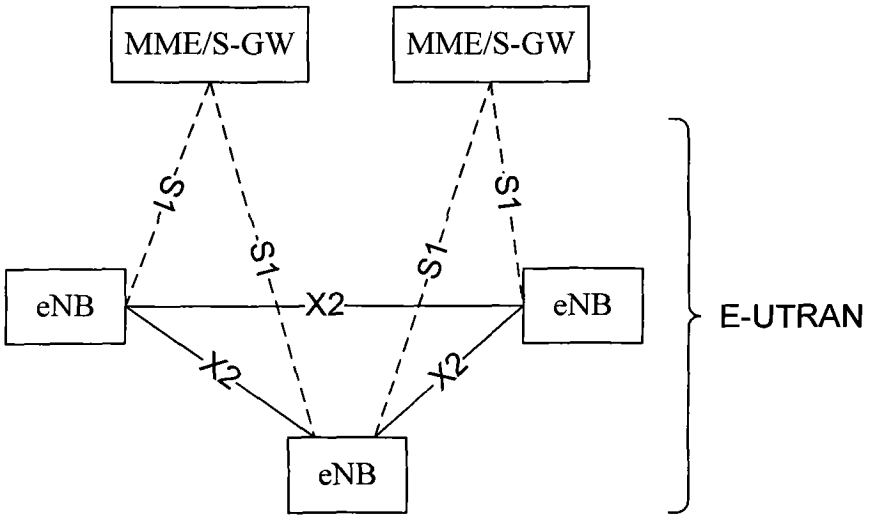

MME/S-GW
MME/S-GW
S1
S1
S1
S1
eNB
X2
eNB
X2
X2
eNB
E-UTRAN

图 1

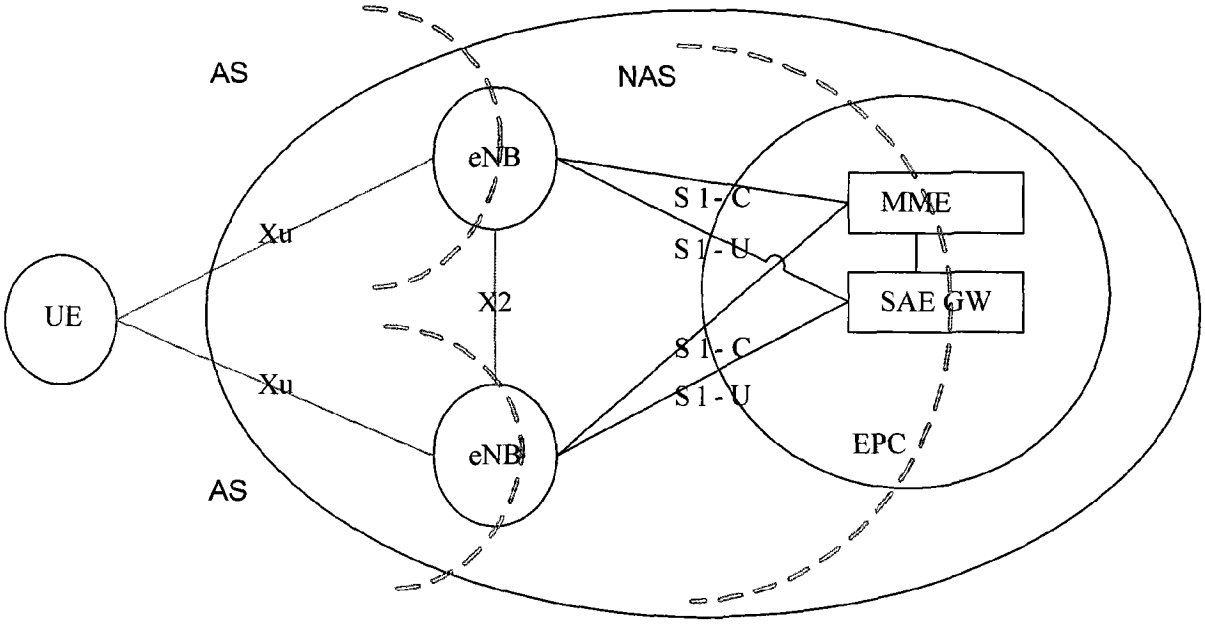

AS
NAS
eNB
S 1 - C
MME
Xu
S 1 - U
UE
X2
SAE GW
S 1 - C
Xu
S 1 - U
eNB
EPC
AS

图 2

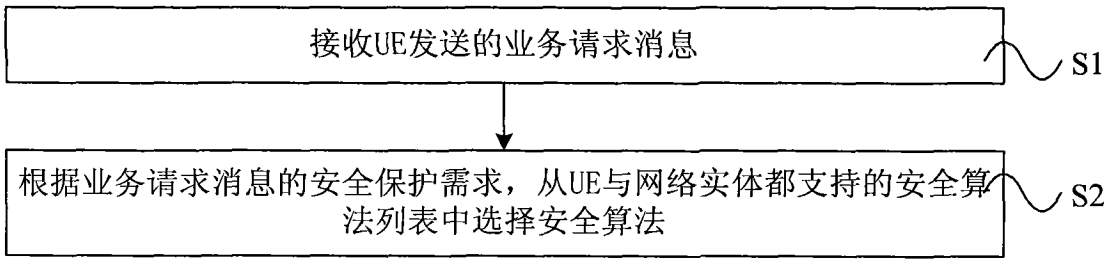

接收UE发送的业务请求消息
S1
根据业务请求消息的安全保护需求，从UE与网络实体都支持的安全算法列表中选择安全算法
S2

图 3

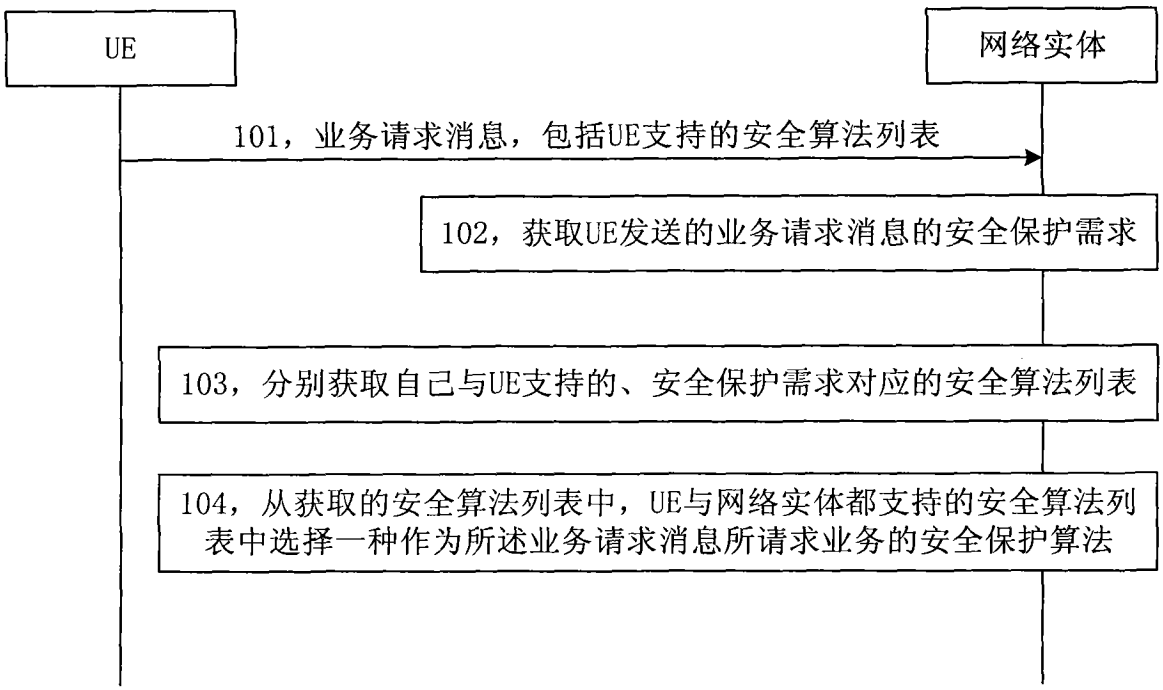

UE
网络实体
101，业务请求消息，包括UE支持的安全算法列表
102，获取UE发送的业务请求消息的安全保护需求
103，分别获取自己与UE支持的、安全保护需求对应的安全算法列表
104，从获取的安全算法列表中，UE与网络实体都支持的安全算法列表中选择一种作为所述业务请求消息所请求业务的安全保护算法

