[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04L 12/56 (2006.01)
H04L 29/06 (2006.01)
H04L 12/26 (2006.01)

[12] 发明专利说明书

专利号 ZL 99815603.5

[45] 授权公告日 2008 年 2 月 13 日

[11] 授权公告号 CN 100369437C

[22] 申请日 1999.1.14 [21] 申请号 99815603.5
[86] 国际申请 PCT/EP1999/000180 1999.1.14
[87] 国际公布 WO2000/042742 英 2000.7.20
[85] 进入国家阶段日期 2001.7.12
[73] 专利权人 诺基亚网络有限公司
地址 芬兰诺基亚集团
[72] 发明人 拉塞·希普莱南
[56] 参考文献
WO9621982 1996.7.18
US5428667 1995.6.27
WO9852337 1998.11.19
审查员 秦 声

[74] 专利代理机构 中国国际贸易促进委员会专利商标事务所
代理人 于 静

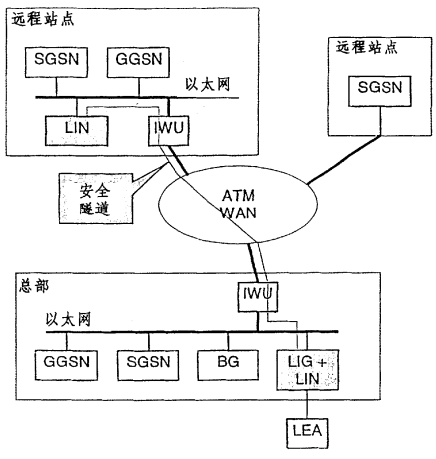
权利要求书 5 页 说明书 11 页 附图 4 页

[54] 发明名称

窃听方法和系统

[57] 摘要

描述了在诸如 GPRS 或者 UMTS 网络的分组网络中执行合法窃听的窃听方法和系统。 提供具有窃听数据分组的窃听功能的第一网络单元，所述窃听功能由在第二网络单元实现的窃听控制装置控制，其中从第一个网络单元通过分组网络将窃听的数据分组发送给窃听网关单元，该窃听网关单元为窃听管理机构提供一个接口。 窃听数据分组通过由加密处理提供的安全的隧道发送。 窃听控制装置和窃听网关单元二者可以集成在第二网络单元中。 窃听系统具有可伸缩性的明显优点，没有单个故障点，对不同的管理机构接口的适应仅仅可以在窃听网关中实现。 对于所有的不同的管理机构要求，网络单元可以高度类似。



1. 在分组网络中用于执行合法窃听的窃听方法，包括步骤：

a)提供具有用于窃听数据分组的窃听功能的第一网络单元；

b)由在第二网络单元中实现的窃听控制装置控制所述窃听功能；其特征在于：

c)通过所述分组网络从所述第一网络单元发送窃听数据分组给一个窃听网关单元，该窃听网关单元提供到至少一个窃听管理机构的接口，其中所述第一网络单元产生要与所述窃听的数据分组一同传输的假的分组，并且所述假的分组从所述第一网络单元发送到所述窃听网关单元。

2. 根据权利要求 1 的方法，其特征在于所述窃听网关单元集成在所述第二网络单元。

3. 根据权利要求 1 或者 2 的方法，其特征在于由所述第二网络单元读取数据分组的标题，并且要被窃听的数据分组被复制。

4. 根据权利要求 1 的方法，其特征在于使用安全的隧道所述窃听数据分组被发送到所述窃听网关单元。

5. 根据权利要求 4 的方法，其特征在于所述安全的隧道通过加密处理实现。

6. 根据权利要求 1 的方法，其特征在于在所述第一网络单元和所述窃听网关单元安排在独立的网络段中时，所述窃听数据分组通过互配单元发送并在所述互配单元之间加密。

7. 根据权利要求 1 的方法，其特征在于所述第一网络单元在所述分组网络的每个网络段中提供。

8. 根据权利要求 1 的方法，其特征在于在所述窃听网关单元中收集接收的窃听数据分组并且提供给所述至少一个窃听管理机构的一个接口。

9. 根据权利要求 8 的方法，其特征在于所述接口包括用于管理任务的第一接口，用于网络信令的第二接口和用于窃听的用户数据的第三接口。

10. 根据前面的任何一个权利要求的方法，其特征在于所述窃听功能包括一个分组探测和滤波功能。

11. 根据权利要求 10 的方法，其特征在于所述窃听功能是在 Gn 接口中实现的。

12. 根据权利要求 1 的方法，其特征在于所述窃听功能包括读出数据分组，分析数据分组的标题以获知该数据分组是否应该窃听，和发送该数据分组给所述窃听网关单元，以及用于窃听和传输标准的管理功能。

13. 根据权利要求 1 的方法，其特征在于在已经检测到相应的网络单元的机壳损坏时，发送一个告警给所述窃听网关单元，并且删除相应的网络单元的所有窃听信息。

14. 根据权利要求 1 的方法，其特征在于所述假的分组随机发送或者在任何经过的分组处触发，使得窃听的总的负荷和发送给所述窃听网关单元的假的分组是恒定的。

15. 根据权利要求 1 的方法，其特征在于所述窃听数据分组被填补到最大长度。

16. 根据权利要求 1 的方法，其特征在于时间信息被加到所述窃听数据分组。

17. 在分组网络中用于执行合法窃听的窃听系统，包括:

a)第一网络单元，具有用于窃听数据分组的窃听功能并且包括用于发送窃听的数据分组到所述分组网络的一个发送装置;

b)一个窃听控制装置，在第二网络单元中实现并且控制所述窃听功能;

其特征在于:

c)一个窃听网关单元，具有用于接收所述窃听数据分组的一个接收装置和用于提供一个接口给至少一个窃听管理机构的一个接口装置;

