(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 104620537 A
(43)申请公布日 2015.05.13

(21)申请号 201280075685.5
(22)申请日 2012.09.11
(85)PCT国际申请进入国家阶段日
2015.03.09
(86)PCT国际申请的申请数据
PCT/KR2012/007294 2012.09.11
(87)PCT国际申请的公布数据
WO2014/042291 KO 2014.03.20
(71)申请人 全仁瑛
地址 韩国首尔市中浪区面牧洞统一路101街11-45申远海兹大厦203号
(72)发明人 全仁瑛
(74)专利代理机构 北京冠和权律师事务所 11399
代理人 朱健
(51)Int.Cl.
H04L 12/22(2006.01)
H04W 12/12(2006.01)

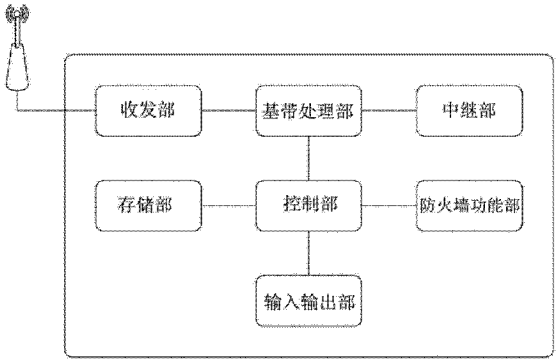
权利要求书2页 说明书6页 附图2页

(54)发明名称

具有防火墙功能的安全移动通信中继器

(57)摘要

本发明的安全移动通信中继器能够包括：基带处理部，其将在终端与移动通信网络基站之间所传输的移动通信信号进行基带调制解调而提取基带数据；控制部，其分析基带数据，并根据所设定的安全策略的违反判定结果而允许或拒绝基带数据的中继；存储部，其存储安全策略的设定信息；以及，防火墙功能部，其按照控制部的指示而对于包含在基带数据中的分组数据判定安全策略的违反与否。



CN 104620537 A

1. 一种安全移动通信中继器，其特征在于，包括：

基带处理部，其将在终端与移动通信网络基站之间所传输的移动通信信号进行基带调制解调而提取基带数据；

控制部，其分析上述基带数据，并根据所设定的安全策略的违反判定结果而允许或拒绝上述基带数据的中继；

存储部，其存储上述安全策略的设定信息；以及，

防火墙功能部，其按照上述控制部的指示而对于包含在上述基带数据中的分组数据判定安全策略的违反与否。

2. 根据权利要求 1 所述的安全移动通信中继器，其特征在于，

上述存储部进一步存储指定是要通过上述防火墙功能部或外部的防火墙设备中哪一个来执行安全策略的违反判定的防火墙选择信息，

上述控制部以根据上述防火墙选择信息来向上述防火墙功能部或外部的防火墙设备中至少一个提供上述分组数据的方式动作。

3. 根据权利要求 1 所述的安全移动通信中继器，其特征在于，

上述控制部在上述安全策略设定成不允许进行无线分组数据服务的情况下，并且在从终端接收的基带数据包含服务选项协商请求信号时，以向上述终端传输服务选项协商拒绝信号的方式动作。

4. 根据权利要求 1 所述的安全移动通信中继器，其特征在于，

上述控制部若判定为上述分组数据违反安全策略，则以向上述终端传输 PDP 上下文释放请求信号的方式动作。

5. 根据权利要求 4 所述的安全移动通信中继器，其特征在于，

上述控制部在终端请求服务选项协商时，存储上述终端的识别号码，并且若判定为上述分组数据违反安全策略，则以基于上述终端的所存储的识别号码而向上述终端传输 PDP 上下文释放请求信号的方式动作。

