[19]中华人民共和国国家知识产权局

[51]Int. Cl[7]
H04L 12/22
H04L 9/12

[12]发明专利申请公开说明书

[21]申请号 00800068.9

[43]公开日 2001年5月2日

[11]公开号 CN 1293847A

[22]申请日 2000.1.10 [21]申请号 00800068.9
[30]优先权
[32]1999.1.28 [33]EP [31]99200245.1
[86]国际申请 PCT/EP00/00212 2000.1.10
[87]国际公布 WO00/45552 英 2000.8.3
[85]进入国家阶段日期 2000.9.25
[71]申请人 皇家菲利浦电子有限公司
地址 荷兰艾恩德霍芬
[72]发明人 B·J·范里恩赛维尔

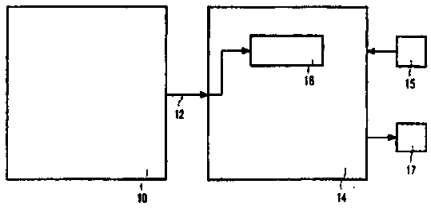
[74]专利代理机构 中国专利代理(香港)有限公司
代理人 吴增勇 傅 康

权利要求书3页 说明书6页 附图页数1页

[54]发明名称 数据分组传输系统中解密密钥的同步

[57]摘要

根据本发明的传输系统包括发射机(10)和接收机(14)。发射机可 发送数据分组例如IP分组到接收机。这些数据分组包含首标(24)如ESP首标;和加密数据字段(26)。通过改变解密密钥(48),可以将接 收机(14)中的数据字段(26)解密。首标(24)包含表示解密密钥(48)的 变 化的信息(32)。信息(32)可以被包含在ESP首标的SPI字段中。这样,接收机(14)可以准确地判定何时开始使用新的解密密钥(48)。



ISSN1008-4274

权 利 要 求 书

1. 用于把数据分组从发射机(10)发送到接收机(14)的传输系统，所述数据分组包含首标(24)和加密数据字段(26)，所述数据字段(26)是可以通过改变解密密钥(48)解密的，其特征在于：所述首标(24)包含表示所述解密密钥(48)的变化的信息(32)。

2. 根据权利要求 1 的传输系统，其特征在于：所述数据分组包含 IP 分组。

3. 根据权利要求 2 的传输系统，其特征在于：所述首标(24)包含 ESP 首标，所述 ESP 首标包含表示所述解密密钥(48)的变化的信息(32)。

4. 根据权利要求 3 的传输系统，其特征在于：所述 ESP 首标包含 SPI 字段，所述 SPI 字段包含表示所述解密密钥(48)的变化的信息(32)。

5. 用于把数据分组发送到接收机(14)的发射机(10)，所述数据分组包含首标(24)和加密数据字段(26)，所述数据字段(26)是可以通过改变解密密钥(48)解密的，其特征在于：所述首标(24)包含表示所述解密密钥(48)的变化的信息(32)。

6. 根据权利要求 5 的发射机(10)，其特征在于：所述数据分组包含 IP 分组。

7. 根据权利要求 6 的发射机(10)，其特征在于：所述首标(24)包含 ESP 首标，所述 ESP 首标包含表示所述解密密钥(48)的变化的信息(32)。

8. 根据权利要求 7 的发射机(10)，其特征在于：所述 ESP 首标包含 SPI 字段，所述 SPI 字段包含表示所述解密密钥(48)的变化的信息(32)。

9. 用来从发射机(10)接收数据分组的接收机(14)，所述数据分组包含首标(24)和加密数据字段(26)，所述数据字段(26)是可以通过改

变解密密钥(48)解密的，这样实现所述接收机(14)、以便将所述加密数据字段(26)解密，其特征在于：所述首标(24)包含表示所述解密密钥(48)的变化的信息(32)。

10. 根据权利要求 9 的接收机(14)，其特征在于：所述数据分组包含 IP 分组。

11. 根据权利要求 10 的接收机(14)，其特征在于：所述首标(24)包含 ESP 首标，所述 ESP 首标包含表示所述解密密钥(48)的变化的信息(32)。

12. 根据权利要求 11 的接收机(14)，其特征在于：所述 ESP 首标包含 SPI 字段，所述 SPI 字段包含表示所述解密密钥(48)的变化的信息(32)。

13. 一种用来把数据分组从发射机(10)发送到接收机的方法，所述数据分组包含首标(24)和加密数据字段(26)，所述数据字段(26)是可以通过改变解密密钥(48)解密的，其特征在于：所述方法在所述首标(24)中包含所述解密密钥(48)的变化的指示。

14. 根据权利要求 13 的方法，其特征在于：所述数据分组包含 IP 分组。

15. 根据权利要求 14 的方法，其特征在于：所述首标(24)包含 ESP 首标，所述解密密钥(48)的变化的所述指示被包含在所述 ESP 首标内。

16. 根据权利要求 15 的方法，其特征在于：所述 ESP 首标包含 SPI 字段，所述解密密钥(48)的变化的所述指示被包含在所述 SPI 字段。

17. 一种包含数据分组的复合信号(12)，所述数据分组包含首标(24)和加密数据字段(26)，所述数据字段(26)是可以通过改变解密密钥(48)解密的，其特征在于：所述首标(24)包含表示所述解密密钥(48)的变化的信息(32)。

