

[19] 中华人民共和国国家知识产权局

[51] Int. Cl.

H04B 7/26 (2006.01)

H04L 29/06 (2006.01)



# [12] 发明专利申请公开说明书

[21] 申请号 200510099179.1

[43] 公开日 2006 年 5 月 3 日

[11] 公开号 CN 1767414A

[22] 申请日 2005.9.9

[21] 申请号 200510099179.1

[30] 优先权

[32] 2004.9.9 [33] US [31] 60/522,270

[71] 申请人 华硕电脑股份有限公司

地址 台湾台北市

[72] 发明人 江孝祥

[74] 专利代理机构 北京市柳沈律师事务所

代理人 黄小临 王志森

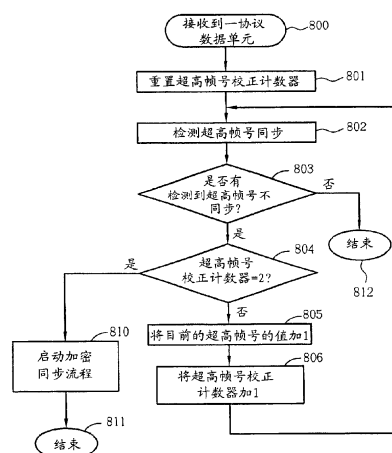
权利要求书 2 页 说明书 14 页 附图 11 页

## [54] 发明名称

在线恢复加密参数同步的方法

## [57] 摘要

根据无线通讯系统中恢复超高帧号同步的方法，接收站台可以在在线恢复超高帧号同步。于数据加密传输期间，利用超高帧号未保持同步所造成的特定结果，可以检测出无线通讯系统中的传送站台与接收站台间的超高帧号未保持同步。将该接收站台目前的超高帧号的值调整过后产生新的值，并采用新的超高帧号的值进行解密。本发明可以减少因为解密参数未保持同步而造成数据错误的机会，并且可以避免无线链接控制层重置程序等恢复加解密参数同步所需的冗长流程。



1. 一种应用于无线通讯系统的接收站台中确保超高帧号同步的方法，其包含下列步骤：
- 5        于加密期间开始时，采用起始超高帧号；  
      检测一串接收到的协议数据单元的序号是否连号；以及  
      假使接收的协议数据单元的序号与其前一协议数据单元的序号及其后一协议数据单元的序号均不连号，则删除该接收的协议数据单元。
2. 一种用于无线通讯系统的接收站台中恢复超高帧号同步的方法，其包含下列步骤：
- 10        (a) 于加密期间开始时，采用与传送站台相同的起始超高帧号；  
      (b) 于加密期间内检测到接收站台中的超高帧号未保持同步；  
      (c) 调整该接收站台中现有的超高帧号以产生调整过的超高帧号；以及  
      (d) 该接收站台采用该调整过的超高帧号进行解密。
- 15        3. 根据权利要求 2 所述的方法，其中步骤 (b) 是以检测协议数据单元中长度指针字段是否不合规定来判断超高帧号是否未保持同步。
4. 根据权利要求 2 所述的方法，其中步骤 (b) 是以在连续接收到第二预定数量的已解密的协议数据单元中检测到第一预定数量的协议数据单元的长度指针字段有不合规定的现象来判断超高帧号是否未保持同步。
- 20        5. 根据权利要求 2 所述的方法，其中步骤 (b) 是以检测协议数据单元中是否有填充字段不符合预定值来判断超高帧号是否未保持同步。
6. 根据权利要求 2 所述的方法，其中在步骤 (c) 包含将现有的超高帧号的值加 1 以产生该调整过的超高帧号。
7. 根据权利要求 2 所述的方法，其中在步骤 (c) 包含将现有的超高帧号
- 25        的值减 1 以产生该调整过的超高帧号。
8. 根据权利要求 2 所述的方法，该方法进一步包含下列的步骤：  
      (e) 在接收到协议数据单元后一段预定时间内，停止超高帧号的校正。
9. 根据权利要求 8 所述的方法，其中在步骤 (e) 中该协议数据单元包含长度指针字段，且当该协议数据单元使用现有的超高帧号进行解密时无任何的超高帧号不同步现象被检测到。
- 30        10. 根据权利要求 8 所述的方法，其中在步骤 (e) 中该段预定时间不短于

传输序号空间数量的协议数据单元所需的时间。

11. 根据权利要求 2 所述的方法, 该方法进一步包含下列的步骤:

(f) 重复步骤 (b) 以确认超高帧号同步是否因为步骤 (c) 的关系而已经恢复; 以及

5 (g) 假使超高帧号同步在按照步骤 (f) 执行后仍未恢复, 重复步骤 (c) 跟步骤 (d)。

12. 根据权利要求 11 所述的方法, 其中步骤 (f) 进一步包含假使在已经重复步骤 (b)、步骤 (c) 及步骤 (d) 预定次数后, 停止进一步的超高帧号校正, 并且回存超高帧号修正前的值。

10 13. 根据权利要求 12 所述的方法, 其中该预定次数为 2。

14. 根据权利要求 12 所述的方法, 进一步包含删除现有的协议数据单元并根据该回存的超高帧号修正前的值对下一个协议数据单元进行解密。

15 15. 根据权利要求 12 所述的方法, 其中假使在目前的协议数据单元的序号与接下来一个协议数据单元的序号间发生序号返转归零时, 将该修正前的超高帧号的值加 1。

16. 根据权利要求 11 所述的方法, 进一步包含假使在步骤 (b)、(c)、(d)、(f) 跟 (g) 已重复执行预定次数后, 停止校正超高帧号程序, 并启动加密同步程序。

17. 根据权利要求 16 所述的方法, 其中该预定次数为 2。

## 在线恢复加密参数同步的方法

## 5 技术领域

本发明是相关于无线通讯的领域，特别是相关于在加密的无线通讯系统中恢复参数同步以避免数据传递产生重大的毁损。

## 背景技术

10 随着信息时代的来临，各种移动通讯的需求日益增加，迫使企业发展出愈来愈精密复杂的通讯标准。第三代移动通讯联盟(3GPP)即为一应运而生的通讯协议标准制定组织。该组织制定的一个标准，编号为：3GPP TS 33.102 V6.1.0 (2004-06)，题目为：「通讯安全架构规范」，提供全球移动通信系统(UMTS)中与通讯安全相关的技术性说明书，为本发明的参考文献之一。此外，  
15 请参考文献 3GPP TS 25.322 V6.1.0(2004-06)，题目为：「无线链接控制协议规范」，该文件详述在全球移动通信系统中无线链接控制的功能。

这些标准规范利用三层子层方式来达成通讯。请参考第1图。第1图为在该通讯协议中的三层子层的方块图。在典型的无线环境中，有第一站台 10 以及一个或是多个第二站台 20 构成无线通联。于第一站台 10 中有应用程序(application)13，其包含消息(message)11 并经由第三层接口 12 将消息 11 传递至第二站台 20。第三层接口 12 可产生一些第三层信令消息(signaling message)14 用来控制第三层的运作。第三层接口 12 通过第二层伺服数据单元(Layer 2 SDU)15 将消息 11 或者第三层信令消息 14 传递至第二层接口 16。第二层伺服数据单元 15 可为任何长度。第二层接口 16 将第二层伺服数据单元 15 转换成一个或多个第二层协议数据单元(Layer 2 PDU)17。每一第二层协议数据单元 17 为固定长度，且被传递到第一层接口 18。该协议数据单元(PDU)的特定长度是由网络所指定的。第一层接口 18 为物理层，将数据传递至第二站台 20。被传送的数据通过第二站台 20 中的第一层接口 28 接收，并重组成一个或者多个协议数据单元 27 而后上传至第二层接口 26。第二层接口 26 接收协议数据单元 27 并产生出一个或者多个第二层伺服数据单元 25。  
25 第二层伺服数据单元 25 被上传至第三层接口(Layer 3)22。第三层接口 22 依

序将第二层伺服数据单元 25 转换回消息 21 或者第三层信令消息 24, 并交由第三层接口 22 处理。其中, 消息 21 应与第一站台 10 中由应用程序 13 所产生的原始消息 11 完全相同, 且第三层信令消息 24 应与由第三层接口 12 所产生的原始信令消息 14 完全相同。将已接收的消息 21 上传至应用程序 5 (application) 23。(特别注意到本发明所用的专业术语, 协议通讯单元 PDU 是指传送给较低子层或是由较低子层传送上来的数据单元, 而伺服数据单元 SDU 是指传送给较高子层或是由较高子层传送上来的数据单元。)