其中所述第一网络单元还包括用于产生与所述窃听的数据分组一起发送的假分组的装置。

18. 根据权利要求 17 的系统，其特征在于所述第二网络单元对

应于所述窃听网关单元。

19. 根据权利要求 17 的系统，其特征在于所述第一网络单元还包括一个加密装置(12)，用于加密所述窃听的数据分组。

20. 根据权利要求 17 的系统，其特征在于所述第一网络单元包括用于读出接收数据分组的标题和用于复制要窃听的数据分组的一个读出装置。

21. 根据权利要求 20 的系统，其特征在于安排所述读出装置填充所述复制的数据分组至最大长度。

22. 根据权利要求 17 的系统，其特征在于所述第一网络单元是所述分组网络的一个网关单元。

23. 根据权利要求 17 的系统，其特征在于所述第一网络单元是一个 BG、一个 SGSN 或者一个 GGSN。

24. 根据权利要求 22 的系统，其特征在于定义要窃听的数据分组的窃听信息包括在提供给所述第一网络单元 且用于路由数据分组的环境信息中。

25. 根据权利要求 24 的系统，其特征在于所述窃听控制装置包括用于存储窃听表的一个存储装置，和其中安排所述窃听控制装置(26)增加所述窃听信息到提供给所述第一网络单元的所述环境信息。

26. 根据权利要求 17 的系统，其特征在于所述第一网络单元安排在所述分组网络的每个段中。

27. 根据权利要求 17 的系统，其特征在于所述第一网络单元包括一个控制装置，用于根据从所述窃听控制装置接收的窃听设置指令控制窃听和加密处理。

28. 根据权利要求 17 的系统，其特征在于所述第一网络单元包括一个检测装置，用于检测它的故障和/或者损坏，和传信装置，用于响应所述检测装置的输出，而发出告警通知所述窃听网关单元。

29. 在分组网络中用于执行合法窃听的窃听系统，包括:

a)第一网络单元，具有用于窃听数据分组的窃听功能并且包括用于发送窃听的数据分组到所述分组网络的一个发送装置;

b)一个窃听控制装置，在第二网络单元中实现并且控制所述窃听

功能;

其特征在于:

c)一个窃听网关单元，具有用于接收所述窃听数据分组的一个接收装置和用于提供一个接口给至少一个窃听管理机构的一个接口装置，其中所述窃听网关单元包括一个存储器装置，用于在将接收的窃听数据分组提供给所述接口装置之前存储接收的窃听数据分组，

其中所述窃听网关单元包括一个解密装置，用于消除接收的窃听数据分组的加密，一个提取装置，用于从假的数据分组中提取窃听的数据分组，和一个装置，用于在所述存储器装置中存储所述接收的窃听数据分组之前，将时间信息添加到所述接收的窃听数据分组。

30. 分组网络的一个网络单元，包括:

a)一个窃听装置，用于窃听从所述分组网络接收的数据分组，和

b)一个发送装置，用于通过所述分组网络将所述窃听的数据分组发送给窃听网关单元，

其特征在于:

c)其中所述窃听装置由安排在另一个网络单元中的窃听控制装置控制，所述第一网络单元进一步包括用于产生要与所述窃听的数据分组一同传输的假的分组的装置，并且所述假的分组从所述第一网络单元发送到所述窃听网关单元。

31. 用于分组网络的窃听系统的一个窃听网关单元，包括:

a)一个接收装置，用于通过所述分组网络从具有窃听功能的网络单元接收窃听的数据分组;

b)一个接口装置，用于提供一个接口给窃听管理机构 ；和

其特征在于:

c)一个存储器装置，用于在将接收的窃听数据分组提供给所述接口装置之前存储接收的窃听数据分组，

其中所述窃听网关单元包括一个解密装置，用于消除接收的窃听数据分组的加密，一个提取装置，用于从假的数据分组中提取窃听的数据分组，和

一个用于在所述存储器装置中存储所述接收的窃听数据分组之

前，将时间信息添加到所述接收的窃听数据分组的装置。

32.根据权利要求 31 的窃听网关单元，还包括一个窃听控制装置，用于控制所述网络单元的所述窃听功能。

窃听方法和系统

技术领域

本发明涉及在分组网络诸如 GPRS(通用分组无线电业务)或者 UMTS(通用移动电信系统)网络中合法窃听的窃听方法和系统。

背景技术

合法的窃听的规定是国家的法律要求的，通常是强制性的。时常，根据合法的授权，要求网络运营商和/或者服务提供商使特定的窃听管理机构或者执法机关(LEA)得到有关具体身份的可用窃听结果。

存在着窃听的各个方面。各个国家的法律描述在什么条件下和具有什么限制窃听是允许的。如果 LEA 希望使用合法的窃听作为工具，它将要求检查官或者其它负责的主体合法的授权，诸如授权令（warrant）。如果授予合法的授权，LEA 将提供合法的授权给访问提供商，提供从用户的终端通过管理接口或者过程访问该网络、该网络运营商或者服务提供商的权限。在授权合法的窃听时，窃听相关信息(IRI)和相应的通信内容传送给 LEA。

具体地说，合法的授权可以描述 IRI 和允许传送用于这个 LEA 的通信内容、调查、期间和窃听主题。对于不同的 LEA 和不同的调查，可以应用不同的约束，进一步限制由法律设置的一般界限。窃听主题还可以以不同的方式在合法的授权中描述，例如用户地址，物理地址，业务等等。

这样的合法的窃听功能在新的移动数据网络（诸如 GPRS 和 UMTS）的分组交换部分中也需要。

合法的窃听是基于 EU 委员会决议，它涉及所有的电信系统，不仅仅是移动电信系统。欧洲通信标准学会(ETSI)已经定义了另外的技术要求。这些要求定义三个接口：

X1: 管理的任务(可以是以书面或者传真)

X2: 网络信令(接近实时)

X3: 窃听的用户数据 (接近实时)

接口 X1 传送窃听请求，授权文件，加密密钥等等。三个接口的准确的定义由本地的法律和管理机构负责。

迄今为止已经建议了几个方法。根据集线器方法，一个集线器加到 GPRS 干线，使得所有的会话经过该集线器。系统的益处是 SGSN(在

服务 GPRS 支持节点)和 GGSN(网关 GPRS 支持节点)不必知道有关合法的窃听功能的任何事情。集线器由伪 GGSN 接口和伪 SGSN 接口组成，它们之间安排一个合法的窃听节点(LIN)。