6. 根据权利要求 4 所述的安全移动通信中继器，其特征在于，

上述控制部若判定为上述分组数据违反安全策略，则以向上述移动通信网络基站传输 PDP 上下文释放请求信号的方式动作。

7. 一种安全移动通信中继方法，利用在终端与移动通信网络基站之间中继移动通信信号的安全中继器，所述安全移动通信中继方法其特征在于，包括：

上述安全中继器，

存储安全策略的设定信息的步骤；

对于将上述移动通信信号进行基带调制解调而得到的上述基带数据中所包含的分组数据，得到关于上述安全策略的违反与否的判定结果的步骤；以及，

仅在判定为未违反上述安全策略的情况下，允许上述基带数据的中继的步骤。

8. 根据权利要求 7 所述的安全移动通信中继方法，其特征在于，

进一步包括：

存储指定是要通过内置于上述安全中继器的防火墙功能部或外部的防火墙设备中哪一个来执行上述安全策略的违反判定的防火墙选择信息的步骤；以及，

根据上述防火墙选择信息，向上述防火墙功能部或外部的防火墙设备中至少一个提供

上述分组数据的步骤。

9. 根据权利要求 7 所述的安全移动通信中继方法，其特征在于，

进一步包括：

在上述安全策略设定成不允许进行无线分组数据服务的情况下，并且在从终端接收的基带数据中包含服务选项协商请求信号时，向上述终端传输服务选项协商拒绝信号的步骤。

10. 根据权利要求 7 所述的安全移动通信中继方法，其特征在于，

进一步包括：

若判定为上述分组数据违反安全策略，则向上述终端传输 PDP 上下文释放请求信号的步骤。

11. 根据权利要求 10 所述的安全移动通信中继方法，其特征在于，

进一步包括：

在终端请求服务选项协商时，存储上述终端的识别号码的步骤；以及，

若判定为上述分组数据违反安全策略，则基于上述终端的所存储的识别号码而向上述终端传输 PDP 上下文释放请求信号的步骤。

12. 根据权利要求 10 所述的安全移动通信中继方法，其特征在于，

进一步包括：

若判定为上述分组数据违反安全策略，则向上述移动通信网络基站传输 PDP 上下文释放请求信号的步骤。

具有防火墙功能的安全移动通信中继器

技术领域

[0001] 本发明涉及移动通信中继器，更详细地讲，涉及小型移动通信中继器。

背景技术

[0002] 过去主要是在不太好接收外部基站信号的室内为了对于那种阴影位置提供移动通信服务而使用的移动通信中继器起着单一的信号中继作用，即、接收基站的信号并发出法所允许的低功率的信号或接收移动通信终端的信号并向基站传递所接收信号。

[0003] 然而最近，移动通信服务和技术的中心从语音服务急剧向无线数字数据服务转移，在数据服务的情况下，从 3G 服务转换为 4G 服务等，以能够稳定且快速传输的状态在发展。

[0004] 而且，始终与通信网络连接且能够高效处理办公业务的智能手机在急剧普及，因而有可能通过智能手机和移动通信服务而瞬间泄密，也不能排除反过来恶意代码通过智能手机而侵入公司内部网络的可能性。

[0005] 在这种无线环境下，在公司内仅将办公用电脑和内部网络用硬件作为对象而构建的安全系统通过智能手机和移动通信服务而易于泄密或被入侵，且处于易受恶意代码的传播攻击的状态。

发明内容

[0006] 技术问题

[0007] 本发明所要解决的问题在于提供一种能够在室内的移动通信终端与外部的基站之间中继信号并能够提供安全功能的、具有防火墙功能的安全移动通信中继器。

[0008] 解决问题方案

[0009] 根据本发明的一实施方式的安全移动通信中继器能够包括 ：

[0010] 基带处理部，其将在终端与移动通信网络基站之间所传输的移动通信信号进行基带调制解调而提取基带数据 ；

[0011] 控制部，其分析上述基带数据，并根据所设定的安全策略的违反判定结果而允许或拒绝上述基带数据的中继 ；

[0012] 存储部，其存储上述安全策略的设定信息 ；以及，

[0013] 防火墙功能部，其按照上述控制部的指示而对于包含在上述基带数据中的分组数据判定安全策略的违反与否。

[0014] 根据一实施例，上述存储部能够进一步存储指定是要通过上述防火墙功能部或外部的防火墙设备中哪一个来执行安全策略的违反判定的防火墙选择信息，

[0015] 上述控制部能够以根据上述防火墙选择信息来向上述防火墙功能部或外部的防火墙设备中至少一个提供上述分组数据的方式动作。

[0016] 根据一实施例，上述控制部在上述安全策略设定成不允许进行无线分组数据服务的情况下，并且在从终端接收的基带数据包含服务选项协商请求信号时，能够以向上述终