请参考第 2 图。第 2 图为现有的第二子层传送/接收流程的简易示意图。在第一站台 40 中, 第二层接口 42 收到从第三层接口 43 送出的一串伺服数据单元 44。伺服数据单元组 44 被依序排列成 SDU1 - SDU5, 且长度不同。第二层接口 42 将第二层伺服数据单元组 44 转换成第二层协议数据单元组 45。协议数据单元组 45 被依序排列成 PDU1 - PDU4, 且长度相同。第二层协议数据单元组 45 中的每一个协议数据单元连结一个标头(header), 包含序号(SN)可以正确标明此协议数据单元并指出其个别的位置。这样可以帮助第二站台 15 50 正确判断所接收到的协议数据单元组 58 的顺序, 且将伺服数据单元组 54 重建成与原本的伺服数据单元组 44 完全一致。此种包括标头的传送模式有确认模式(AM)传输与非确认模式(UM)传输两种。两种模式皆需要在每一个协议数据单元中增加一标头以包含序号。(本发明只与包括标头的传送模式有关, 其它的传送模式忽略不提。)序号的位大小(bit size)会随着所使用的传送方式而改变。举例而言, 在非确认模式传输中, 每一协议数据单元标头中的序号为 7 位, 而在确认模式传输中, 每一协议数据单元标头中的序号为 12 位。20

第 2 图中, 第二层协议数据单元组 45 中的每一个协议数据单元 PDU1 - PDU4 有其相对应的序号, 编号为 400 - 403。该等序号为 n 位的数字, 由第二层接口 42 分派给协议数据单元组 45 中的各个协议数据单元。该协议数据单元 PDU1 所对应的序号 400 可以为任何 n 位的数字, 不一定要是 0, 后续的协议数据单元的序号 401 - 403 是依据序号 400 的数值而增加。举例而言, 假设该第一协议数据单元 410 的序号 400 的值为 192, 则该第二协议数据单元 411 的序号 401 的值为 193, 依此类推。值得注意的是当序号超出其最大表示值而返转归零(SN rollover)时, 会造成后面的协议数据单元的序号值反而会小于前面的协议数据单元的序号。假设系统的序号长度为八位, 第一个起始值为 0 且每次增加 1, 每当增加到 256 时该序号会被归零。也就是说, 序号有 25 30

周期性的特质。每经过  $2^n$  个的协议数据单元, 序号会重复, 因此协议数据单元组 45 并非拥有独一无二的序号, 虽然其在每一序号周期(SN cycle)中是唯一的。假使序号是唯一的鉴别号码, 这可能会造成传递于该第一站台与该第二站台中的信令消息顺序上的混淆。因此, 除了序号之外, 超高帧号(HFN)的存在是必要的。于下文中会详述这些特征。

第 2 图的例子中还提及该第二层协议数据单元组 45 经过加密模块(encryption engine)46 进行加密。该协议数据单元的加密包含很多变量, 特别是加密模块 45 利用到各个协议数据单元(PDU1 - PDU4)的序号(400 - 403)以及加密金钥(ciphering key)47。加密金钥(ciphering key)47 是由第三层接口 43 直接下指令所提供的。所产生出的加密的协议数据单元组(ePDU)48, 经由第一层接口 41 传送出去。第二站台 50 包含相反的流程。第二站台中接收到的协议数据单元组 58 中的每一数据协议单元 ePDU1 - ePDU4 有其相对应的序号, 编号为 500 - 503。在确认模式与非确认模式传输中, 该相对应的连结是明确的, 当将每一接收到的协议数据单元的序号从标头提取出来, 序号 400 - 403 应与序号 500 - 503 完全相同。解密模块(decryption engine)56 利用序号 500 - 503 以及加密金钥(ciphering key)57 将加密的协议数据单元组(ePDU)58 解密成协议数据单元组 55。解密的协议数据单元组 55 被转换成第二层伺服数据单元组 54, 且上传至第三层接口 53。

至于将加密的协议数据单元组(ePDU)58 解密成协议数据单元组(PDU)55, 解密模块 56 必须使用与加密金钥 47 完全相同的加密金钥 57。第三子层信令消息(所谓的加密重组指令)是用来使加密金钥 47、57 同步。第一站台 40 偶尔会因为安全的目的更改加密金钥 47。第三层接口 43 会因此发出第三子层加密重组指令(ciphering reconfiguration activation command)要求更改加密金钥 47 且设定该更改金钥的启用的时间。考虑简单的原则, 该加密重组指令表示启用时间(activation time)而非实际的时间。该启用时间为第二子层协议数据单元的序号的值。因此, 又可称其为启用序号。在该启用序号之前, 协议数据单元用旧的加密金钥来进行加密。在该启用序号上或之后, 协议数据单元用新的加密金钥来进行加密。将该加密金钥以及该启用时间包含于该加密重组指令中, 可以确保第一站台 40 于加密过程中与第二站台 50 同步。在接收到该加密重组指令后, 于该启用时间之前, 第二站台 50 会用旧的加密金钥来对加密的协议数据单元(ePDU)进行解密。于该启用时间

(启用序号)上或之后,第二站台 50 会用新的加密金钥来对加密的协议数据单元 (ePDU) 进行解密。由上面所描述的,于全球移动通讯系统的加密机制中,于该传送站台与该接收站台的所有参数必须匹配,必须保持同步。

请参考第 3 图,第 3 图为先前技术中第二层接口 60 的详细方块图。第二层接口 60 最上面包含无线链接控制子层 (RLC layer) 62,与媒体存取控制子层 (MAC layer) 64 相连接。媒体存取控制子层 64 扮演无线链接控制子层 62 与第一层接口 61 之间的桥梁。媒体存取控制子层 64 将协议数据单元 63 的传递分成一连串的传送时间间隔 (transmission time intervals, TTIs) 72。请参考第 4 图。每一传送时间间隔 72 的间隔长度相同,且在每一段传送时间间隔 72 内,媒体存取控制子层 64 将传送区块组 (transport block set) 74 送至第一层接口 61 等候传递。每一传送区块组 74 包含预定数目的传送区块 (transport block) 704,每一传送区块 704 包含无线链接控制协议数据单元 75 且传送媒体存取控制标头。于不同的传送时间间隔 72 内,无线链接控制协议数据单元 75 的数目可能更改。

虽然于每一协议数据单元 63 中皆内嵌序号,但是在加密开始之前,起始的超高帧号的值才会在两个站台之间传送。于加密开始之后,只有序号被传送,超高帧号并不被传送。相反地,每个站台必需分别依照每一个传输或接收到的协议数据单元的序号来维护目前的超高帧号。每一协议数据单元 63/75 所跟随的序号 76 是用来产生 C 计数值 (Count-C) 680。C 计数值 680 为 32 位的数字,包含超高帧号 681 当作最高阶的  $(32 - n)$  位,且包含序号 682 当作最低阶的  $n$  位。超高帧号 681 起始值被设为 0 或由该无线存取网络指定的值,且当协议数据单元 63/75 的序号 76 返转归零 (rollover) 时加 1。举例而言,假设超高帧号的值为 0,且协议数据单元 63/75 的序号 76 的值为 255, C 计数值 680 会使用 255 的值来对协议数据单元 63 进行加密产生加密的协议数据单元 75。因为序号返转归零的关系,接下来一个的协议数据单元 63/75 的序号 76 的值为 0,而加密模块 67 会将超高帧号 681 的值加 1。因此,用在对下一个协议数据单元 63 进行加密的 C 计数值 680 会变成 256。

由于每个站台必须记录及维护自己的超高帧号,只有在加密开始进行前所接收到的超高帧号的值是有效的同步依据。因此,一站台与其它的站台的超高帧号有失去同步的风险。因为当序号超过其最大表示值会将超高帧号加 1,有两种情况会造成超高帧号不同步:当接收端漏收了超过序号空间 (SN

space)数量的协议数据单元,或者序号字段中某些位于无线传送中因干扰而发生数据错误。

- 为了帮助该接收端正确地将解密过的伺服数据单元正确地串接还原,该传送端的第二层子层在协议数据单元之前端插入长度指标字段,标示出该伺服数据单元的数据的结束位置(假设原始的伺服数据单元长度够长,允许划分成多个协议数据单元)。另外,假使多个短伺服数据单元可以放在同一个协议数据单元之内,也可以将这些短伺服数据单元前后串接放在一个协议数据单元,并在其前端插入恰当的长度指标字段,以指示伺服数据单元结束的位置。长度指标字段的大小取决于该协议数据单元的大小,可以是7位或是15位。
- 假使没有足够的数据量来填满整个协议数据单元,可附加上填充字段或者附挂式状态回报单元。第5图为非确认模式协议数据单元的例子。该标头包含序号81,延伸位82。该标头另外可能包含一长度指标字段83以及另一延伸位84。跟随在序号81之后的延伸位82系用来表示接下来一个字节的内容是否为数据还是长度指针字段。同样地,跟随在长度指标字段83之后的延伸位84系用来表示接下来一个字节的内容是否为数据还是另一长度指标字段。当一个协议数据单元80包含不只一个伺服数据单元,或者加入填充位或附挂式状态回报单元,如此一来,长度指标字段83是必须的且紧紧跟随在序号81之后。所有在数据85之后未使用到的字节皆必须加上填充字段86。协议数据单元的所有未使用的区域需放在该协议数据单元的最后部分,即所谓的填充字段。特定的长度指标字段值,称为填充长度指标字段,被用来标示填充字段的的存在与否。该填充字段需为恰当的长度,以令该协议数据单元的长度完全符合无线链接控制子层所规定的长度。该填充字段可为任意值,且该传送站台与接收站台会直接忽略填充字段的内容。在确认模式协议数据单元中,状态回报单元也可以是附挂式的,使用到部分或全部的填充字段的的空间,且以特定的长度指标字段值来标示附挂式状态回报单元的存在与否。当该协议数据单元的数据后面接着的是附挂式状态回报单元,用此长度指针字段值来取代原先的填充长度指标字段值。假使只使用填充字段的部分空间,附挂式状态回报单元之后所剩余的空间自动被视为填充区。