图 4

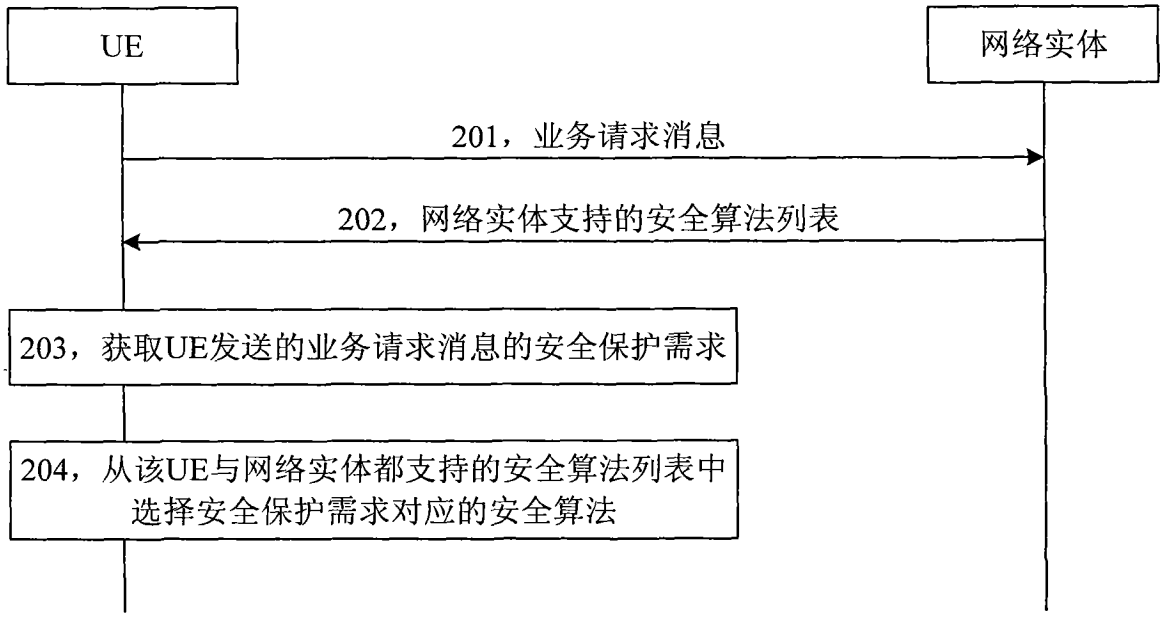

UE
网络实体
201，业务请求消息
202，网络实体支持的安全算法列表
203，获取UE发送的业务请求消息的安全保护需求
204，从该UE与网络实体都支持的安全算法列表中选择安全保护需求对应的安全算法

图 5

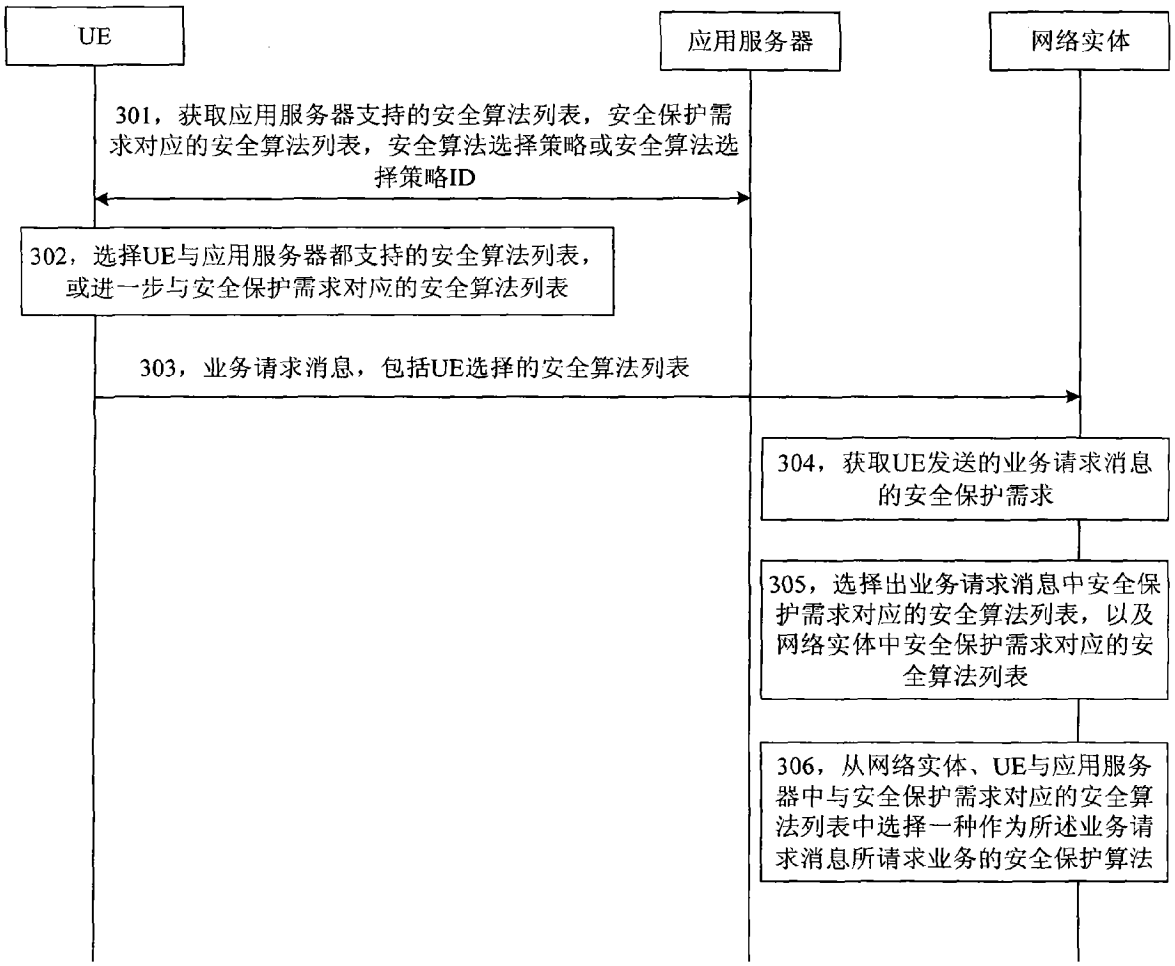

UE
应用服务器
网络实体
301，获取应用服务器支持的安全算法列表，安全保护需求对应的安全算法列表，安全算法选择策略或安全算法选择策略ID
302，选择UE与应用服务器都支持的安全算法列表，或进一步与安全保护需求对应的安全算法列表
303，业务请求消息，包括UE选择的安全算法列表
304，获取UE发送的业务请求消息的安全保护需求
305，选择出业务请求消息中安全保护需求对应的安全算法列表，以及网络实体中安全保护需求对应的安全算法列表
306，从网络实体、UE与应用服务器中与安全保护需求对应的安全算法列表中选择一种作为所述业务请求消息所请求业务的安全保护算法