端传输服务选项协商拒绝信号的方式动作。

[0017] 根据一实施例，上述控制部若判定为上述分组数据违反安全策略，则能够以向上述终端传输 PDP（分组数据协议）上下文释放请求信号的方式动作。

[0018] 根据一实施例，上述控制部在终端请求服务选项协商时，存储上述终端的识别号码，并且若判定为上述分组数据违反安全策略，则能够以基于上述终端的所存储的识别号码而向上述终端传输 PDP 上下文释放请求信号的方式动作。

[0019] 根据一实施例，上述控制部若判定为上述分组数据违反安全策略，则能够以向上述移动通信网络基站传输 PDP 上下文释放请求信号的方式动作。

[0020] 根据本发明的另一实施方式的安全移动通信中继方法，利用在终端与移动通信网络基站之间中继移动通信信号的安全中继器，所述安全移动通信中继方法能够包括：

[0021] 上述安全中继器，

[0022] 存储安全策略的设定信息的步骤；

[0023] 对于将上述移动通信信号进行基带调制解调而得到的上述基带数据中所包含的分组数据，得到关于上述安全策略的违反与否的判定结果的步骤；以及，

[0024] 仅在判定为未违反上述安全策略的情况下，允许上述基带数据的中继的步骤。

[0025] 根据一实施例，上述安全移动通信中继方法，能够进一步包括：

[0026] 存储指定是要通过内置于上述安全中继器的防火墙功能部或外部的防火墙设备中哪一个来执行上述安全策略的违反判定的防火墙选择信息的步骤；以及，

[0027] 根据上述防火墙选择信息，向上述防火墙功能部或外部的防火墙设备中至少一个提供上述分组数据的步骤。

[0028] 根据一实施例，上述安全移动通信中继方法，能够进一步包括：

[0029] 在上述安全策略设定成不允许进行无线分组数据服务的情况下，并且在从终端接收的基带数据中包含服务选项协商请求信号时，向上述终端传输服务选项协商拒绝信号的步骤。

[0030] 根据一实施例，上述安全移动通信中继方法，能够进一步包括：

[0031] 若判定为上述分组数据违反安全策略，则向上述终端传输 PDP 上下文释放请求信号的步骤。

[0032] 根据一实施例，上述安全移动通信中继方法，能够进一步包括：

[0033] 在终端请求服务选项协商时，存储上述终端的识别号码的步骤；以及，

[0034] 若判定为上述分组数据违反安全策略，则基于上述终端的所存储的识别号码而向上述终端传输 PDP 上下文释放请求信号的步骤。

[0035] 根据一实施例，上述安全移动通信中继方法，能够进一步包括：

[0036] 若判定为上述分组数据违反安全策略，则向上述移动通信网络基站传输 PDP 上下文释放请求信号的步骤。

[0037] 发明效果

[0038] 根据本发明的安全移动通信中继器，在需要安全的区域内对于移动通信终端提供无线数据服务时，能够控制服务的启动和停止以及分组的中继。

[0039] 根据本发明的安全移动通信中继器，能够依旧利用现有的防火墙设备而在进行无线数据服务时提供安全。

[0040] 而且，根据本发明的安全移动通信中继器，在存在违反安全策略的活动的情况下，分别向进行通信中的移动通信终端和服务器侧传输连接释放消息，从而能够减少通信负载。

[0041] 进而，根据本发明的安全移动通信中继器，由于能够依旧利用现有的协议而提供安全，因而不仅能够在通常称之为功能手机（feature phone）的一般手机终端或智能手机上适用既定的安全策略，甚至在PC所尝试的网络共享（tethering）的情况下也能够适用既定的安全策略。