- 当对非确认模式传输进行加密时(其序号为7位且其超高帧号为25位),协议数据单元除了第一个字节(包含序号及延伸位)外的所有的字节都要经过加密。至于确认模式传输(其序号为12位且其超高帧号为20位),协议数据



单元除了前两个字节(包含序号及延伸位)外的所有的字节都要经过加密。

由上文可知,长度指标字段可以用来检测上述传送端与接收端之间的超高帧号不同步的问题。事实上,这些发现可以在“错误的长度指针字段与无线链接控制重置流程”(R2-031831)文章以及美国专利申请案 2003/0091048  
5 “于无线链接控制架构中检测加密参数的不同步”中找到。此外,如美国专利申请案 91048 所揭露的,特定数值的填充字段也可用来检测超高帧号的不同步。

内嵌于协议数据单元的长度指针字段不合规定的种类包含:

(a) 当内嵌于协议数据单元的长度指针字段的数值大于该协议数据单元  
10 所能容纳的最大数据长度。

(b) 当有多个长度指标字段时,其排列并非按照依序递增的顺序。

(c) 当长度指标字段值是依规定所保留而不得使用的值。

(d) 当内嵌于协议数据单元的长度指针字段系特定的值但不在其所必需的特定位置上。

15 然而,上述文件用来检测超高帧号不同步的方法仍有其缺点。以 R2-031831 文件而言,当检测到错误的长度指标字段值,该文件假设该错误的长度指标字段值是由超高帧号不同步所造成的,且触发无线链接控制层的重置流程来恢复超高帧号同步。值得注意的是这种技术只能用在确认模式传输。于 R2-031831 文件所揭露的方法并不适用于非确认模式传输,因为  
20 R2-031831 文件以及 3GPP TS 25.322 均未提到非确认模式传输的无线链接控制层的重置流程。以美国专利申请案 91048 而言,该专利技术利用信令传输流程来恢复同步。同时适用于确认模式与非确认模式的信令传输流程为:无线链接控制重置流程以及保密参数同步流程。对于确认模式而言,无线链接控制重置流程是另外一种信令传输流程。

25 信令传输流程包含传送端与接收端之间的信令传输及处理,额外的传输是相当费时的。由于传输的延迟、无线传输中讯号遗失以及重传逾时机制等因素,造成超高帧号同步流程非常费时。因此,为了维持站台中的超高帧号同步,以及为了避免费时流程及系统重置所招致的数据遗失,寻求新的方法是有必要的。

30

发明内容

本发明是关于一种恢复无线通讯系统超高帧号同步的方法，包含在加密期间开始前，采用起始的超高帧号，于加密期间检测无线通讯系统各个站台间的超高帧号是否不同步，调整目前的超高帧号以产生调整过后的超高帧号，以及采用该调整过后的超高帧号进行加密。

5 根据本发明的一个方面，提供了一种应用于无线通讯系统的接收站台中确保超高帧号同步的方法，其包含下列步骤：于加密期间开始时，采用起始超高帧号；检测一串接收到的协议数据单元的序号是否连号；以及假使接收的协议数据单元的序号与其前一协议数据单元的序号及其后一协议数据单元的序号均不连号，则删除该接收的协议数据单元。

10 根据本发明的另一个方面，提供了一种用于无线通讯系统的接收站台中恢复超高帧号同步的方法，其包含下列步骤：(a) 于加密期间开始时，采用与传送站台相同的起始超高帧号；(b) 于加密期间内检测到接收站台中的超高帧号未保持同步；(c) 调整该接收站台中现有的超高帧号以产生调整过的超高帧号；以及(d) 该接收站台采用该调整过的超高帧号进行解密。

15

#### 附图说明

第 1 图为已知的第三代移动通讯联盟 (3GPP) 通讯协议的三层式架构的方块图。

第 2 图为已知的第二子层传送/接收流程的简易示意图。

20 第 3 图为先前技术第二子层接口的详细方块图。

第 4 图为先前技术典型的传送时间间隔分配的示意图。

第 5 图为先前技术非确认模式协议数据单元 (UMD PDU) 的示意图。

第 6 图表示先前技术协议数据单元中的序号毁损造成超高帧号不同步的示意图。

25 第 7 图为本发明一实施例避免协议数据单元中的序号毁损造成超高帧号不同步的示意图。

第 8 图为本发明较佳的实施例的流程图。

第 9 图为本发明另一较佳的实施例的流程图。

30 第 10 图为本发明利用校正超高帧号来对已接收的协议数据单元进行解密的示意图。

第 11 图为本发明利用校正超高帧号来对已接收的协议数据单元进行解

密的另一示意图。

[主要元件标号说明]

|    |           |           |     |           |
|----|-----------|-----------|-----|-----------|
|    | 10        | 第一站台      | 11  | 消息        |
|    | 12        | 第三层接口     | 13  | 应用程序      |
| 5  | 14        | 信令消息      | 15  | 第二层伺服数据单元 |
|    | 16        | 第二层接口     | 17  | 第二层协议数据单元 |
|    | 18        | 第一层接口     |     |           |
|    | 20        | 第二站台      | 21  | 消息        |
|    | 22        | 第三层接口     | 23  | 应用程序      |
| 10 | 24        | 信令消息      | 25  | 第二层伺服数据单元 |
|    | 26        | 第二层接口     | 27  | 第二层协议数据单元 |
|    | 28        | 第一层接口     |     |           |
|    | 40        | 第一站台      | 41  | 第一层接口     |
|    | 42        | 第二层接口     | 43  | 第三层接口     |
| 15 | 44        | 伺服数据单元    | 45  | 协议数据单元    |
|    | 46        | 加密模块      | 47  | 加密金钥      |
|    | 48        | 加密的协议数据单元 |     |           |
|    | 400 - 403 | 序号        | 410 | 第一协议数据单元  |
|    | 411       | 第二协议数据单元  |     |           |
| 20 | 50        | 第二站台      | 51  | 第一层接口     |
|    | 52        | 第二层接口     | 53  | 第三层接口     |
|    | 54        | 伺服数据单元    | 55  | 协议数据单元    |
|    | 56        | 解密模块      | 57  | 加密金钥      |
|    | 58        | 加密的协议数据单元 |     |           |
| 25 | 500 - 503 | 序号        |     |           |
|    | 60        | 第二层接口     | 61  | 第一层接口     |
|    | 62        | 无线链接控制子层  | 63  | 协议数据单元    |
|    | 64        | 媒体存取控制子层  | 65  | 缓冲存储器     |
|    | 66        | 伺服数据单元    | 67  | 加密模块      |
| 30 | 680       | C 计数值     | 681 | 超高帧号      |
|    | 682       | 序号        |     |           |

|    |           |              |           |          |
|----|-----------|--------------|-----------|----------|
|    | 72        | 传送时间间隔       | 74        | 传送区块组    |
|    | 75        | 无线链接控制协议数据单元 |           |          |
|    | 76        | 序号           |           |          |
|    | 704       | 传送区块         |           |          |
| 5  | 80        | 协议数据单元       | 81        | 序号       |
|    | 82、84     | 延伸位          | 83        | 长度指针字段   |
|    | 85        | 数据           | 86        | 填充字段     |
|    | 90        | 接收站台         | 91        | 协议数据单元组  |
|    | 92        | 第一协议数据单元     | 93        | 第二协议数据单元 |
| 10 | 94        | 第三协议数据单元     |           |          |
|    | 800 - 812 | 步骤           | 900 - 924 | 步骤       |