图 6

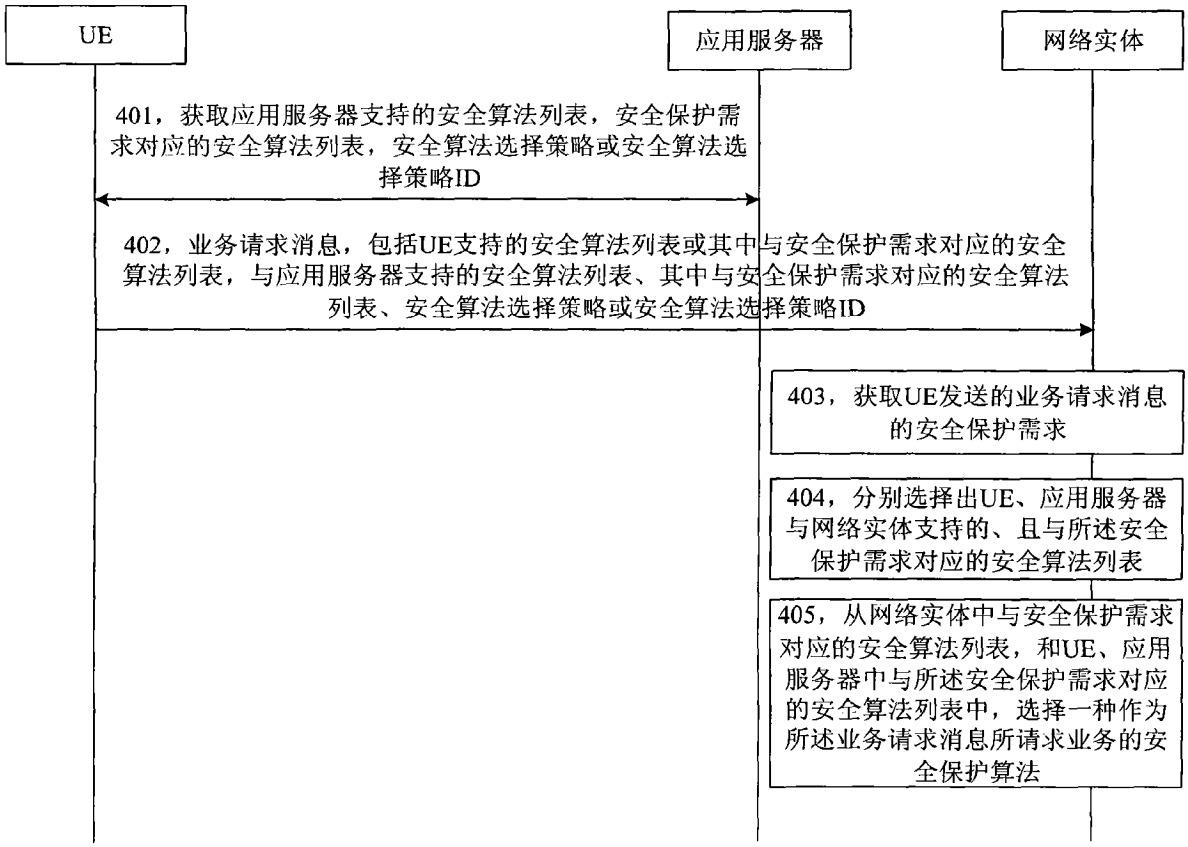

UE
应用服务器
网络实体
401，获取应用服务器支持的安全算法列表，安全保护需求对应的安全算法列表，安全算法选择策略或安全算法选择策略ID
402，业务请求消息，包括UE支持的安全算法列表或其中与安全保护需求对应的安全算法列表，与应用服务器支持的安全算法列表、其中与安全保护需求对应的安全算法列表、安全算法选择策略或安全算法选择策略ID
403，获取UE发送的业务请求消息的安全保护需求
404，分别选择出UE、应用服务器与网络实体支持的、且与所述安全保护需求对应的安全算法列表
405，从网络实体中与安全保护需求对应的安全算法列表，和UE、应用服务器中与所述安全保护需求对应的安全算法列表中，选择一种作为所述业务请求消息所请求业务的安全保护算法