附图说明

[0042] 图1是例示了利用根据本发明一实施例的具有防火墙功能的安全移动通信中继器的移动通信系统的示意图。

[0043] 图2是示意性地例示了根据本发明一实施例的具有防火墙功能的安全移动通信中继器的框图。

[0044] 图3是例示了根据本发明一实施例的具有防火墙功能的安全移动通信中继器的消息流的流程图。

具体实施方式

[0045] 对于本文中所公开的本发明的各实施例而言，特定的构造性乃至功能性说明只是为了说明本发明的实施例之目的而例示的，本发明的各实施例能够以多种方式实施，不得解释为限定于本文中所说明的各实施例。

[0046] 下面要参照各附图而更为详细地说明本发明的优选实施例。对于附图中的相同的构成要素使用相同的附图标记并对于相同的构成要素省略重复的说明。

[0047] 图1是例示了利用根据本发明一实施例的具有防火墙功能的安全移动通信中继器的移动通信系统的示意图。

[0048] 参照图1，移动通信系统10能够通过移动通信终端11、安全移动通信中继器12、外部防火墙设备13、防火墙管理服务器14、外部移动通信中继器15、基站16、以及应用服务器17来说明。

[0049] 在如办公室那样需要安全服务的场所设置用于移动通信服务的具有防火墙功能的安全移动通信中继器（以下称为安全中继器）12，而以通过这种安全中继器12才能提供移动通信服务的方式设置各安全中继器12。

[0050] 例如，由于移动通信终端11通常自动选择所接收的移动通信电波中强度最强的基站，因而在办公室内若安全中继器12的信号比房屋外部的基站16的信号更强，则移动通信终端11仅与安全中继器12连接。

[0051] 移动通信终端11能够包括智能手机、一般手机、平板电脑（Tablet PC）、掌上电脑（Personal Digital Assistant，PDA）等，通过这种终端和网络共享（tethering）而要利用无线数据服务的电脑也可以包括在这一范畴。

[0052] 移动通信终端11经安全中继器12而与外部移动通信中继器15、基站16连接，并经基站16所代表的移动通信分组交换网络就能够与如网络服务那样提供实质性互联网服务的应用服务器17连接。

[0053] 此时，外部移动通信中继器 15 只是起着连接负责室内的信号中继的安全中继器 12 与外部的基站 16 之间的作用。安全中继器 12 与外部移动通信中继器 15 能够通过有线例如光缆连接。

[0054] 外部防火墙设备 13 是选择性的构成要素，安全中继器 12 能够驱动自身就提供防火墙功能的内部防火墙功能部和外部防火墙设备 13 中至一个而适用安全策略。

[0055] 防火墙管理服务器 14 能够设定并管理外部防火墙设备 13 或安全中继器 12 内部的防火墙功能部的安全策略。

[0056] 安全中继器 12 从移动通信终端 11 为了经移动通信基站 16 与应用服务器 17 连接而收发的各信息中将终端识别信息和 IP 信息提取而存储，并对于移动通信终端 11 所尝试的无线数据分组传输，通过防火墙管理服务器 14 并按照管理者所设定的安全策略，从一开始就拒绝无线数据分组传输本身，或驱动内置的防火墙功能或外部防火墙设备 13，从而能够实行与所传输的无线数据分组相关的具体安全策略。

[0057] 进而，安全中继器 12 在无线数据分组违反安全策略的情况下，不仅拒绝传输相应分组，而且分别向移动通信终端 11 和基站 16 发送请求连接释放的信号（例如，撤销 PDP 上下文信息）而能够结束无线分组数据服务。

[0058] 图 2 是示意性地例示了根据本发明一实施例的具有防火墙功能的安全移动通信中继器的框图。

[0059] 参照图 2，安全移动通信中继器 12 能够包括天线 121、收发部 122、基带处理部 123、控制部 124、中继部 125、存储部 126、防火墙功能部 127、以及输入输出部 128。

[0060] 首先，移动通信信号在与安全中继器 12 连接的终端 11 与安全中继器 12 之间经天线 121 和收发部 122 而被接收，并下行调制成基带信号之后在基带处理部 123 以语音通信或数据通信中之一进行处理。