#### 具体实施方式

虽然本发明是以第三代移动通讯联盟 (3GPP) 所制定的标准规范为背景，  
15 但值得注意的是，本发明也可应用在任何类似架构的通讯系统上。

在协议数据单元中，并没有特定的字段用来检测超高帧号是否同步。尽管长度指标字段以及填充字段可以达到上述的目的，但并非专注于此，且在很多情况下并不适用。因此，依靠长度指标字段来检测超高帧号不同步的技术并不能适用于某些不包含长度指针字段的协议数据单元，且不能保证可以  
20 正确检测出超高帧号不同步。而且，使用依据长度指标字段技术调整过后的超高帧号来对协议数据单元进行解密，既使没有发现其它的超高帧号不同步的现象，并不能保证该调整过后的超高帧号是正确同步的值。此外，考虑循环冗余校验 (CRC) 机制无法检测出协议数据单元的位损毁，所检测到的超高帧号不同步的现象并不能保证该超高帧号是真的不同步。(因为循环冗余校验机  
25 制无法检测出协议数据单元的位损毁的机率相当低，单一事件中无法检测出两个协议数据单元的位损毁的机率太低，并不列入本发明的考虑。) 基于上面的因素，本发明利用先前提到的检测超高帧号不同步的技术，但加上一些改良，以克服先前技术所遇到的问题。

由上面可得知，造成超高帧号未保持同步的可能性有二：(1) 该接收端连续漏收协议数据单元的数目超过“序号空间总数”，以及(2) 内嵌于协议数据  
30 单元的序号字段位在无线传输过程中损毁。

考虑第二项造成超高帧号失去同步的可能性,也就是,循环冗余校验机制未能检测出协议数据单元的位损毁的状况。当该位损毁的情况发生在序号字段,该损毁的序号会跳号,下一协议数据单元的序号则恢复正常的顺序。请参考第6图。第6图代表接收站台90接收到一连串的协议数据单元且从左到右依序进行解密。就非确认模式传输而言(重传是不允许的),协议数据单元91的正常序号应为000、001、002、003、004、005等。然而,第二个协议数据单元93的位损毁造成其序号变成100,因此该接收站台会收到一连串的协议数据单元,序号为000、100、002、003、004、005等。根据先前技术,该接收站台会因为第三个协议数据单元94的序号(SN=002)小于先前一个已接收的协议数据单元93(SN=100),判定第三个协议数据单元94是属于下一循环,而将其超高帧号加1。再者,由于非确认模式协议的规定,该第三个协议数据单元94不会重传。于是,接下来所收到的协议数据单元的超高帧号在该传送站台与该接收站台的差值会保持为1。(特别注意的是,单一事件中循环冗余校验机制连续未检测出两个协议数据单元的位损毁的机率太低。)根据本发明,假使接收到的协议数据单元的序号,既不跟前一个收到的协议数据单元的序号连号,也不跟后一个收到的协议数据单元的序号连续,则删除该协议数据单元,当作从未接收到。因此,例子中的第二个协议数据单元93(SN=100)会被删除(请参考第7图),而下一个协议数据单元94(SN=002)会被认定与第一个协议数据单元92(SN=000)属于同一个超高帧号循环。因此,这种方法可保持超高帧号的同步。

考虑第一项造成超高帧号失去同步的可能性。当该接收端连续漏收协议数据单元的数量超过“序号空间总数”时,该传送端与该接收端的超高帧号的差距为1。除非接收端连续漏收协议数据单元的数量超过序号空间总数的两倍(在非确认模式中序号空间总数=128,必须连续漏收超过256个协议数据单元),否则该传送端与该接收端的超高帧号的差距只可能为1。因此,将该接收端的超高帧号加1即可恢复超高帧号同步。对于连续漏收超过256个协议数据单元的状况,如果将原先的超高帧号加1以后仍然检测到超高帧号不同步,可再将该接收站台的超高帧号加1,即可恢复同步。由于连续漏收更多的协议数据单元的机率会愈来愈小,在线调整超高帧号的次数可限定在预定的次数以内。当调整超高帧号达到该限定的预定次数后,仍然检测到超高帧号不同步,则中止该在线校正超高帧号流程,并启动信令传输流程。

上面的实施例可以概括成以下的步骤，请参考第 8 图：

步骤 800： 流程开始。接收到协议数据单元。

步骤 801： 将超高帧号校正计数器的值重置为 0。

5 步骤 802： 对所接收到的协议数据单元，检测是否有超高帧号不同步的现象。

步骤 803： 判断是否有检测到超高帧号异步的现象。假如没有，程序中  
止于步骤 812。否则，程序继续进行到步骤 804。

步骤 804： 检查超高帧号校正计数器的值。假如计数器的值小于 2，程  
序继续进行到步骤 805。否则，程序进行到步骤 810。

10 步骤 805： 将目前的超高帧号的值加 1。

步骤 806： 将超高帧号校正计数器加 1，程序并回到步骤 802。

步骤 810： 假使该超高帧号的值已经加了 2，则停止再行校正超高帧号  
并启动加密同步流程。

步骤 811： 程序中止。

15 步骤 812： 程序中止。

该超高帧号校正计数器所允许最大的值是考虑到较佳实施例的值。此限  
值可以是其它任何实际的数值。此外，该流程的步骤可以是其它的顺序，或  
者插入其它的步骤。且步骤 804 可以被省略，直接从步骤 803 进行到步骤 805。  
此外，传送端传送序号空间数量的协议数据单元相当费时，在接收到协议数  
据单元一段预定时间并成功进行解密后，该接收端可以停止超高帧号校正步  
20 骤(步骤 805)。该预定时间不能小于该传送端传送一序号空间数量的协议数  
据单元所花费的时间。

上面的实施例，当该超高帧号校正流程被中止且视为失败时，删除该经  
过超高帧号校正流程的协议数据单元。指派原先超高帧号的值给下一协议数  
25 据单元，除非该被删除的协议数据单元的序号与下一协议数据单元的序号有  
序号返转归零的情况发生，此种情况自然需将原先超高帧号的值加 1。由于  
该超高帧号校正最大次数被预设为 2(步骤 804)，当超高帧号校正流程被中止  
且被视为失败时，原先的超高帧号的值已被加 1 加了两次，因此目前的超高  
帧号的值为原先超高帧号的值加 2。因此，指派给下一个协议数据单元的超  
30 高帧号应为目前修正过的超高帧号的值减 2，即原先超高帧号的值。

值得注意的是，一协议数据单元的每一个位都有可能毁损，而循环冗余校

验机制无法检测到该毁损的机率虽然不高，却有可能。假使协议数据单元中用来检测超高帧号不同步现象的字段毁损，譬如，长度指标字段或者填充字段，则会误判为超高帧号不同步。无论是由此类协议数据单元数据毁损或是由接收端连续漏收超出一序号空间数目的协议数据单元都会判断成超高帧号不同步，都同样会启动超高帧号校正，后者固然会恢复同步，前者则愈修正愈糟糕。因此，需利用额外的方法来处理因误判而持续启动超高帧号校正的状况。该超高帧号校正流程被限定成只能执行预定的次数(本实施例为两次)。假使超高帧号校正流程第二次中止，表示有两个连续的协议数据单元被删除，该在线恢复超高帧号同步的方法被视为失败，且启动信令传输流程。

10 上述的实施例可以概括于下述的步骤，请参考第 9 图：

步骤 900： 流程开始。接收到协议数据单元。

步骤 901： 将超高帧号校正计数器及流程计数器重置为 0。

步骤 902： 检测是否有超高帧号不同步的现象。

步骤 903： 判断是否有检测到超高帧号不同步的现象。假如没有，

15 程序中中止于步骤 924。否则，程序继续进行到步骤 904。

步骤 904： 检查超高帧号校正计数器的值。假如其值小于 2，程序继续进行到步骤 905。否则，程序进行到步骤 908。

步骤 905： 将目前的超高帧号的值加 1。

步骤 906： 将超高帧号校正计数器加 1，程序并回到步骤 902。

20 步骤 908： 假使该超高帧号的值已经加了 2，则删除此协议数据单元并回存原先超高帧号的值。

步骤 910： 将流程计数器加 1，以记录该超高帧号校正流程执行过的次数。

25 步骤 912： 检查该流程计数器。假如计数器的值小于 2，程序继续进行到步骤 914。否则，程序进行到步骤 918。

步骤 914： 假使该流程计数器尚未到达 2，而目前的超高帧号校正流程被视为失败，则回存校正前的超高帧号的值且重置该超高帧号校正计数器为 0。

30 步骤 916： 等到该接收端接收到下一个协议数据单元，程序回到步骤 902。

步骤 918： 假使该流程计数器的值已到达 2，中止超高帧号校正流程且

将目前的协议数据单元删除，并启动加密同步流程。

步骤 920: 程序中止。

步骤 924: 程序中止。

5 该超高帧号校正计数器及流程计数器所允许的最大的值是考虑到一个较佳实施例的值，此限值可以是其它任何实际的数值。此外，该流程的步骤可以是其它的顺序，或者插入其它的步骤。