图 7

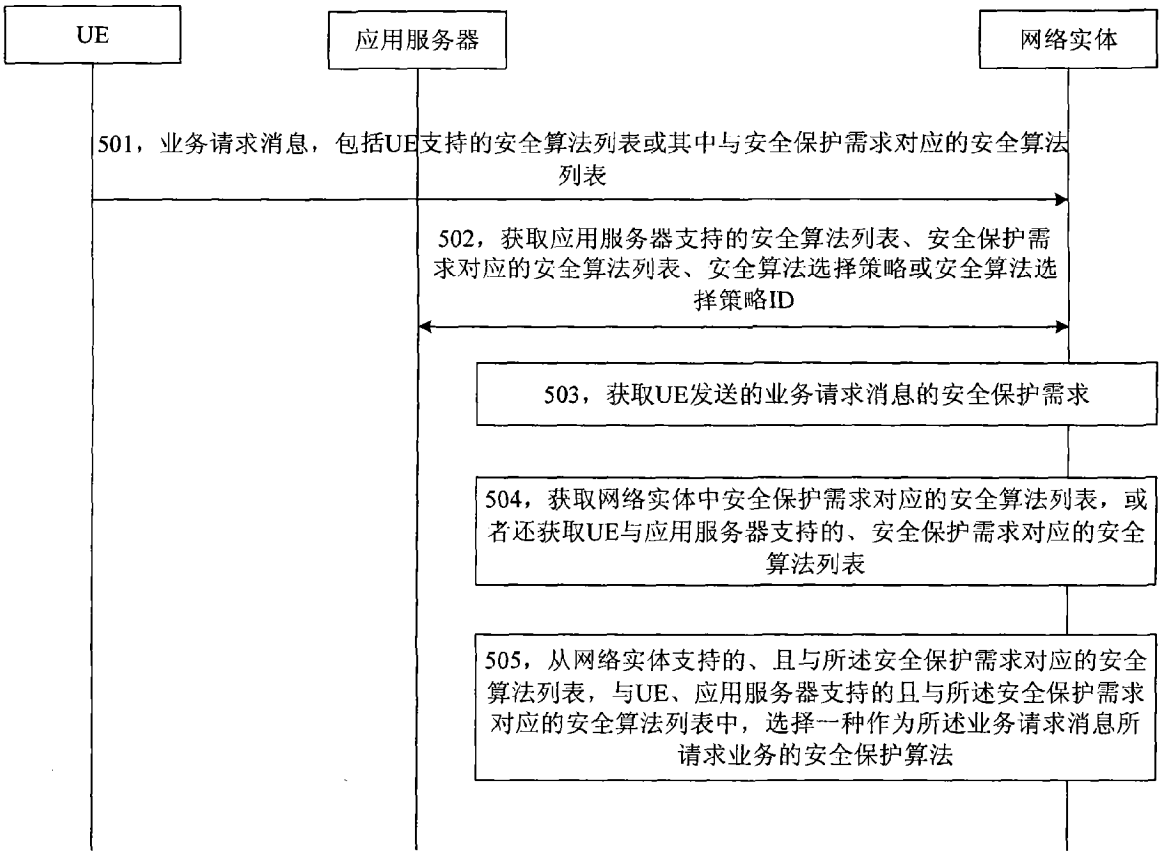

UE
应用服务器
网络实体
501，业务请求消息，包括UE支持的安全算法列表或其中与安全保护需求对应的安全算法列表
502，获取应用服务器支持的安全算法列表、安全保护需求对应的安全算法列表、安全算法选择策略或安全算法选择策略ID
503，获取UE发送的业务请求消息的安全保护需求
504，获取网络实体中安全保护需求对应的安全算法列表，或者还获取UE与应用服务器支持的、安全保护需求对应的安全算法列表
505，从网络实体支持的、且与所述安全保护需求对应的安全算法列表，与UE、应用服务器支持的且与所述安全保护需求对应的安全算法列表中，选择一种作为所述业务请求消息所请求业务的安全保护算法

图 8

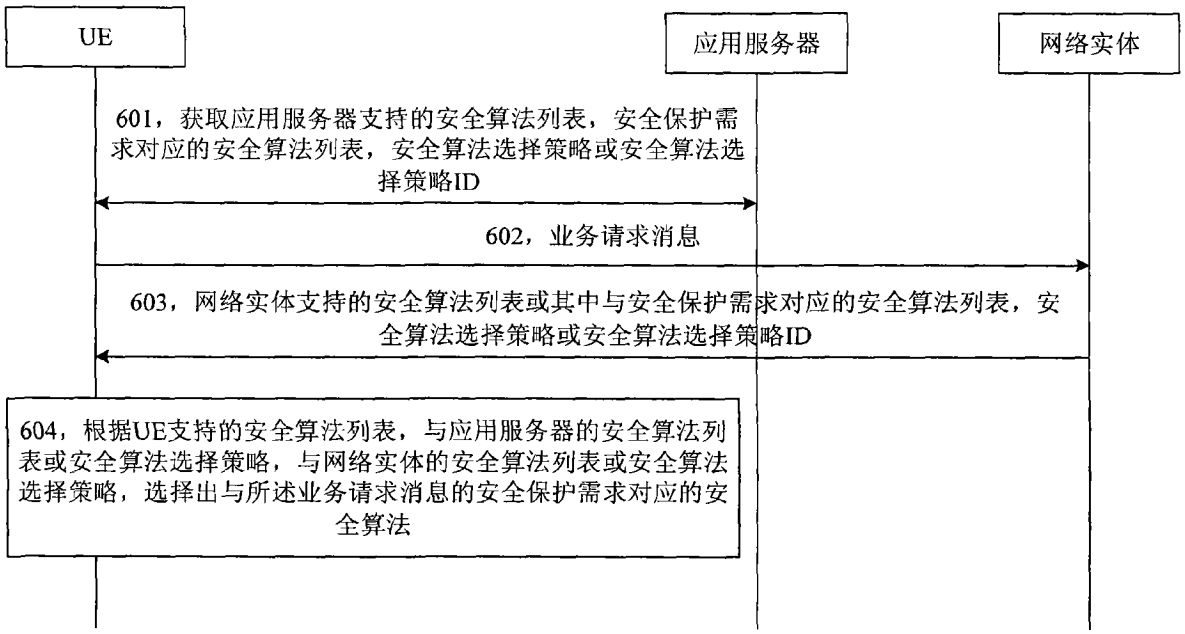

UE
应用服务器
网络实体
601，获取应用服务器支持的安全算法列表，安全保护需求对应的安全算法列表，安全算法选择策略或安全算法选择策略ID
602，业务请求消息
603，网络实体支持的安全算法列表或其中与安全保护需求对应的安全算法列表，安全算法选择策略或安全算法选择策略ID
604，根据UE支持的安全算法列表，与应用服务器的安全算法列表或安全算法选择策略，与网络实体的安全算法列表或安全算法选择策略，选择出与所述业务请求消息的安全保护需求对应的安全算法