但是，这个方法的缺点是可伸缩性。LIN 必须能够处理干线中的所有的数据分组。而且，它构成单个故障点。如果 LIN 崩溃，整个网络将中止。因此，LIN 是非常昂贵的，可能是整个网络中最昂贵的单元。

图 1 表示另一个所谓的 SGSN/GGSN 方法的原理方框图，整个窃听功能集成到一个组合的 SGSN/GGSN 单元。每个物理 SGSN/GGSN 单元以自己的 X1 接口链接到一个管理的功能。

根据图 1，传送 GPRS 窃听消息的访问方法是基于从被窃听的用户通过 SGSN/GGSN 单元发送给另一方的分组的复制。复制的分组发送给用于将相应的 IRI 和通信内容传送给 LEA 的传送功能。

如果存在几个 SGSN/GGSN 单元，这个系统不具有单个故障点。而且，在新的合法的窃听能力可以与每个增加的新的 SGSN/GGSN 单元安装到该干线的意义上它是可伸缩的。但是，利用每个安装的新的 SGSN/GGSN 单元，要求到管理功能的新的接口并且没有对 UMTS 的自然的扩充路径。

发明内容

本发明的一个目的是提供一个灵活的和可伸缩的窃听方法和系统。

这个目的是由在分组网络中用于执行合法窃听的窃听方法实现的，包括步骤:

a)提供具有用于窃听数据分组的窃听功能的第一网络单元;

b)由在第二网络单元中实现的窃听控制装置控制所述窃听功能;和

c)通过所述分组网络从所述第一网络单元发送窃听数据分组给一个窃听网关单元，该窃听网关单元提供到至少一个窃听管理机构的接口，其中所述第一网络单元产生要与所述窃听的数据分组一同传输的假的分组，并且所述假的分组从所述第一网络单元发送到所述窃听网关单元。

另外，上面的目的由用于在分组网络中执行合法窃听的窃听系统实现了，包括:

第一网络单元，具有用于窃听数据分组的窃听功能并且包括用于发送窃听的数据分组到所述分组网络的一个发送装置;

一个窃听控制装置，在第二网络单元中实现并且控制所述窃听功能；和

一个窃听网关单元，具有用于接收所述窃听数据分组的一个接收装置和用于提供一个接口给至少一个窃听管理机构的一个接口装置；

其中所述第一网络单元还包括用于产生与所述窃听的数据分组一起发送的假分组的装置。

根据本发明另一个方面的在分组网络中执行合法窃听的窃听系统包括：在分组网络中用于执行合法窃听的窃听系统，包括：

第一网络单元，具有用于窃听数据分组的窃听功能并且包括用于发送窃听的数据分组到所述分组网络的一个发送装置；

一个窃听控制装置，在第二网络单元中实现并且控制所述窃听功能；和

一个窃听网关单元，具有用于接收所述窃听数据分组的一个接收装置和用于提供一个接口给至少一个窃听管理机构的一个接口装置，其中所述窃听网关单元包括一个存储器装置，用于在将接收的窃听数据分组提供给所述接口装置之前存储接收的窃听数据分组，

其中所述窃听网关单元包括一个解密装置，用于消除接收的窃听数据分组的加密，一个提取装置，用于从假的数据分组中提取窃听的数据分组，和一个装置，用于在所述存储器装置中存储所述接收的窃听数据分组之前，将时间信息添加到所述接收的窃听数据分组。

因此，窃听控制和网关功能可以从处理用户数据的网络单元中去除。因此，可以获得下面的优点。

该系统是容易地可伸缩的，因为新的 LIN 能力可以随着负荷增加而增加。因此，LIN 自己是可与个人计算机相比的。而且，窃听网关功能可以分布在几个单元，其中可以从一个 LIN 建立几个隧道而不给它增加硬件。以相同的方式，由在第二网络单元实现的窃听控制装置控制的窃听功能可以发送窃听的数据分组给另一个网络单元或者多个其它网络单元。

如果 LIN 失效，一些窃听功能可能不可得到，但是该网络仍然能够工作。即使 LIG 的故障不保持该网络。LIN 和 LIG 实际上是可热交换的（hot swappable），即它们可以被代替而不中断该网络的运行。

此外，诸如点对多点服务中心或者多媒体消息服务中心的新的网络单元可以加到该网络。但是，这不要求新的合法的窃听功能集成在里面。对于 UMTS 节点也是这样，即使由于更高的带宽它们要求更强大的处理器也不例外。因此，相同的干线同时地支持 GPRS 和 UMTS

二者，使得对第三代系统的扩充简单化了。

由于仅仅 LIG 包括到 LEA 的 Xn 接口，它可以充当对不同的 LEA 要求的一个中间设备。在要求变化时，仅仅 LIG 需要重新编程。LIG 和/或者 LIN 甚至可以作为独立的可定做的产品销售给其它(非移动的)IP 网络。

窃听网关单元也可以集成在第二网络单元中。

最好由第一网络单元读出数据分组的标题并且复制被窃听的数据分组。窃听的数据分组可以使用安全的隧道发送给窃听网关单元，安全的隧道可以通过加密处理实现。因此，不要求独立的传输线路，而独立的传输线路正是易受到运营商人员的物理攻击。

在独立的网络段中安排第一网络单元和窃听网关单元的情况下，窃听的数据分组可以通过互配单元发送和在互配单元之间加密。

最好，在移动分组网络的每个网络段中提供具有窃听功能的一个第一网络单元。

此外，在窃听网关单元中收集接收的窃听的数据分组并且提供给至少一个窃听管理机构的一个接口。该接口可以包括用于管理任务的第一接口，用于网络信令的第二接口和用于窃听的用户数据的第三接口。