除了超高帧号同步校正程序失败而回存原先的超高帧号值之外，此中所描述的超高帧号校正通常都是增加，上述的实施例中并没有提到将目前的超高帧号的值减少来恢复超高帧号同步。因此，另一实施例中，在增加超高帧号限定的次数仍无法成功时，将原先的超高帧号的值减 1，以代替直接将该协议数据单元删除。如同先前实施例中将超高帧号的值加 1 的方法，超高帧号修正次数及流程执行次数亦可限制在预定的次数以内。

10 根据另一实施例，以序号跳号检测超高帧号不同步的方法改为以长度指标字段来检测。考虑下述状况：在连续接收到第二预定数量的已解密的非确认模式协议数据单元中检测到第一预定数量的协议数据单元的长度指针字段有不合规定的现象，譬如说，10 个协议数据单元中发现有 2 个协议数据单元的长度指针字段不合规定。根据本实施例，将目前的超高帧号的值加 1，将长度指标字段不合规定的最后一个协议数据单元，及其后所接收到的协议数据单元，使用此调整过的超高帧号的值来进行解密。只要每 10 个协议数据单元中有 2 个以上的协议数据单元发现其长度指针字段不合规定，本实施例即可执行一次。如同其它实施例所述，可限定本实例所述流程的最大执行次数，超过此次数，此流程即视为失败而启动信令传输程序。

25 举例说明如下。假设该接收端收到一连串的非确认模式协议数据单元，其序号为 000、001、002、006、007、008、009、010、011、012、013、014、015、016、017、019。为求简化，假设序号为奇数的协议数据单元才包含长度指针字段，而序号为偶数的协议数据单元不包含长度指针字段；因此，只有序号为 001、007、009、011、013、015、017、019 的协议数据单元会检测到不合规定的长度指标字段(请参考第 10 图)。假设超高帧号的值为 0 时，检测到序号为 001、009 的协议数据单元(前三个已解密的且包含长度指针字段的非确认模式协议数据单元中的两个)含有不合规定的长度指标字段。因此，30 将该超高帧号的值加 1 并对序号为 009 及其后所有的协议数据单元重新解密。



假设超高帧号的值为 1 时, 序号为 011、017 的协议数据单元(接下来四个已解密的且包含长度指针字段的非确认模式协议数据单元中的两个), 又检测到不合规定的长度指标字段, 因此将该超高帧号的值再加 1, 并对序号为 017 及其后的所有协议数据单元重新解密。

- 5 事实上, 检测不合规定的长度指标字段并不能百分之百保证可以正确地检测到超高帧号不同步的错误情况。本实施例的第二预定数目如果较小, 由于条件较严, 触发超高帧号校正程序的机率较低, 所需恢复同步的时间会比较长。然而, 不管时间需要多长, 仅需要重复几次校正程序, 就一定可以恢复超高帧号同步。另一方面, 选择较大的第一预定数目, 可以减少误判, 而
- 10 使此机制更可靠, 但会增加恢复超高帧号同步的时间。值得注意的是, 本实施例中更新过后的超高帧号是从最后一个不合规定的长度指针字段的非确认模式协议数据单元才开始套用, 以对其后的所有协议数据单元进行重新解密。这样做可以减少存储器的需求, 假使不将减少存储器需求列入主要的考虑, 可以将更新过后的超高帧号套用在每一个检测到不合规定的长度指针字段的
- 15 非确认模式协议数据单元上, 如第 11 图所示。

- 另外超高帧号不同步的现象是填充字段不符合预定值。如先前技术所述, 填充字段占据协议数据单元后面所有剩余的空间, 其目的是为了为了满足该协议数据单元符合通讯系统所要求的预定长度。填充字段如规定特定的值, 当发现填充字段非该特定值时, 即代表超高帧号的未保持同步。因此, 我们也可
- 20 以用填充字段的值来判断超高帧号是否保持同步。

上述任何数目或是任何组合的超高帧号不同步现象, 都可以用在本发明的方法之中, 来检测超高帧号是否保持同步。

- 本发明的优点是, 该接收站台可以在线恢复超高帧号同步, 无须中断传输流程。可以将因为套用不同步的解密参数而造成数据错误的情况降到最低。
- 25 此外, 除非必要, 不必启动信令传输流程(像是无线链接层的重置流程), 可以因而避免其所需的冗长流程, 增加传输效能。