图 9

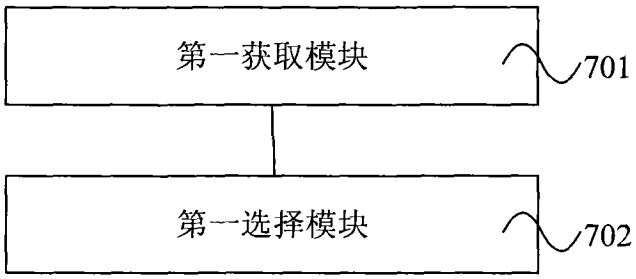

第一获取模块
701
第一选择模块
702

图 10

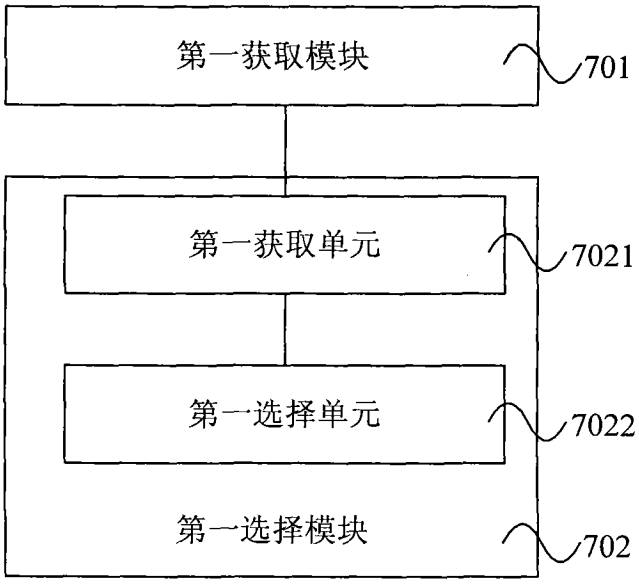

第一获取模块
701
第一获取单元
7021
第一选择单元
7022
第一选择模块
702

图 11

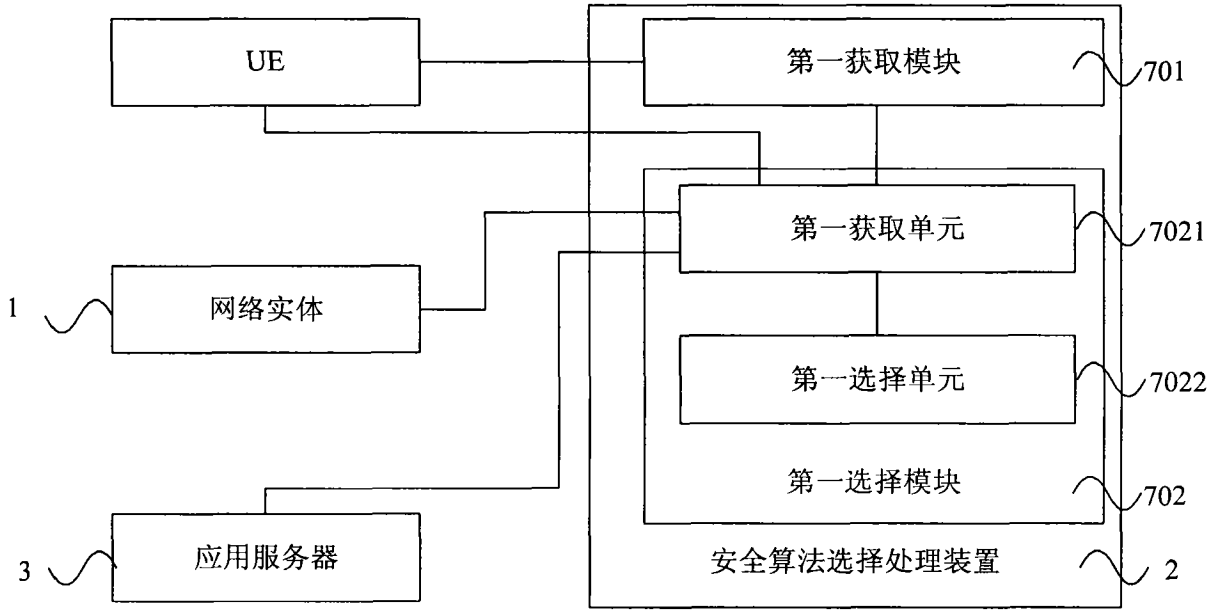

UE
第一获取模块
701
第一获取单元
7021
1
网络实体
第一选择单元
7022
第一选择模块
702
3
应用服务器
安全算法选择处理装置
2

图 12

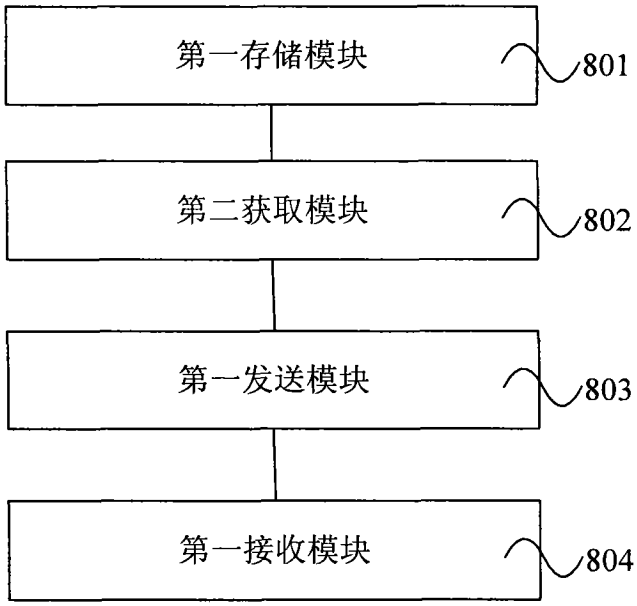

第一存储模块
801
第二获取模块
802
第一发送模块
803
第一接收模块
804

图 13

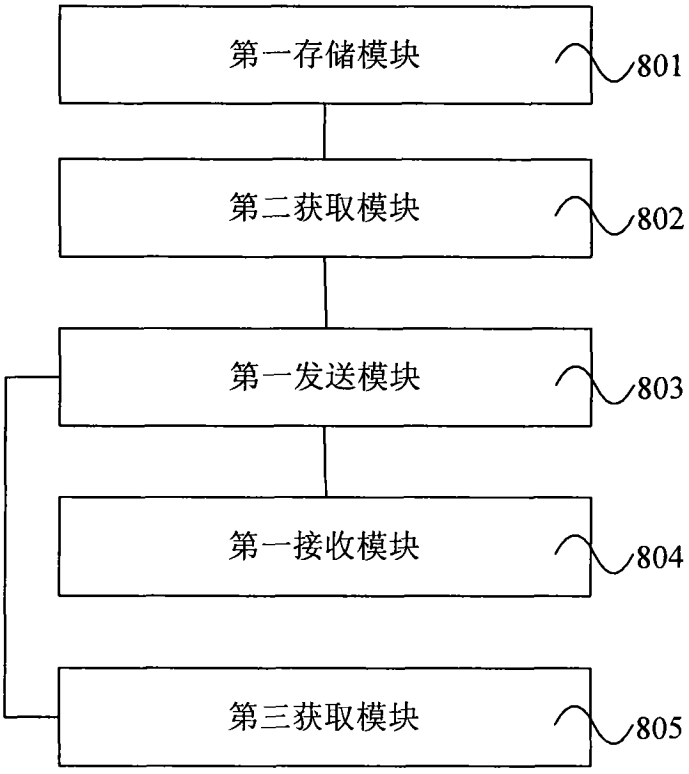

第一存储模块
801
第二获取模块
802
第一发送模块
803
第一接收模块
804
第三获取模块
805

图 14

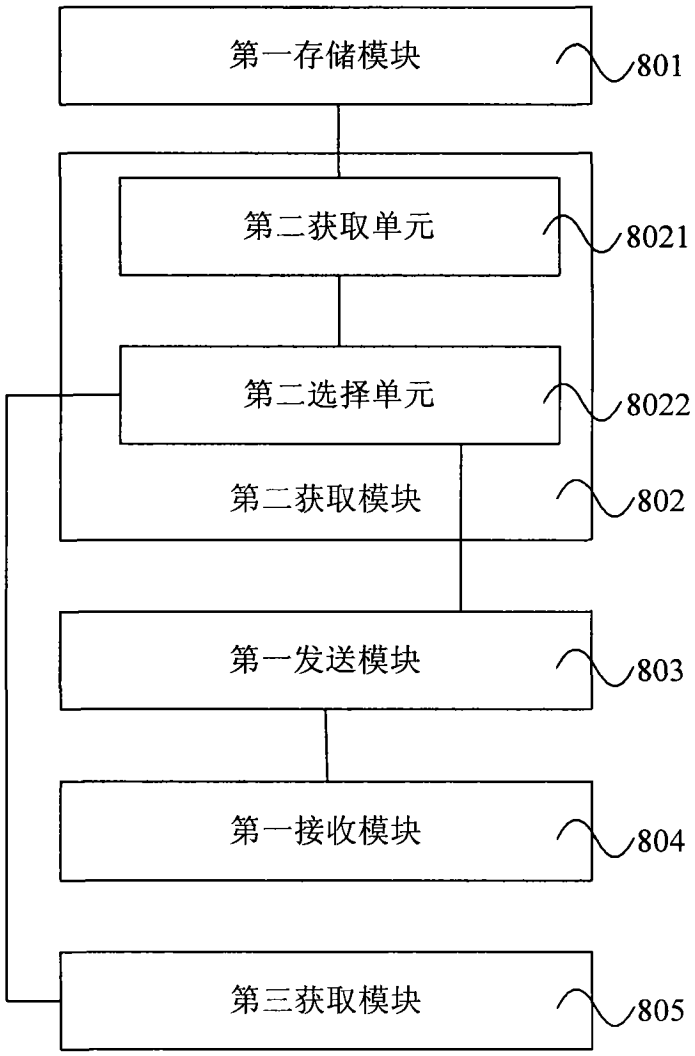