第一网络单元的窃听功能可以包括分组探测和滤波功能。特别地，窃听功能可以在 Gn 接口（除去任何传输）中实现。详细地说，窃听功能可以包括读出数据分组，分析数据分组的标题以获知是否应该窃听该数据分组，和发送该数据分组给窃听网关单元，以及用于窃听和传输标准的一个管理功能。

最好在已经检测到第一网络单元的机壳损坏或者另一个事故时，可以给窃听网关单元发送一个告警并且可以删除相应的第一网络单元的所有的窃听信息。因此，可以防止对窃听数据的不需要的访问。

而且，假的分组可以从第一个网络单元发送给窃听网关单元。假的分组可以随机发送或者在任何经过的分组处触发。这可用这样的方式进行：总的窃听的负荷和发送给窃听网关单元的假的分组是恒定的。因此，操作人员不能使用定时分析检测谁的分组正被窃听。另外，如果窃听的数据分组的负荷是恒定的，就不能确定真正的窃听活动。

另外，窃听的数据分组可以总是填补到最大长度，这进一步妨碍窃听活动。

最好一个时间标记可以加到该窃听的数据分组。因此，在传送到窃听管理机构之前窃听信息可以存储在慢的或者脱机的存储器中，使得第一网络单元、窃听控制装置和窃听网关单元的实时要求以及窃听

管理机构可以脱开。

第一网络单元可以包括一个读出装置，用于读出接收数据分组的标题和用于复制被窃听的数据分组。可以安排这个读出装置填充该复制的数据分组到最大长度。

而且，第一网络单元可以是诸如BG(边界网关)、GGSN(网关GPRS支持节点)的网关单元和诸如SGSN（在服务GPRS支持节点）的服务节点。在这种情况下，在窃听的连接上的信息最好可以存储在相应的连接的PDP环境信息中，它是用于以正确的方式路由连接的数据分组的记录。因此，每次路由分组时，关于数据分组是否需要窃听的信息随时可得到。因此，用于窃听功能要求的资源可以最小化。

第一网络单元可以包括一个控制装置，根据从窃听网关单元接收的窃听设置指令控制窃听和加密处理。

此外，窃听网关单元可以包括一个存储器装置，在接收的窃听数据分组提供给接口装置之前存储该接收的窃听数据分组。而且，窃听网关单元可以包括一个解密装置，用于解密接收的窃听数据分组，一个提取装置，用于从假的数据分组中提取窃听的数据分组，和在将接收的窃听数据分组存储在存储器装置之前用于增加时间信息到接收的窃听数据分组的一个装置。

第一网络单元可以包括一个检测装置，用于检测第一网络单元机壳的损坏，和一个传信装置，为响应该检测装置的输出而发告警信号通知窃听网关单元。

根据本发明的分组网络的一个网络单元，包括:

一个窃听装置，用于窃听从所述分组网络接收的数据分组，和

一个发送装置，用于通过所述分组网络将所述窃听的数据分组发送给窃听网关单元，

其中所述窃听装置由安排在另一个网络单元中的窃听控制装置控制，所述第一网络单元进一步包括用于产生要与所述窃听的数据分组一同传输的假的分组的装置，并且所述假的分组从所述第一网络单元发送到所述窃听网关单元。

根据本发明的用于分组网络的窃听系统的一个窃听网关，包括:

一个接收装置，用于通过所述分组网络从具有窃听功能的网络单元接收窃听的数据分组;

一个接口装置，用于提供一个接口给窃听管理机构；和

一个存储器装置，用于在将接收的窃听数据分组提供给所述接口装置之前存储接收的窃听数据分组，其中所述窃听网关单元包括一个解密装置，用于消除接收的窃听数据分组的加密，和一个用于在所述

存储器装置中存储所述接收的窃听数据分组之前，将时间信息添加到所述接收的窃听数据分组的装置。

附图说明

在下面，根据优选实施例参考附图更详细地描述本发明，其中：

图 1 表示执行合法的窃听的已知系统的原理方框图，

图 2 表示根据本发明的优选实施例执行合法的窃听的一个系统的原理方框图，

图 3 表示根据本发明的优选实施例执行合法的窃听的一个方法的流程和信息传递图，

图 4 表示根据本发明的优选实施例通过分组网络连接到窃听网关的一个窃听节点的原理方框图。

具体实施方式

在下面，根据诸如 GPRS 或者 UMTS 网络的移动分组网络描述根据本发明的方法和系统的优选实施例，如图 2 中所示的。

根据图 2，可能包括一个以太网段或者仅仅一个 SGSN 的远程站点和总部以太网段连接到 ATM WAN(异步传输模式广域网)。具有 GGSN 或者 BG 的每个段具有合法的窃听节点(LIN)或者分组探测器。远程独立的 SGSN 不必具有 LIN。LIN 没有必要是一个独立的网络单元，但是可以集成到与 GGSN 或者 BG 相同的物理单元。

安排 LIN 作为无源的分组探测器，用于读出和复制窃听的数据分组。每个以太网段必须具有一个 LIN，以使通过干线发送的所有的数据分组可以被窃听。应当注意，独立的 LIN 要求一个广播干线，诸如以太网，而由 GPRS 支持节点(GSN)实现的 LIN 能够共享相同的接口和窃听所有的数据分组。LIN 可以在任何 GSN（包括 SGSN）中实现。

安排每个 LIN 作为一个分组探测器和滤波器，实质上是具有以太网接口和 GTP 协议组的个人计算机。在实施中，每个 LIN 可能实现正如在 GSM 技术规范 09.60 中定义的一个 Gn 接口。在这种情况下，安排 LIN 作为一个无源的侦听节点，它能够读出 GPRS 隧道协议(GTP)。然而，尽管有无源的侦听功能，仍安排 LIN 通过相同的物理接口发送给 LIG，该接口还运行 Gn 接口，但是在不同的 TCP(传输控制协议)或者 UDP(用户数据报协议)端口。

由 LIN 窃听的数据分组是由合法的窃听网关(LIG)收集，再提供给至少一个窃听管理机构(LEA)的 X1，X2 和 X3 接口。在几个 LEA

连接到一个 LIG 的情况下，LEA 甚至可以访问具有不同的授权的相同的目标连接，即，一个 LEA 仅通过 X2 接口监视该目标连接，而同时另一个 LEA 也使用 X3 接口执行窃听。