以上所述仅为本发明的较佳实施例, 凡依本发明权利要求范围所做的均等变化与修饰, 皆应属本发明的涵盖范围。

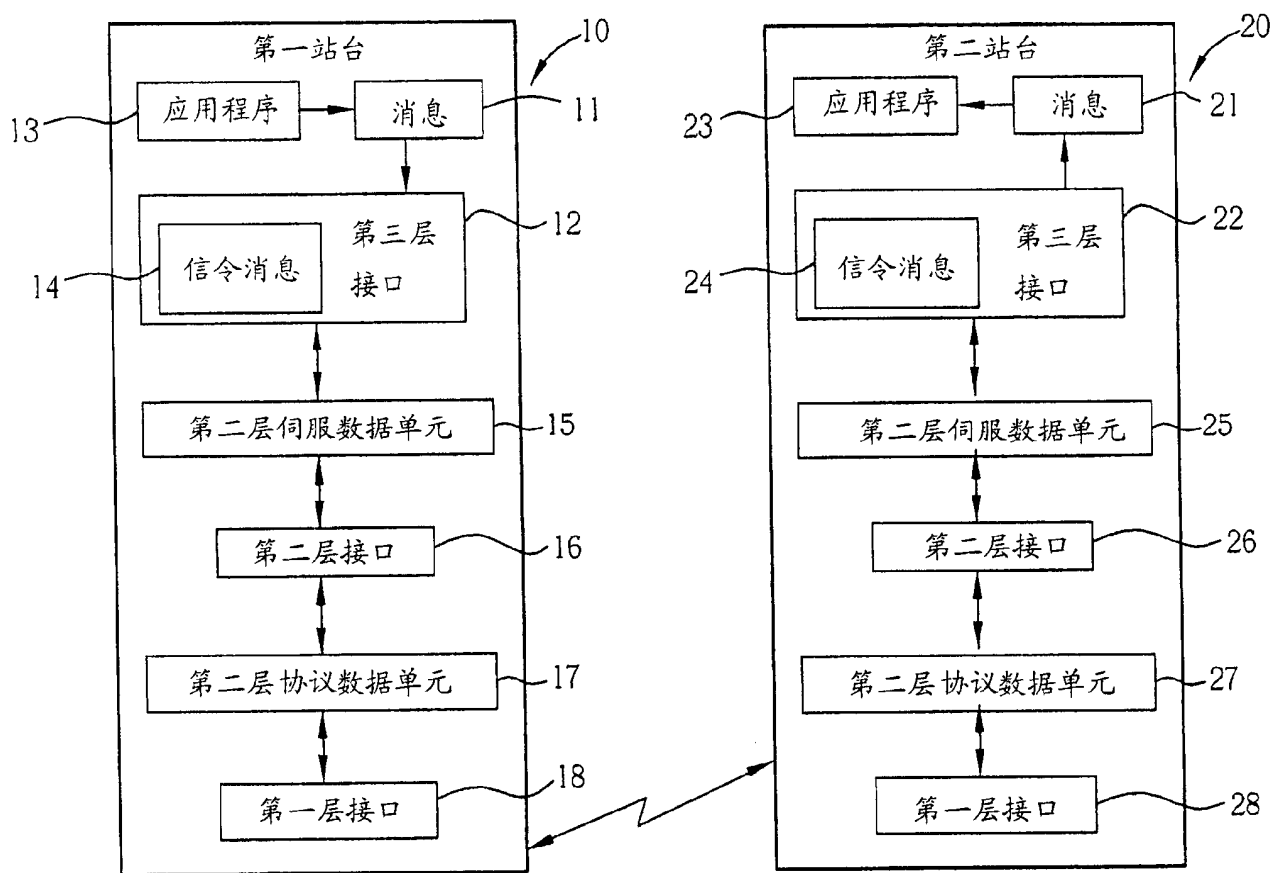


图 1

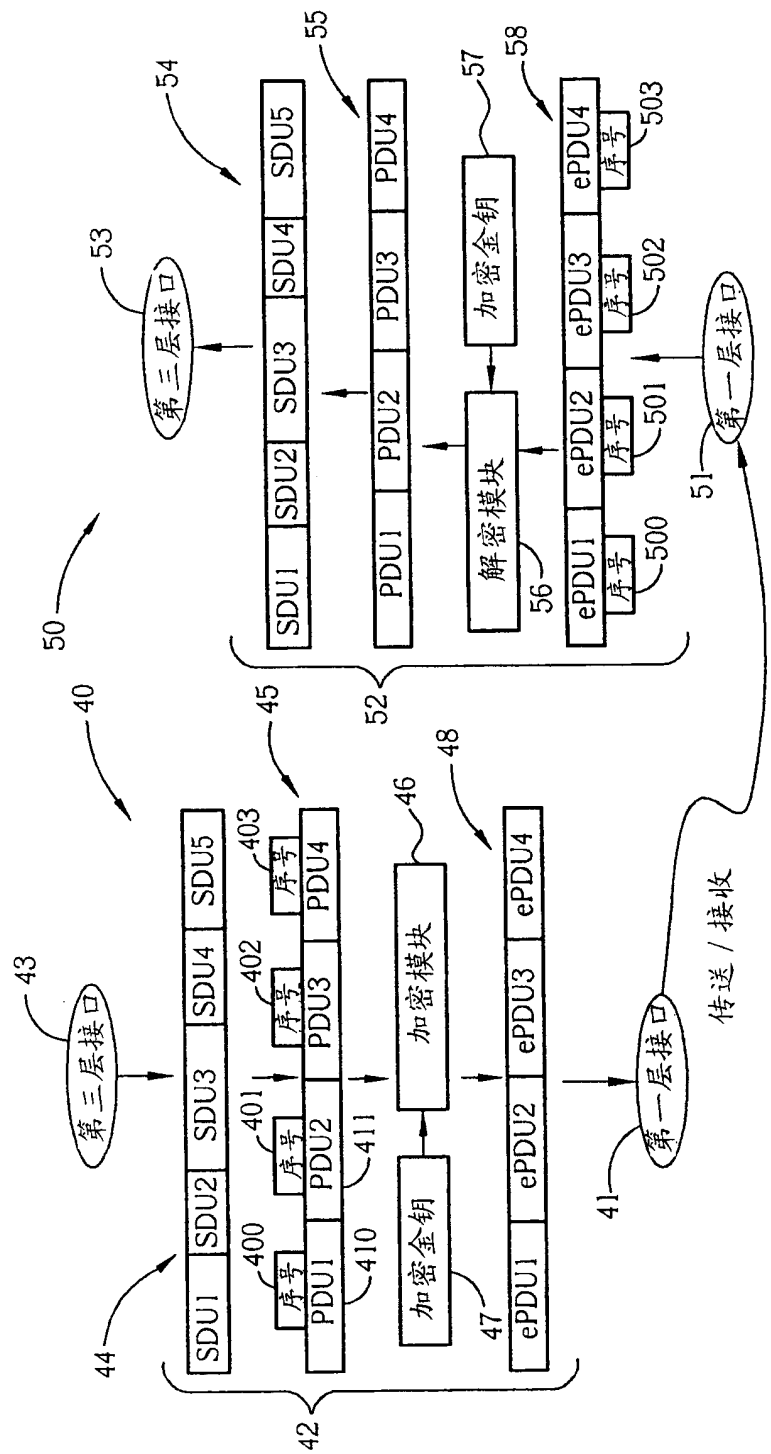


图 2

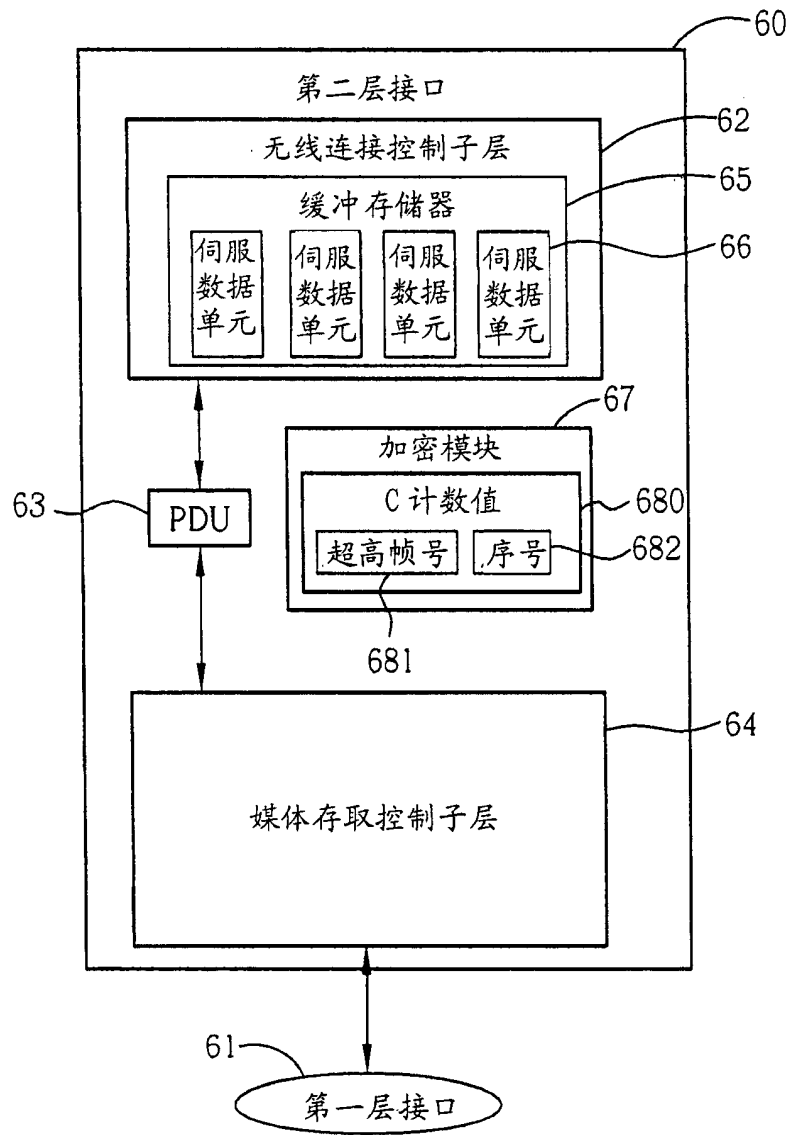