第一存储模块
801
第二获取单元
8021
第二选择单元
8022
第二获取模块
802
第一发送模块
803
第一接收模块
804
第三获取模块
805

图 15

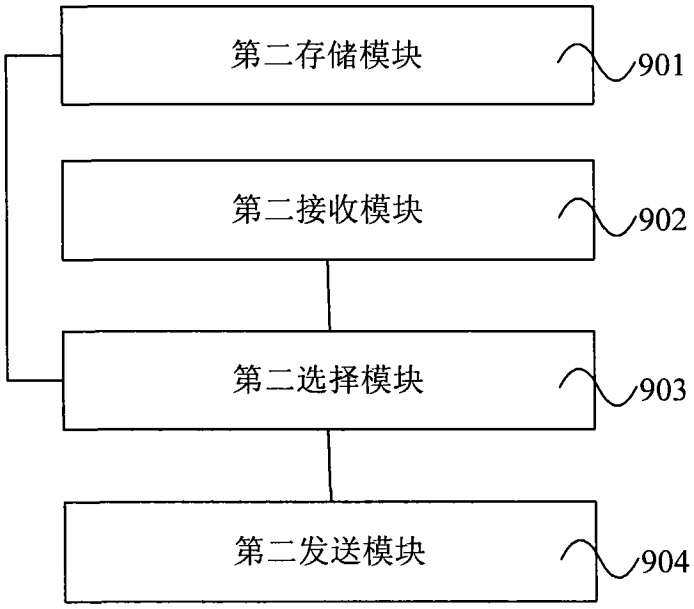

第二存储模块
901
第二接收模块
902
第二选择模块
903
第二发送模块
904

图 16

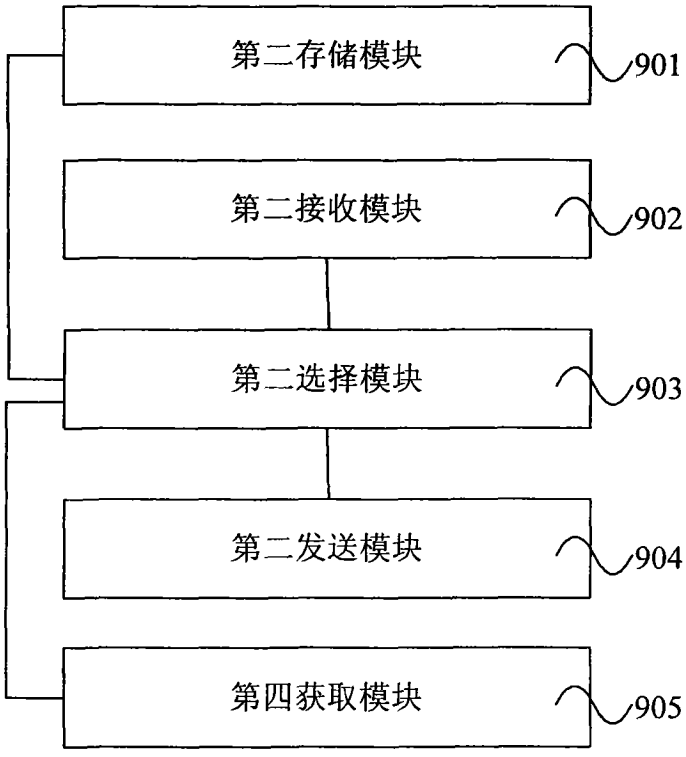

第二存储模块
901
第二接收模块
902
第二选择模块
903
第二发送模块
904
第四获取模块
905

图 17

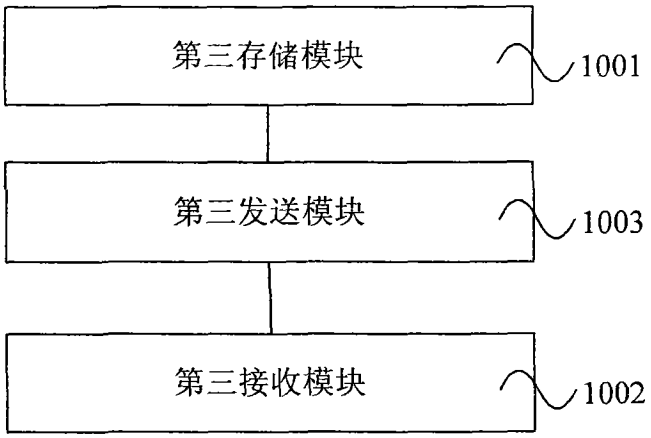

第三存储模块
1001
第三发送模块
1003
第三接收模块
1002

图 18

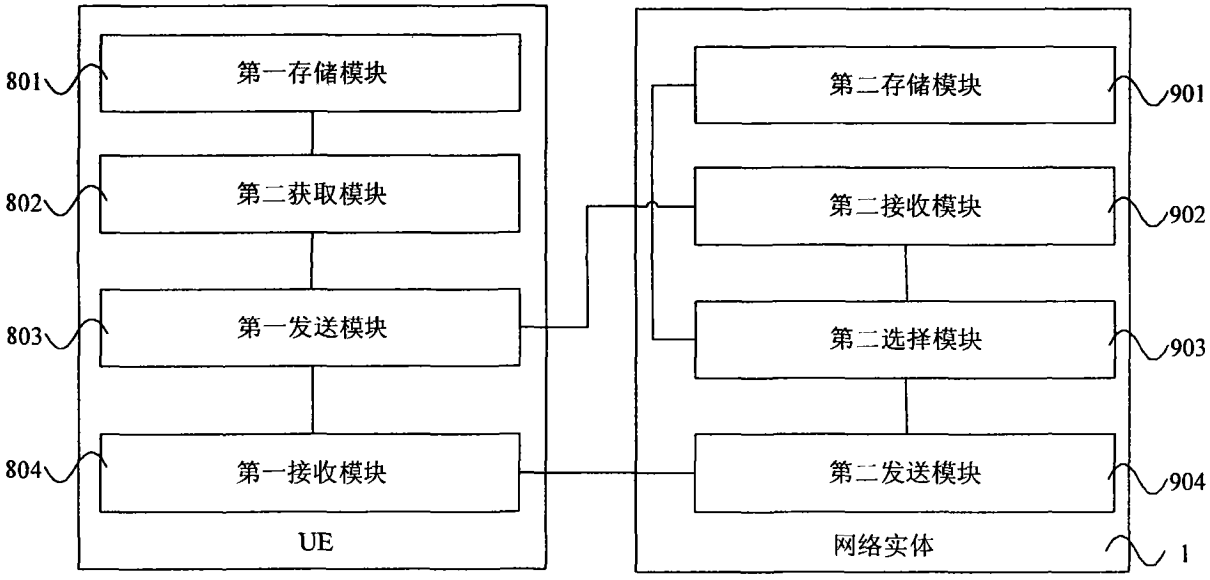

801
第一存储模块
802
第二获取模块
803
第一发送模块
804
第一接收模块
UE
第二存储模块
901
第二接收模块
902
第二选择模块
903
第二发送模块
904
网络实体
1