配置 LIN 在最高电平窃听。因此 LIG 的任务是仅仅传送窃听消息中授权相应的 LEA 接收的那部分。用这种方式，关于传送的信息的种类和目的地的判定集中在 LIG，使得 LIN 的结构可以保持简单。

在总部以太网，相应的 LIN 和 LIG 可以集成在单个网络单元中，如图 3 中所示的。作为选择，独立的 LIN 和 LIG 可以在以太网段中提供。

通过该网络发送的呼叫通过三个功能，即 BG，GGSN 或者 SGSN 中的两个功能。为了经济的原因，为每个具有一个 GGSN 或者 BG 的端装备一个 LIN 是足够的。因此，任何呼叫可以被窃听。

在下面参照图 3 描述根据优选实施例执行合法的窃听的方法。图 3 表示一个流程和信息传递图，它是从顶部到底部读出的。

根据图 3，从 LEA 向 LIG 发出初始的窃听请求。实际上，LEA 传送合法的授权给网络运营商、访问提供者或者服务提供商。网络运营商、访问提供者或者服务提供商从合法的授权中给出的信息中确定有关的目标身份。然后，网络运营商、访问提供者或者服务提供商命令用于控制 LIN 的窃听功能的窃听控制单元，以提供相应的窃听信息给有关的目标身份的 LIN。窃听控制单元可以安排在 LEA(正如在图 3 的情况下)中或者在独立的网络单元中。

随后，窃听控制单元通过分组网络发送要求的 LIN 设定给相应的 LIN。响应 LIN 设定的接收，LIN 执行分组窃听和根据它们的标题信息复制被窃听的那些分组。然后，加密窃听的分组和产生假的分组并且加到该窃听分组。这些加密的和模糊的数据分组通过相应的互配单元(IWU)通过 ATM WAN 发送给该 LIG。由于加密处理，建立了安全的隧道，虽然窃听的数据分组通过分组网络的常规信道发送。

但是，应注意，只要可以建立要求的安全性，任何其它种类的传输和/或者传输信道都可以实现在优选实施例中发送窃听数据分组。

在 LIG，收集和评估接收数据分组，以便产生窃听相关的数据(IRI)和窃听通信的内容，最后通过 X3 接口发送给 LEA。

在下面参照图 4 更详细地描述 LIN 和 LIG。应当注意，根据图 2 的互配单元 IWU 在图 4 中没有表示。

根据图 4，安排 LIN 执行下面的功能，这也可以作为软件单元或者作为离散的硬件单元建立。

LIN 包括一个交换装置 14，用于从该网络接收和向该网络发送数据分组，并将其提供给分组读出装置 11，在这里读出提取的数据分组的标题和分析该数据分组是否应该窃听。窃听的数据分组提供给安排用于加密数据分组从而实现安全的隧道的一种加密装置 12。另外，加密的数据分组可以提供给用于增加假的分组从而搞混窃听活动的一个装置 13。加密的和假的数据分组提供给交换装置 14，以便通过 ATM WAN 发送到 LIG。假的分组可以在任何时间发送或者由任何经过的分组处触发。而且，可以安排分组读出装置 11 或者加密装置 12 以便填充窃听的分组到最大长度。

此外，控制装置 15 可以执行控制，以便将该窃听的数据分组延迟一个随机的期间，从而使得它难于确定谁在窃听。但是，在这种情况下，定义实际的窃听瞬时或者该延迟的附加信息应该加到发送给 LIG 的数据分组。

通常，应该提供合法的窃听分组的恒定负荷，而与真正的窃听活动无关。提供恒定的窃听负荷有助于计费，排除监视窃听业务，和模糊真正的截听活动。

此外，LIN 包括一个控制装置 15，用于根据关于窃听标准和安全的隧道的窃听控制信息控制 LIN 的其它装置，它是从在 LIG 或者独立的网络单元中提供的窃听控制单元通过交换装置 14 接收的。

另外，可以提供检测装置(未示出)用于检测 LIN 机壳的损坏。在这种情况下，还可以提供传信装置(未示出)用于发送告警给 LIG 和命令控制装置 15，以便从 LIN 存储器(未示出)中擦除所有的窃听信息，诸如滤波器设定等等。而且，可以安排检测装置也检测 LIN 的其它故

障，诸如电源故障或者其他的故障，其中安排传信装置发出相应的告警给 LIG。

安排 LIG 作为 LIN 的主装置和向至少一个 LEA 提供用户接口 27。LIG 可以是个人计算机，微计算机或者大型机。特别地，可以安排 LIG 执行下面功能，这也可以作为软件或者硬件单元实现。

安排接口 27 提供 Xn 接口给至少一个 LEA，其中在提供几个 LEA 的情况下，接口模块可以提供用于每个 LEA。此外，提供交换装置 21 用于从 ATM WAN 通过安全的隧道接收窃听的数据分组和通过交换装置 14 发送 LIN 设定以及其它控制信息到 LIN 的控制装置 15。

通过安全的隧道接收的窃听的数据分组和假的分组从交换装置 14 提供给解密装置 22，安排解密装置 22 去掉窃听分组的 LIN 加密。此外，可以提供提取装置 23 用于去掉复制和可能的假分组或者填充信息。LIN 加密和复制或者假的分组已经去除的窃听的数据分组提供给时间标记产生装置 24，时间标记加到窃听的数据分组，以便在存储器 25 中存储窃听的数据分组之前提供一个时间基准，存储器 25 构成用于窃听信息的大容量存储器。

时间标记应该尽可能快地添加，或者它甚至可能已经加到相应的 LIN，使得可以无需时间标记产生装置 24。由于该时间标记，在传送给 LEA 之前，窃听信息可以存储在存储器 25 中。因此，不要求实时处理。