[0061] 数据分组从基带处理部 123 经控制部 124 和中继部 125 而向外部中继器 15 传递，并经基站 16 而传递至应用服务器 17。

[0062] 这里，在安全中继器 12 通过光缆与外部中继器 15 连接的情况下，能够以光输入输出端口来具体实现中继部 125。在安全中继器 12 通过无线与外部中继器 15 连接的情况下，能够以无线收发器来具体实现中继部 125，而此时能够与天线 121 和收发部 122 另行具体实现无线收发器，还能够以共享一定部分的方式设计无线收发器。

[0063] 控制部 124 参照存储于存储部 126 的安全策略设定信息和防火墙选择信息来能够决定是否对于数据分组适用安全策略，而且能够决定通过内部的防火墙功能部 127 或外部防火墙设备 13 中哪一个来判定安全策略的违反与否。

[0064] 为此，控制部 124 分析从移动通信终端 11 所传输的数据分组而分别获取终端 11 的识别信息（例如电话号、ENS、IMEI、SIM、MSN、PIN 等）和赋予于终端 11 的 IP 信息，进而获取分组的目的地即应用服务器 17 的 IP 信息，并将这些信息存储于存储部 126。

[0065] 而且，控制部 124 能够在存储部 126 存储由防火墙管理服务器 14 所指定的安全策略设定信息。此时，能够根据终端的号码或识别信息而相异地设定安全策略。

[0066] 以由防火墙管理服务器 14 所适用安全策略的方式设定防火墙功能部 127，而且，在设定成能够利用内部防火墙功能部 127 的情况下，防火墙功能部 127 按照所指定的安全策略而分析在终端 11 与应用服务器 17 之间所传输的分组并判定是符合安全策略还是违反

安全策略。

[0067] 在防火墙功能部 127 判定为所传输的分组违反安全策略的情况下，控制部 124 参照存储于存储部 126 的相应终端 11 的识别信息和应用服务器 17 的 IP 信息，并对各个信息生成包括 PDP 上下文释放在内的连接终止信号而向终端 11 和应用服务器 17 传输，且对于相应分组，不是向中继部 125 传递而是丢弃，从而以阻止中继动作的方式进行控制。

[0068] 输入输出部 128 使得防火墙管理服务器 14 能够与安全中继器 12 连接而设定各种安全策略。而且，控制部 124 能够通过输入输出部 128 而与外部防火墙设备 13 进行通信以便能够委托分组的分析。

[0069] 图 3 是例示了根据本发明一实施例的具有防火墙功能的安全移动通信中继器的消息流的流程图，例示性地、基于在 3GPP2 标准中在终端与网络基站之间所进行的服务选项协商。

[0070] 在 3GPPS 标准中 TIA:TSB58 明确了在移动通信终端启动无线移动通信服务时首先在终端与基站之间对于应该利用何种服务而进行服务选项协商 (service option negotiation) 的过程。

[0071] 服务选项随移动技术的发展而扩大，但根据网络设备状况而有可能提供不了特定服务。为了应对这一问题，在提供服务之前就规定了在终端与基站之间协商的过程，这就是服务选项协商。

[0072] 服务选项协商是请求服务的主体对于所要使用相应服务的意图和对方装置或中间设备能否提供那种服务提出询问并应答的过程。

[0073] 参照图 3，首先在步骤 S31，用户为了在位于安全中继器 12 的工作范围内的终端 11 与特定的应用服务器 17 之间建立数据传输路径，而向安全中继器 12 发送包括终端 11 的识别信息在内的服务选项协商请求信号 (Service_Option_Request 信号)。

[0074] 在步骤 S32，安全中继器 12 存储终端 11 的识别信息，并且判定终端 11 所请求的服务是否为无线数据服务。在例如为语音服务或短信服务而非为无线数据服务的情况下，允许相应服务并使终端 11 与基站 16 连接。

[0075] 在所请求的服务为无线数据服务的情况下，在步骤 S33，安全中继器 12 参照所设定的安全策略而判定无线数据服务是否被允许。

[0076] 若是无线数据服务在安全策略上未被允许的状态，则在步骤 S34，安全中继器 12 停止服务选项协商请求的中继并向终端 11 传递拒绝服务选项协商的信号 (Service_Option_Reject)。在该情况下，终端 11 显示为不能利用无线数据服务并终止连接尝试。