图 19

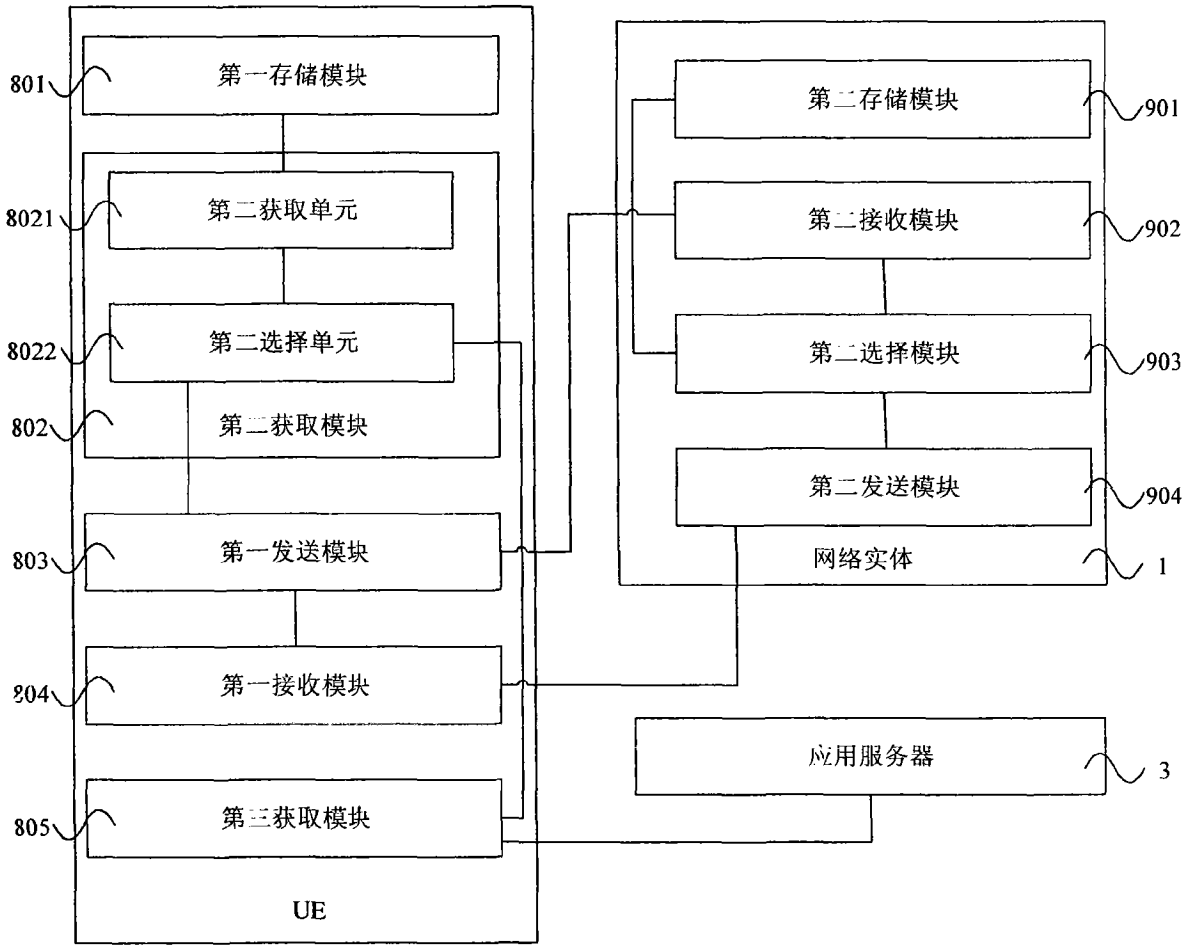

801
第一存储模块
8021
第二获取单元
8022
第二选择单元
802
第二获取模块
803
第一发送模块
804
第一接收模块
805
第三获取模块
UE
第二存储模块
901
第二接收模块
902
第二选择模块
903
第二发送模块
904
网络实体
1
应用服务器
3