此外，在 LIG 中提供控制装置 26 并且安排控制 LIG 的每个单元。控制装置 26 可以包括几个控制单元，用于接口 27 的每个 LEA 接口模块。而且，控制装置 26 可以包括窃听控制单元，通过交换装置 21 和 14 发送一个相应的控制信息给 LIN 的控制装置 15，用于管理 LIN 设定作为主功能。

应注意，LIN 的位置不局限于 LAN 段，但是 LIN 可能作为 GPRS 单元的一部分实现，例如 GGSN 或者 BG 本身。

一般地，有两个方式配置用于窃听的 LIN。一种方式是传送每个窃听授权给每个 LIN。这意味着将定义用于窃听的目标连接的完整目

标登记传送给每个 LIN。如果有许多目标连接，LIN 必须相对所有的目标连接检验每个数据分组，这是耗时的任务。

配置 LIN 的更有效方式是仅仅在窃听控制单元存储整个目标登记，正如已经提到的，窃听控制单元可能在 LIG 或者另一个网络单元中提供。在每个 PDP 环境激活中，相应的 LIN 发送激活请求的拷贝给窃听控制单元，窃听控制单元检验它的目标登记，以获知是否涉及目标连接。如果如此，配置 LIN 用于窃听。

在环境禁用或者在窃听请求期满时，目标从在 LIN 中提供的实际的窃听表中去除。

因此，控制 LIN 的窃听信息是 GPRS 网络单元保持的 PDP(分组数据协议)环境的一部分并且用于以正确的方式路由连接的分组。关于被窃听的目标连接的信息存储在相应连接的 PDP 环境信息中。因此每次路由分组时，在 PDP 环境中存储的窃听信息可随时得到。因此，LIN 窃听表可以保持得非常短，导致 LIN 的处理速度增加。但是，因为该环境具有长寿命，窃听控制单元必须存储所有的有效环境的登记，以使当从 LEA 接收窃听请求时，它能够检查目标连接是否具有进行的任何打开会话。如果如此，相应地配置有关的 LIN 窃听表。

而且，本发明不局限于描述的 GPRS 或者 UMTS 网络并且可用于各种分组网络，诸如 IP 网络。因此，上面描述的优选的实施例和附图仅仅是要说明本发明。本发明的优选的实施例可以在所附的权利要求书的范围内变化。

总之，描述了在诸如 GPRS 或者 UMTS 网络的分组网络中执行合法窃听的窃听方法和系统。提供具有用于窃听数据分组的窃听功能的第一网络单元，所述窃听功能由在第二网络单元实现的窃听控制装置控制，其中从第一个网络单元通过分组网络将窃听的数据分组发送给窃听网关单元，窃听网关单元向窃听管理机构提供一个接口。窃听数据分组通过由加密处理提供的安全的隧道发送。窃听控制装置和窃听网关单元二者可以集成在第二网络单元中。窃听系统具有可伸缩性的明显优点，没有单个故障点，对不同的管理机构接口的适应仅仅可以