图 3

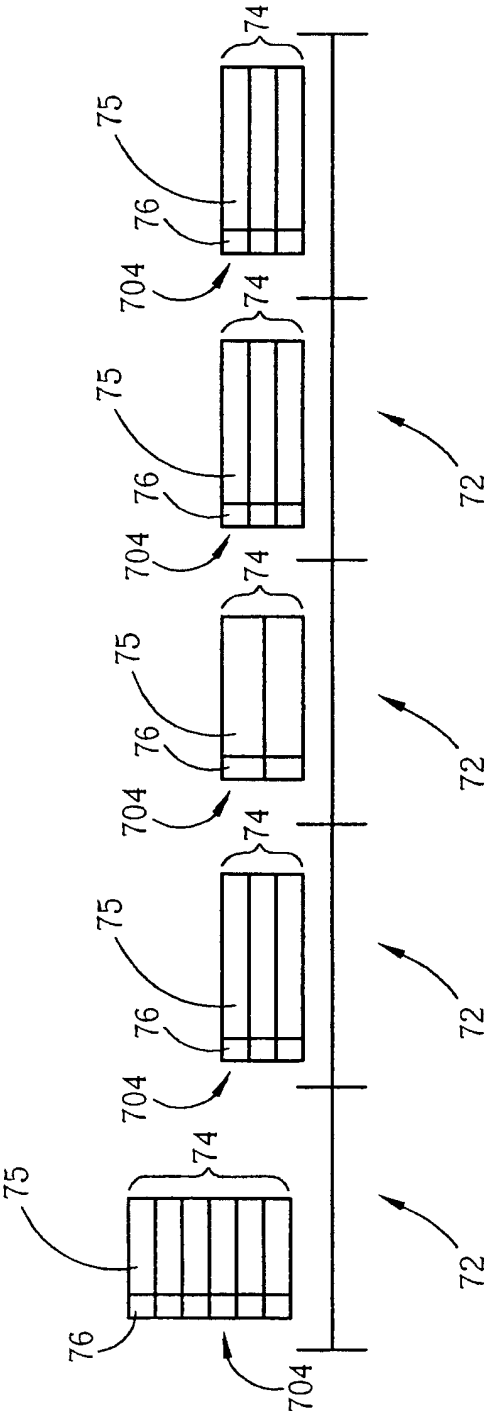


图 4

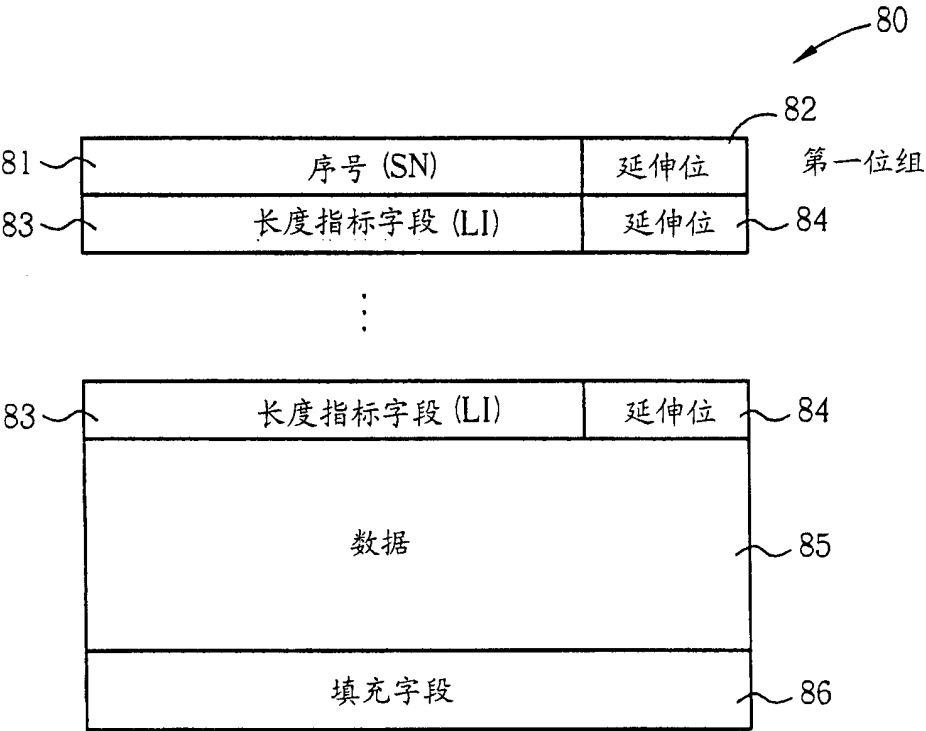


图 5

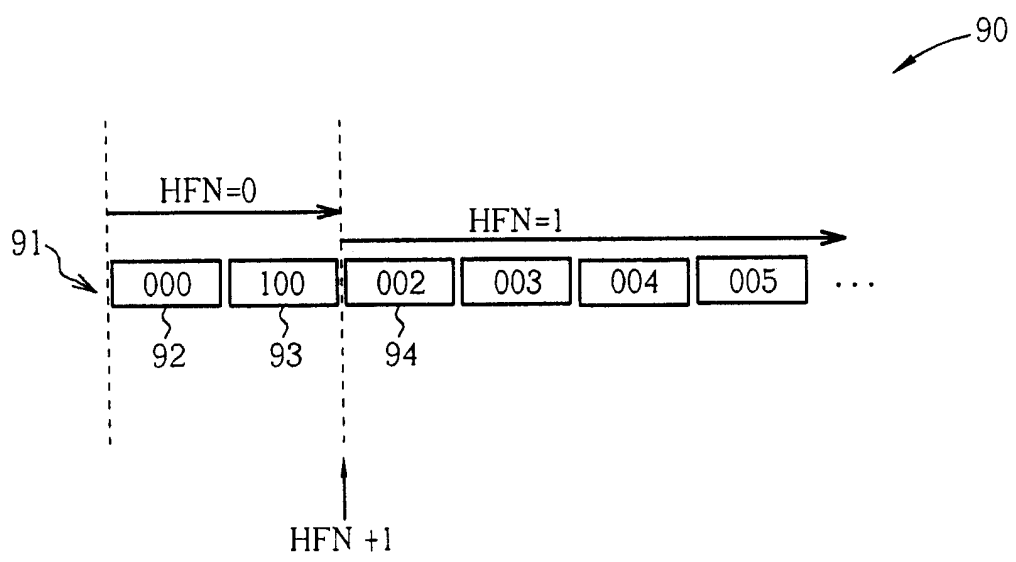


图 6

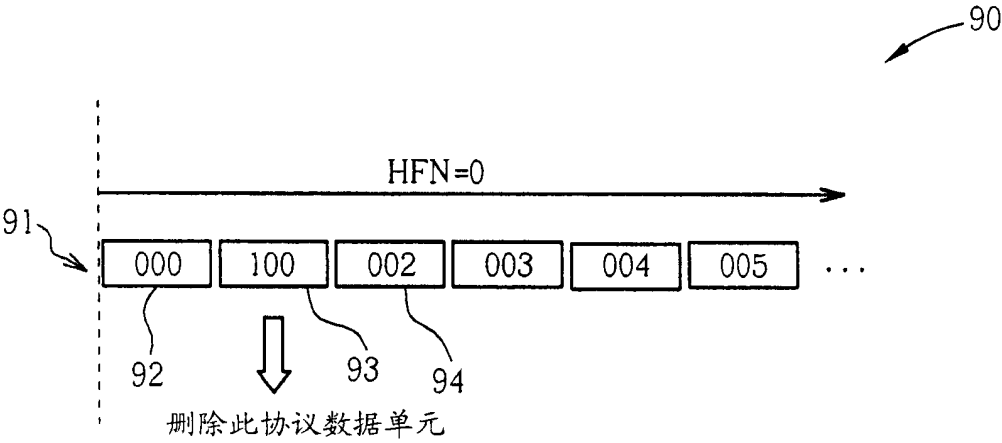


图 7