图 20

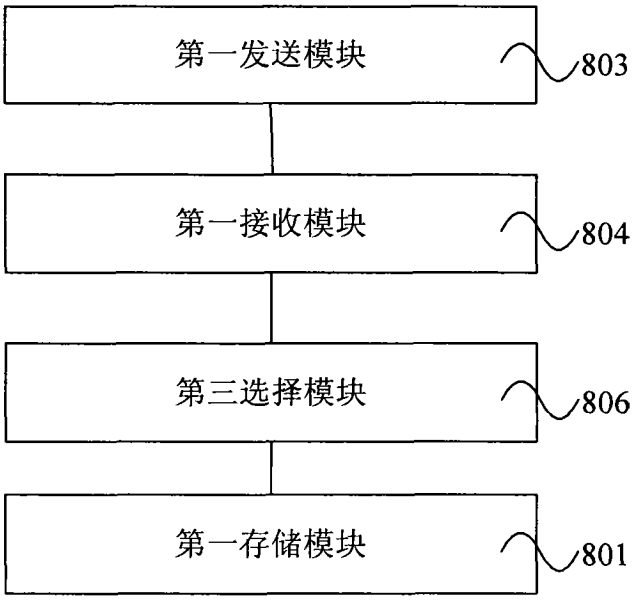

第一发送模块
803
第一接收模块
804
第三选择模块
806
第一存储模块
801

图 21

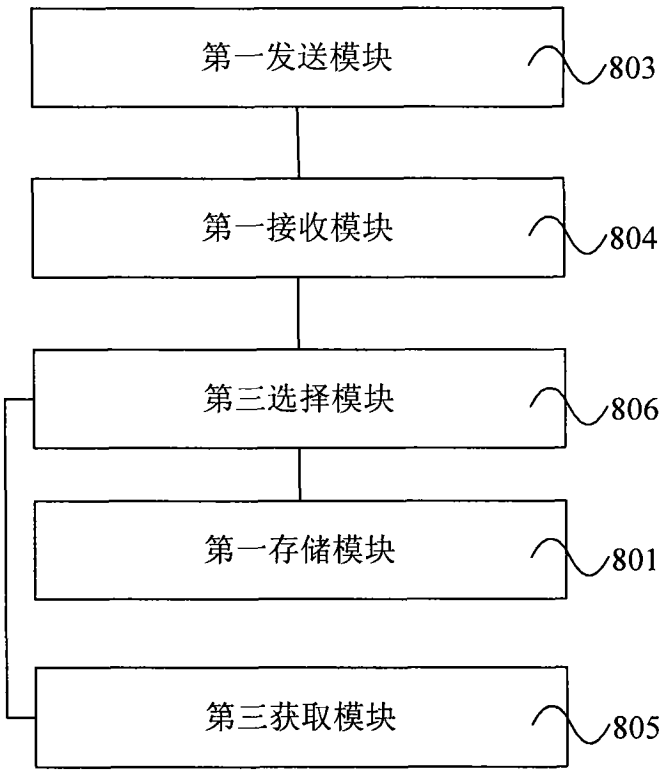

第一发送模块
803
第一接收模块
804
第三选择模块
806
第一存储模块
801
第三获取模块
805

图 22

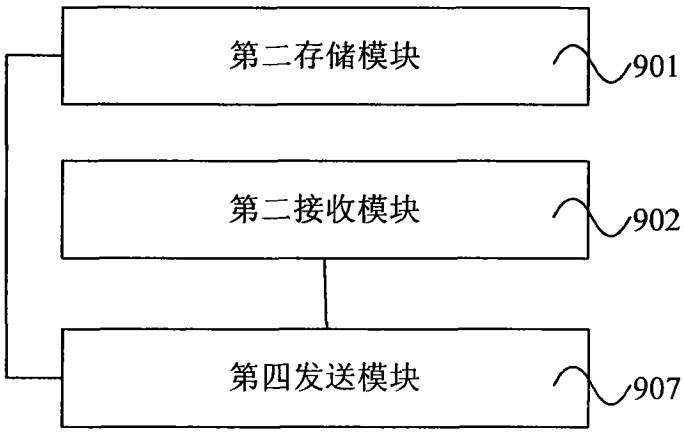

第二存储模块
901
第二接收模块
902
第四发送模块
907

图 23

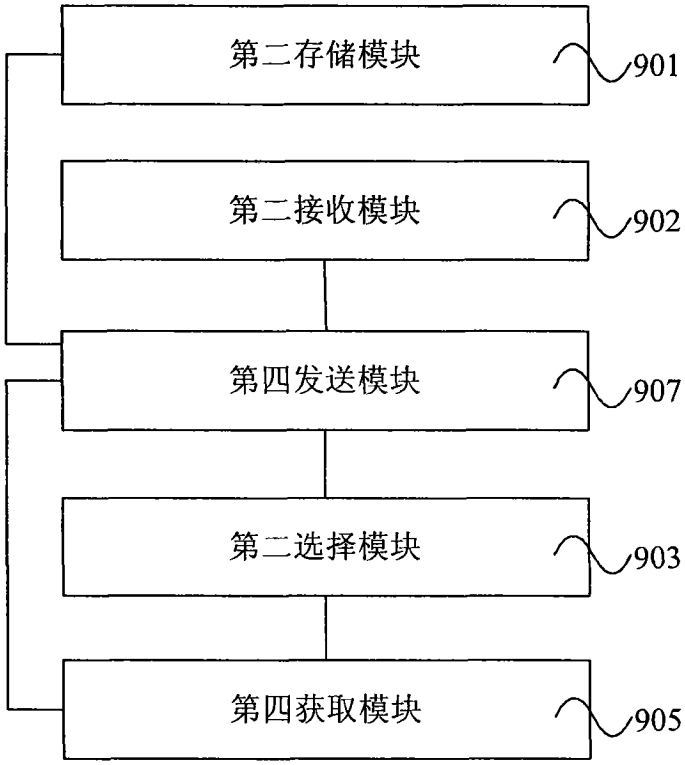

第二存储模块
901
第二接收模块
902
第四发送模块
907
第二选择模块
903
第四获取模块
905

图 24

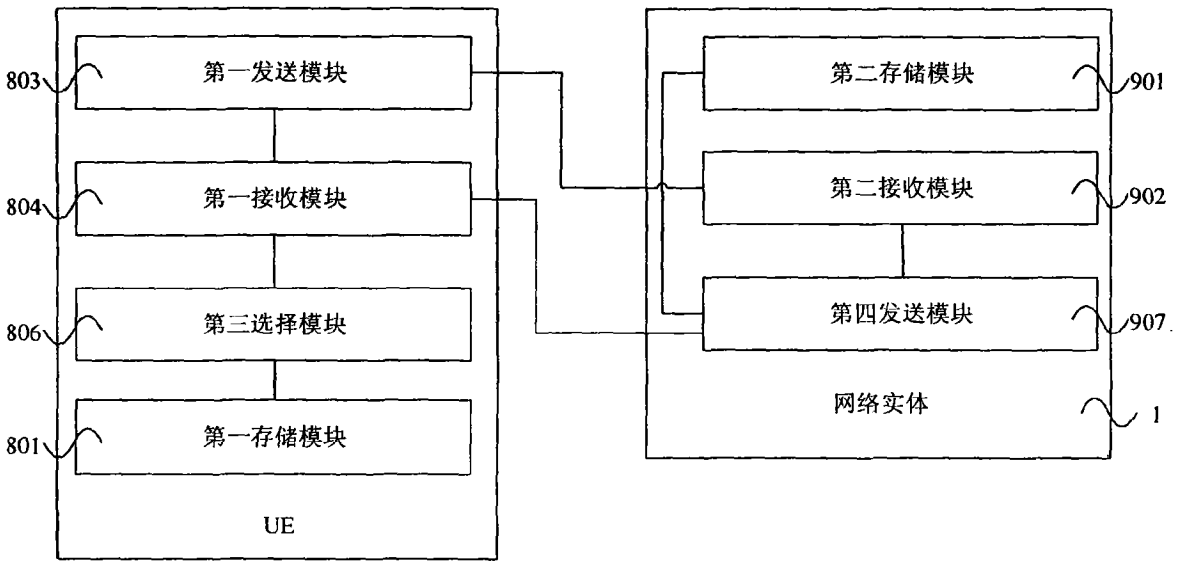

803
第一发送模块
804
第一接收模块
806
第三选择模块
801
第一存储模块
UE
第二存储模块
901
第二接收模块
902
第四发送模块
907
网络实体
1

图 25

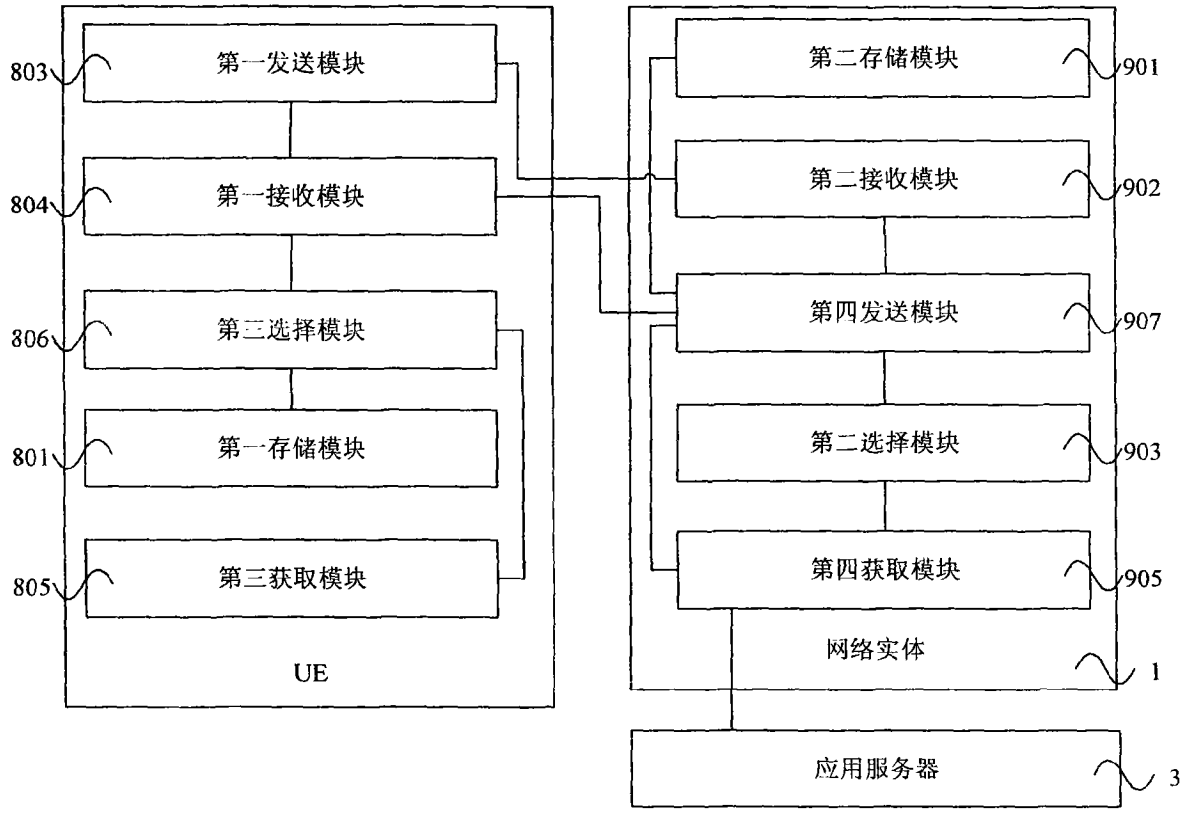

803
第一发送模块
804
第一接收模块
806
第三选择模块
801
第一存储模块
805
第三获取模块
UE
第二存储模块
901
第二接收模块
902
第四发送模块
907
第二选择模块
903
第四获取模块
905
网络实体
1
应用服务器
3

图 26