在窃听网关中实现。对于所有的不同的管理机构要求，网络单元可以高度类似。

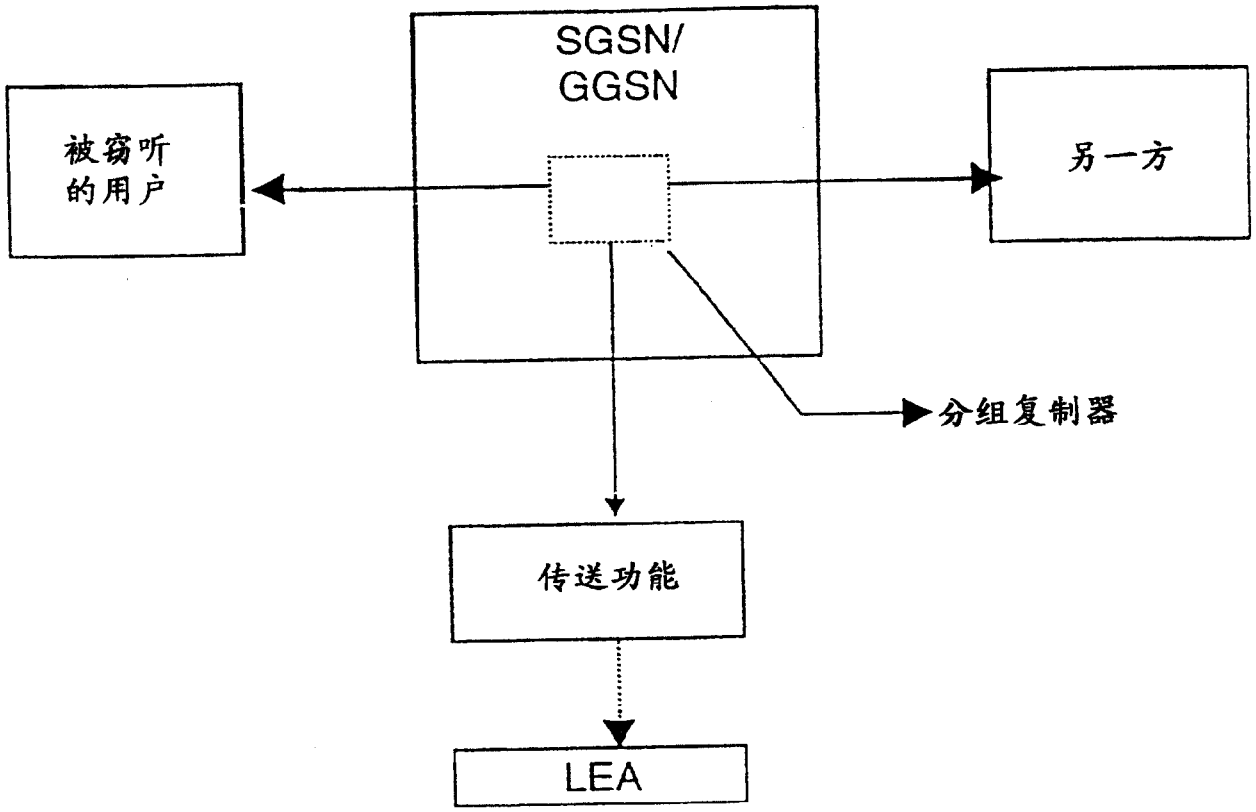


图1

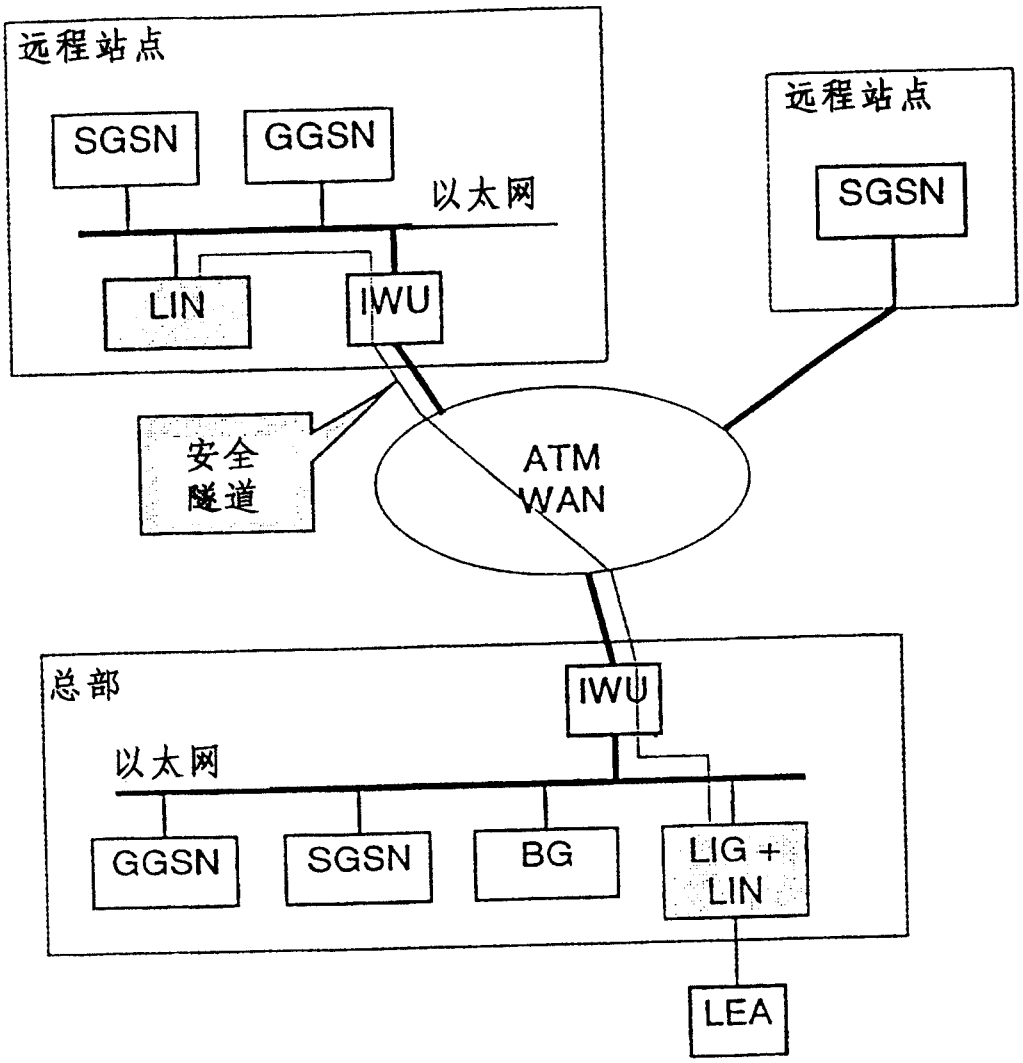

远程站点
SGSN
GGSN
以太网
LIN
IWU
远程站点
SGSN
安全
隧道
ATM
WAN
总部
IWU
以太网
GGSN
SGSN
BG
LIG +
LIN
LEA