[0077] 在无线数据服务在安全策略上被允许的情况下，在步骤 S35，安全中继器 12 向基站 16 传递服务选项协商请求信号，接着，若从基站 16 接收服务选项的接受 (Sevice_Option_Accept) 或拒绝信号，则安全中继器 12 将它照直向终端 11 中继。

[0078] 服务所接受的终端 11 在步骤 S36 通过安全中继器 12 而向基站 16 请求 PDP 上下文 (Packet Data Protocol context) 以能够得到用于利用各种分组数据服务的信息的集合即 PDP 上下文，并从基站 16 接收 PDP 上下文。PDP 上下文能够包括 PDP 的种类 (IP 或 PPP)、PDP 地址与其种类、QoS(Quality of Service，服务质量) 简档、认证、DNS 等各参数。终端 11 通过接收 PDP 上下文信息的过程而被分配 IP 地址并能够设定 QoS。

[0079] 这样一来，终端 11 成为结束了使用实际想要利用的分组服务的准备的状态，在步

骤 S37，将关于所希望的无线分组服务的分组生成并发送。

[0080] 在步骤 S38，安全中继器 12 能够按照设定通过内部防火墙功能部 127 或外部防火墙设备 13 中某一个而分析从终端 11 或应用服务器 17 接收的分组，并能够判定所接收的分组是否违反安全策略。

[0081] 在步骤 S39，在分组不违反安全策略的情况下，安全中继器 12 向基站 16 或终端 11 允许相应分组的中继。

[0082] 在步骤 S40，在判定为违反了分组安全策略的情况下，安全中继器 12 丢弃相应分组，进而为了强行终止相应无线分组服务，参照之前所存储的终端 11 的识别信息而向相应终端 11 传输请求释放 PDP 上下文的信号 (Deactivate_PDP_Context_Request)。

[0083] 虽然经步骤 S40 而不会进一步进行分组数据服务，但根据需要，例如在终端 11 所连接中的应用服务器 17 在等待接收分组的情况下，或在服务器 17 继续传输恶意代码的情况下，在步骤 S41，安全中继器 12 向基站 16 也传输告知 PDP 上下文的释放的信号 (Deactivate_PDP_Context_Request)。

[0084] 虽然通过有限的实施例和附图来如上说明了本发明，但本发明并不限定于上述的实施例，本领域普通技术人员根据这些描述能够进行多种修改和变形。因此，可谓本发明的思想仅由所付的权利要求书所解释，且与其等同或等价的变形均属于本发明思想的范畴。