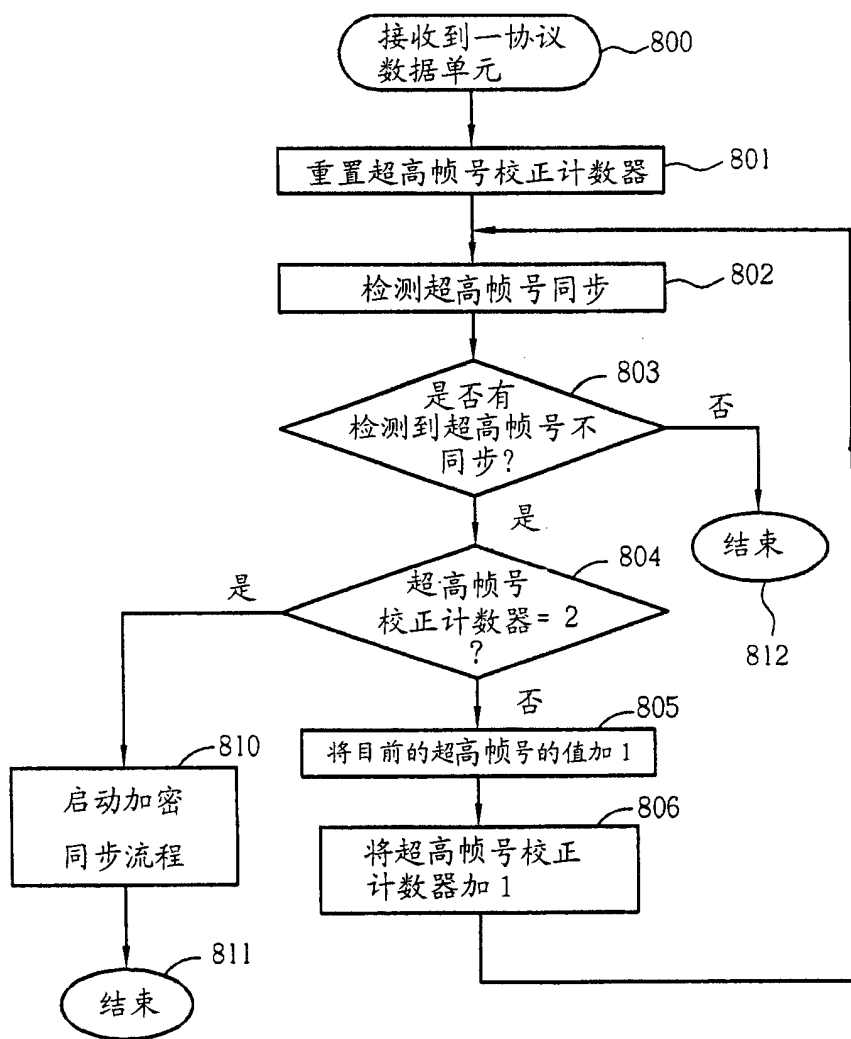


图 8

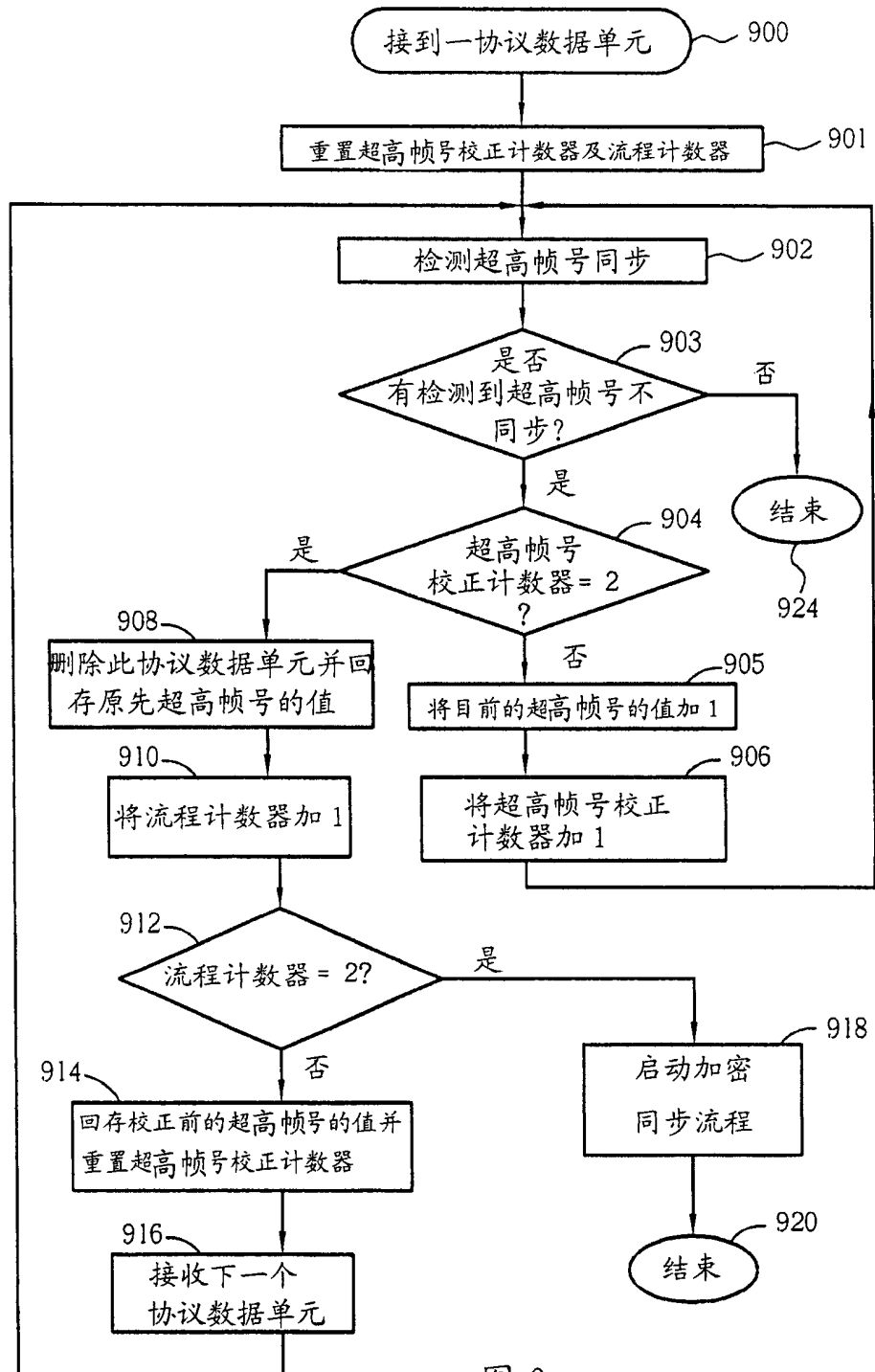


图 9

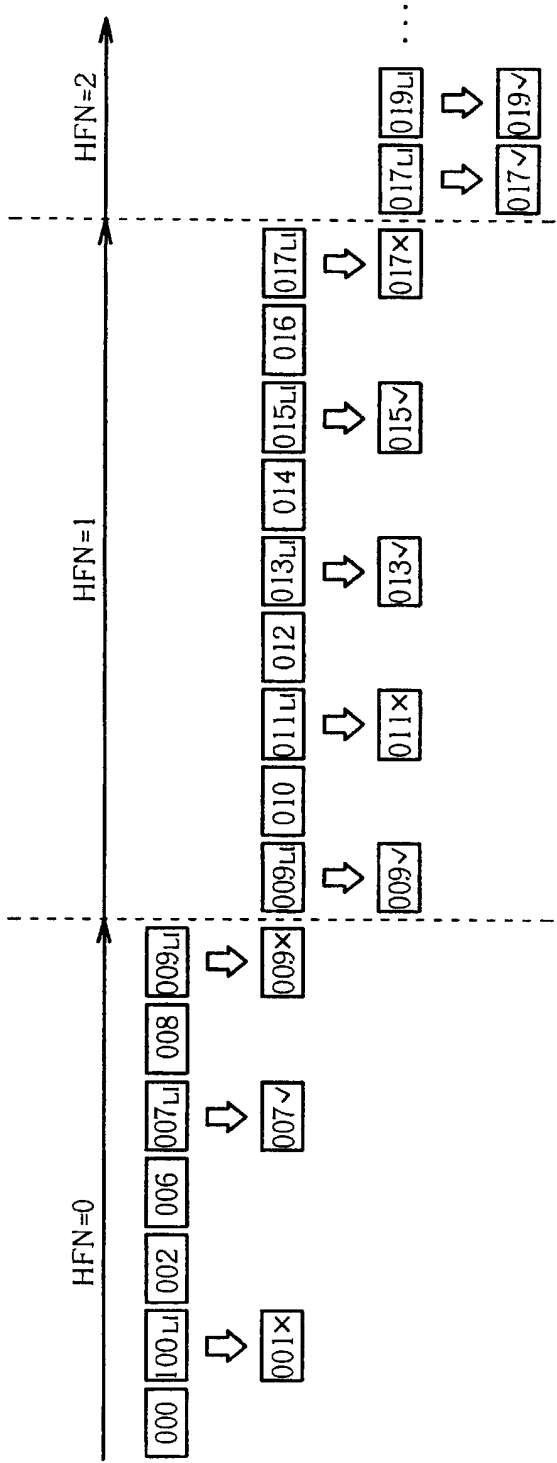


图 10

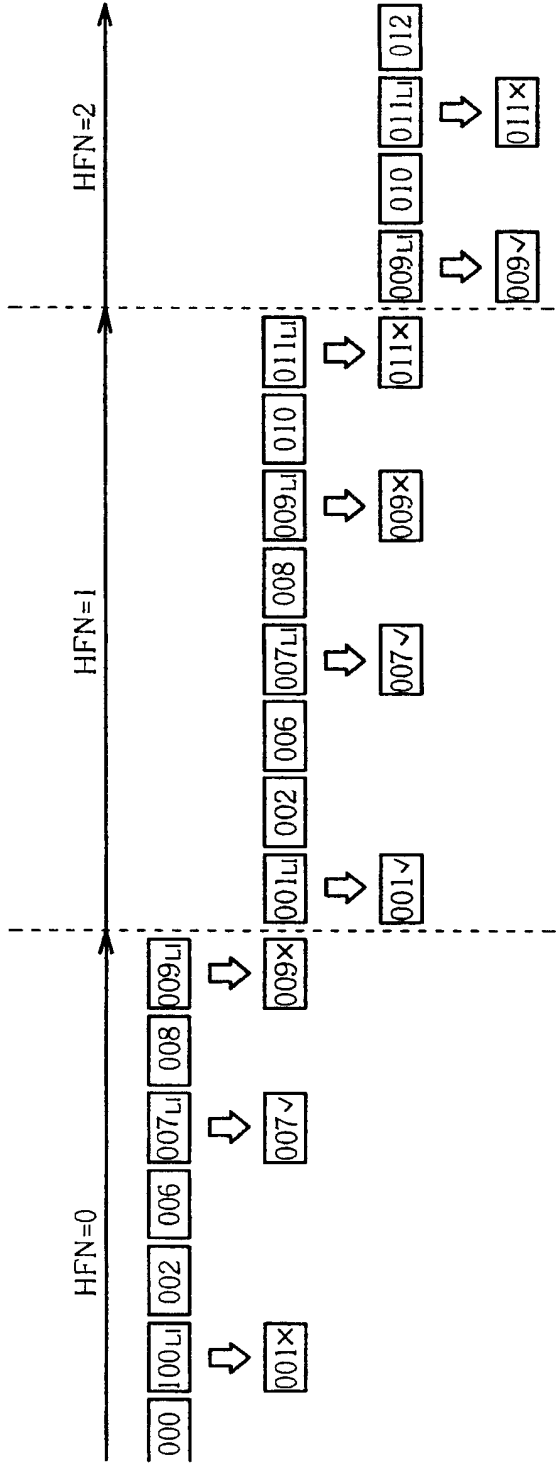


图 11