图2

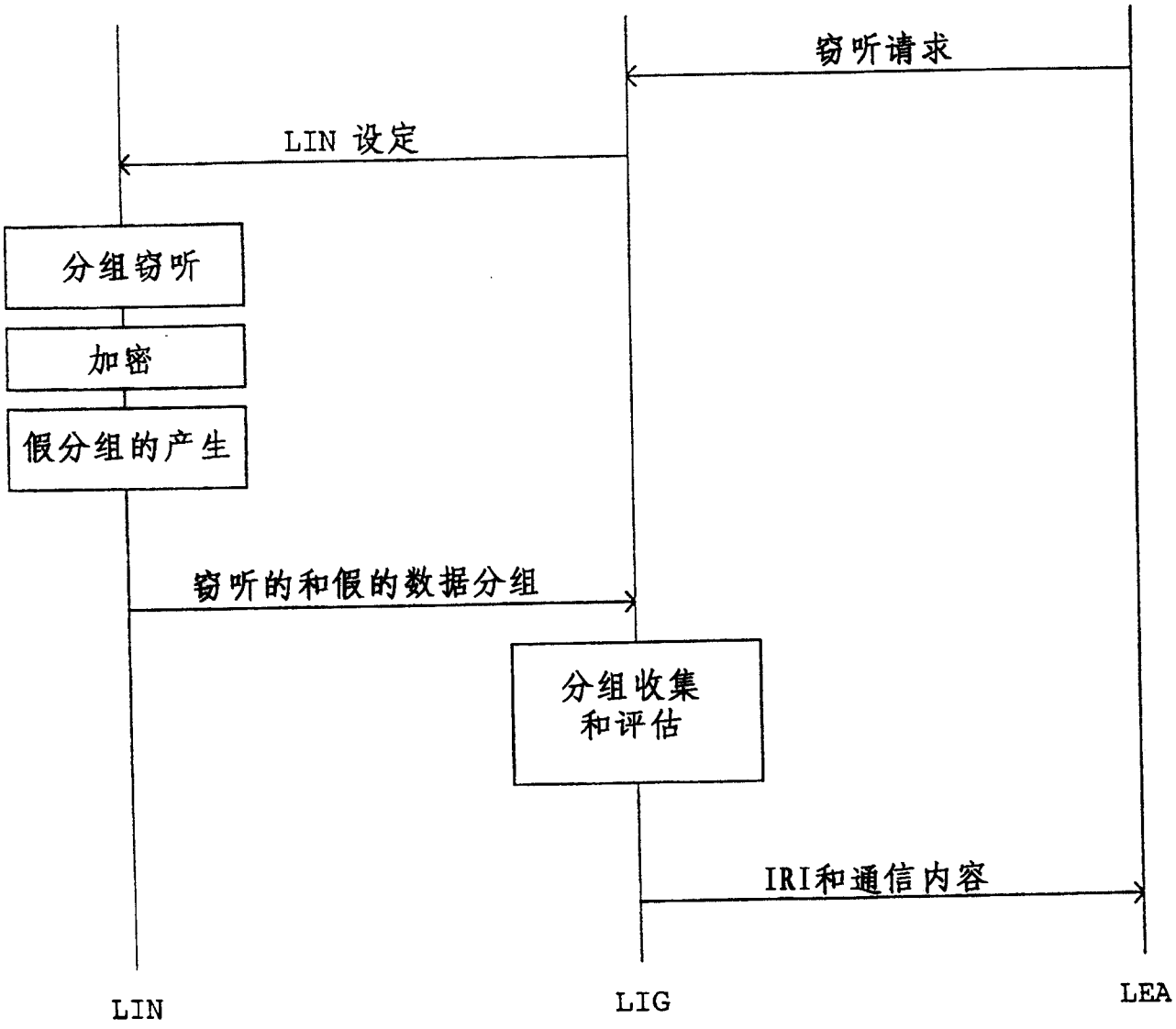

窃听请求
LIN 设定
分组窃听
加密
假分组的产生
窃听的和假的数据分组
分组收集
和评估
IRI和通信内容
LIN
LIG
LEA

图3

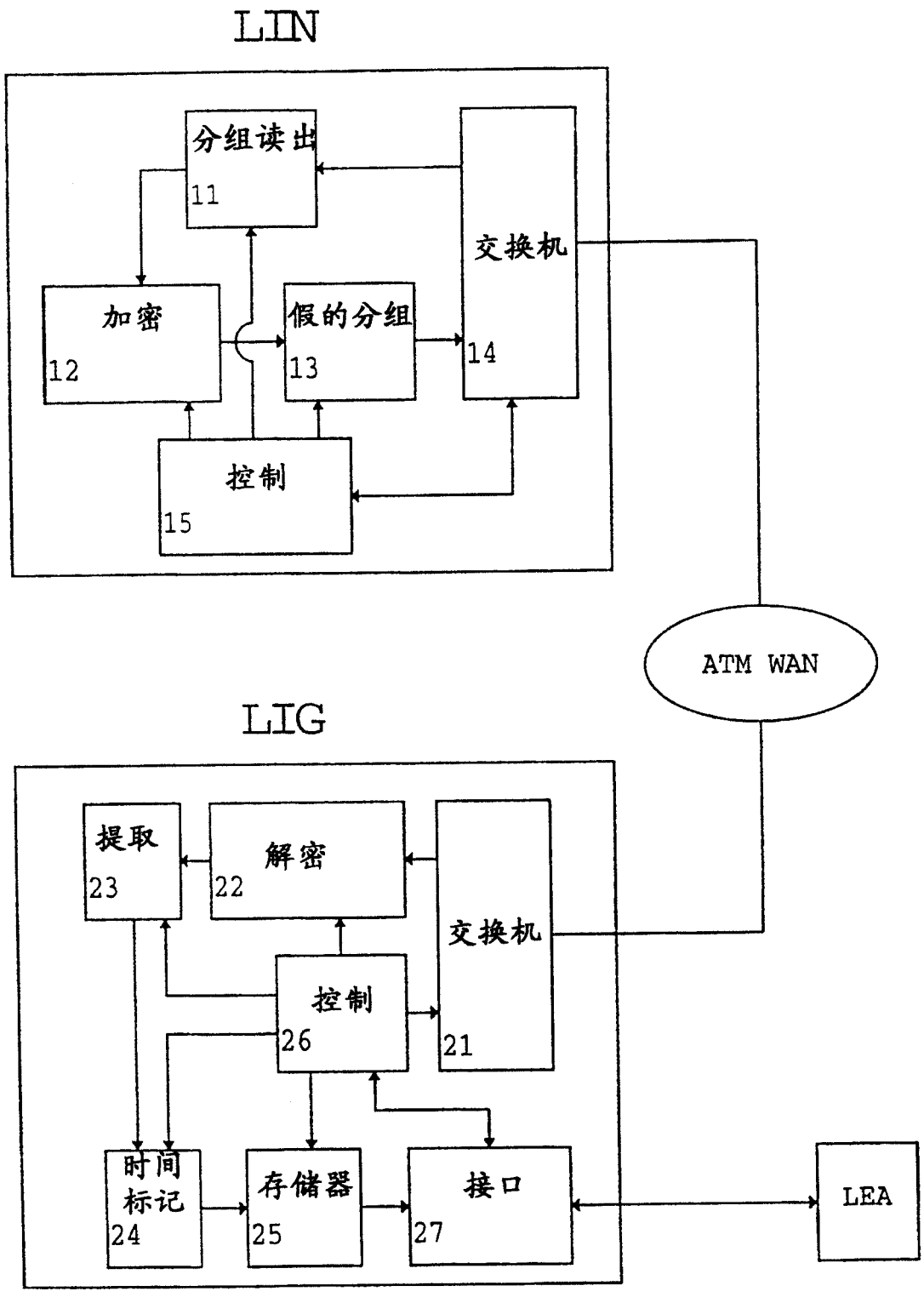

LIN
分组读出
11
交换机
加密
12
假的分组
13
14
控制
15
ATM WAN
LIG
提取
23
解密
22
交换机
控制
26
21
时间
标记
24
存储器
25
接口
27
LEA

图4