[0085] 工业上利用可能性

[0086] 本发明能够应用于多种方式的通信中继器。

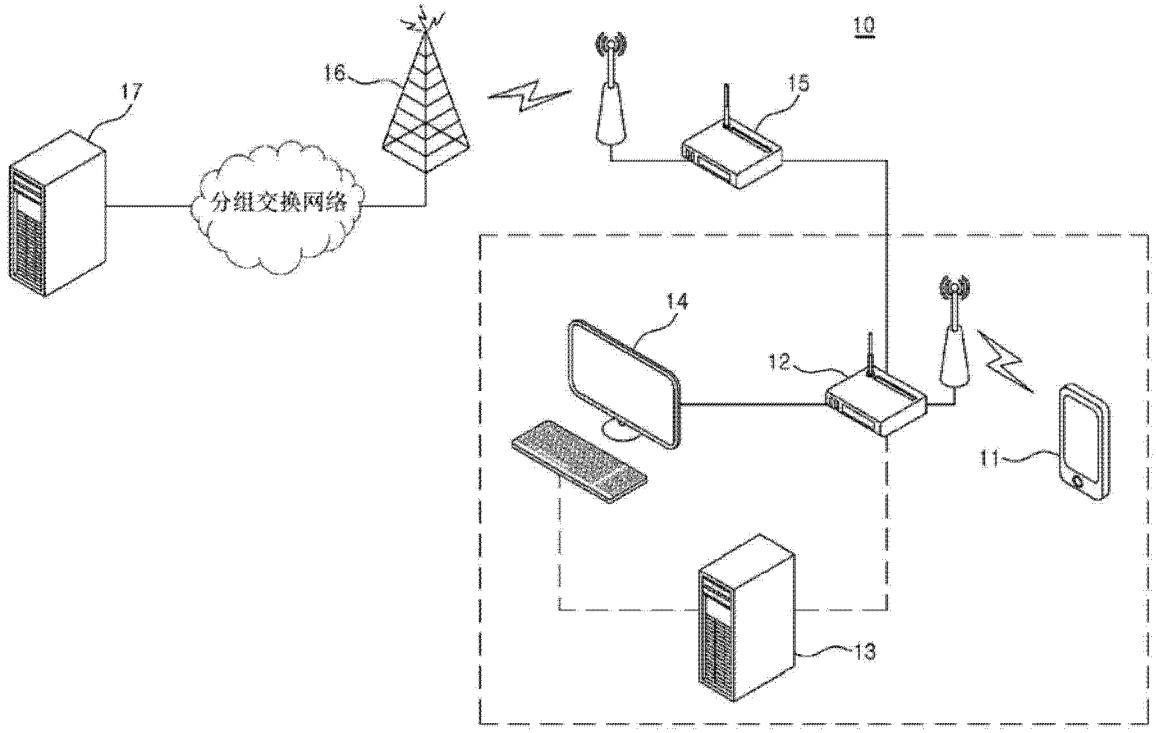

10
17
16
15
分组交换网络
14
12
11
13

图 1

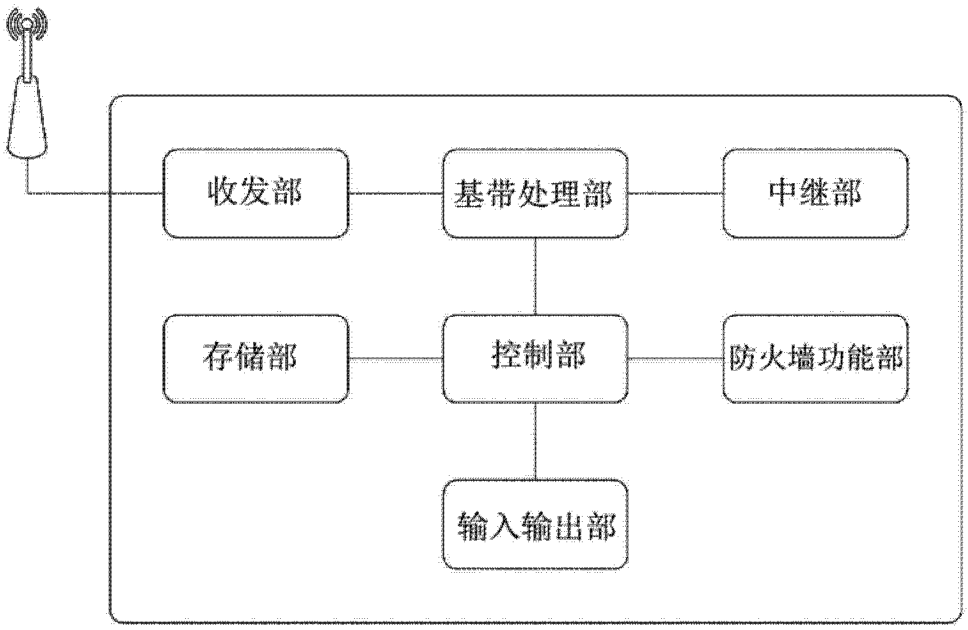

收发部
基带处理部
中继部
存储部
控制部
防火墙功能部
输入输出部

图 2

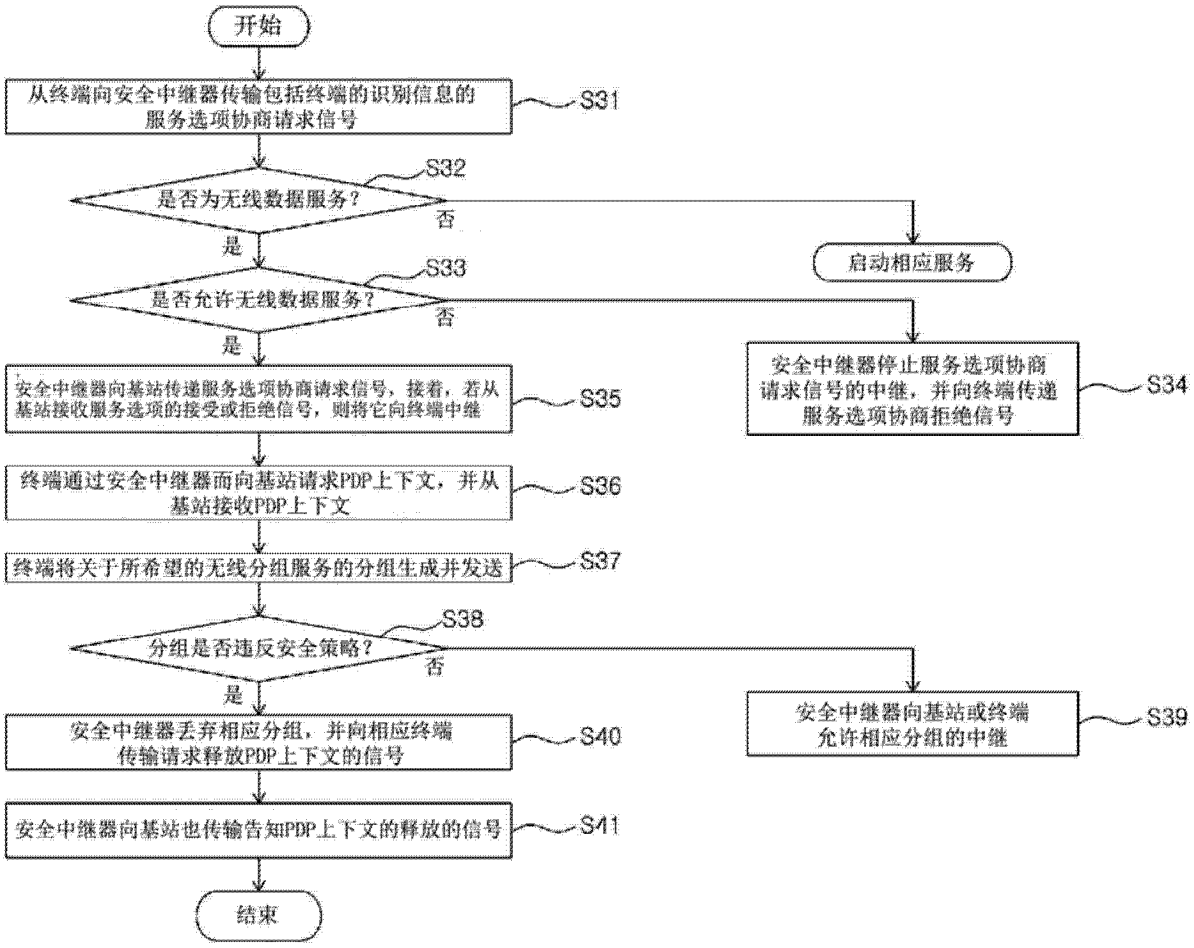

开始
从终端向安全中继器传输包括终端的识别信息的服务选项协商请求信号
S31
是否为无线数据服务？
S32
否
是
启动相应服务
是否允许无线数据服务？
S33
否
是
安全中继器停止服务选项协商请求信号的中继，并向终端传递服务选项协商拒绝信号
S34
安全中继器向基站传递服务选项协商请求信号，接着，若从基站接收服务选项的接受或拒绝信号，则将它向终端中继
S35
终端通过安全中继器而向基站请求PDP上下文，并从基站接收PDP上下文
S36
终端将关于所希望的无线分组服务的分组生成并发送
S37
分组是否违反安全策略？
S38
否
是
安全中继器向基站或终端允许相应分组的中继
S39
安全中继器丢弃相应分组，并向相应终端传输请求释放PDP上下文的信号
S40
安全中继器向基站也传输告知PDP上下文的释放的信号
S41
结束

图 3