18. 根据权利要求 17 的复合信号(12)，其特征在于：所述数据

分组包含 IP 分组。

19. 根据权利要求 18 的复合信号(12), 其特征在于: 所述首标(24)包含 ESP 首标, 所述 ESP 首标包含表示所述解密密钥(48)的变化的信息(32)。

20. 根据权利要求 19 的复合信号(12), 其特征在于: 所述 ESP 首标包含 SPI 字段, 所述 SPI 字段包含表示所述解密密钥(48)的变化的信息(32)。

00·09·25

说　明　书

数据分组传输系统中解密密钥的同步

本发明涉及传输系统，该系统把数据分组从发射机发送到接收机，所述数据分组包含首标和加密数据字段，所述数据字段是可以通过改变解密密钥解密的。

本发明还涉及把数据分组发送到接收机的发射机、从发射机接收数据分组的接收机，把数据分组从发射机发送到接收机的方法和含有数据分组的复合信号。

按照前序的传输系统可以从1995年8月颁布的RFC1825文件《因特网协议安全框架》中得以了解。在许多现代数据传输系统中，发射机向多个接收机广播数据业务。在这样的系统中，希望只有有限数量的接收机用户，例如只有那些付了费或者属于某个组的接收机用户访问数据业务。通过对数据加密、通过将加密的数据发送到接收机、并且通过只向被授权享有所述数据的那些用户提供用于将所述数据解码所需的解密密钥，就可以实现对数据业务的这种有条件访问。由于安全原因，解密密钥在使用一段时间或发送一定量数据后必须改变。向新的解密密钥的转变必须在发射机和接收机之间同步。

已知的传输系统如何处理这种同步还不清楚。

本发明的目的是提供一种传输系统，其中接收机能够有效地处理加密数据分组的解密。这个目的在依据本发明的传输系统中实现，所述传输系统具有以下特征：所述首标包含表示解密密钥的变化的信息。借助于在首标中包含这种信息，接收机能够准确地确定什么时候开始使用新的解密密钥。

根据本发明的传输系统的一个实施例具有以下特征：所述数据分组包含IP分组。这样，按IP级定义的数据业务就能安全地广播。

根据本发明的传输系统的另一个实施例具有以下特征：所述首标包含ESP首标，所述ESP首标包含表示解密密钥的变化的信息。通过包含表示ESP首标的SPI字段中所述解密密钥的变化的信息，实现与因特网上使用的IP加密机制的最大共同性。这种SPI字段是所有不同的加密方法中唯一的强制字段，所以这个字段不作改变。

从下面参考附图对最佳实施例的描述中，本发明的上述目的和特征将更加明显，附图中：

图1示出按照本发明的传输系统的方框图。

图2示出被包含在一个部分中的数据分组的结构图。

图3示出SPI字段的结构图的例子。

图1示出按照本发明的传输系统的方框图。在这样的传输系统中，代表许多数据业务的许多数据信号12或复合信号12由发射机10发送到接收机14。该传输系统可以包括其它接收机14。终端用户可以通过例如象键盘或遥控单元的输入装置15来控制接收机14。被选择的业务可以显示在显示装置17上。可以借助数据信号12，通过发射机10把数据分组、例如IP分组广播到许多接收机14。

在这样的传输系统中，最好只有有限数量的接收机14的用户、例如只有那些已经付费或属于某个组的用户，访问数据业务。这种有条件的访问数据业务可以通过在发射机10加密数据并发送该加密的数据到接收机14来实现。而且，解密数据所需的解密密钥本身被加密并且只有那些被授权享有所述数据的接收机14才能够对所述解密密钥解密。依靠解密密钥，接收机14可以将所述数据解密。解密密钥可以发送许多次，以便接收机14能够迅速地访问解密密钥。

发射机10以所谓的授权控制消息(Entitlement Control Message)或ECMs的形式将解密密钥传送到接收机14。这种可嵌入在IP分组中的ECM包含解密密钥或控制字的加密形式。通过在接收机14中将ECM解密，例如依靠包括在接收机14中的智能卡，如果接收机还具有相应的数据业务或授权，则该解密密钥可被揭示。出于安全

的目的，控制字值经常改变，例如在一定的时期后或在一定数量的数据传输后。在控制字值已经改变的情况下，新 ECM 必须传送到接收机。因此 ECMs 流与每一个可以有条件地访问的数据业务相联系。可能需要重发未改变的 ECMs 好几次，以便减小接收机 14 访问所述业务占用的时间。(为了访问业务，接收机 14 必须首先获取相应的 ECM。)接收机 14 中可以包括滤波装置 16，用于滤出第二和进一步的相同解密密钥事件的目的。

用于计算机网络环境下的、例如因特网的广播数据业务的传输系统的例子可从文件 RFC 1825“用于互联网协议的安全体系结构”(1995 年 8 月)中了解到。在这一文件中，描述了 IP 分组加密的两种方式:

传送方式: IP 分组的有效载荷被加密。

隧道方式: 整个 IP 分组被加密，并且新的 IP 首标位于加密后的分组前。这种方式，例如，用来加密通过非受托网络的虚拟专用网的业务。

在两种方式中，所谓的 ESP(Encapsulating Security Payload-封装安全有效载荷)首标包括在包含加密的数据的新建立的 IP 分组中。这种 ESP 首标从被称为安全参数索引(SPI)的 32 位的字段开始。与目标地址一道，SPI 尤其限定了哪些密钥用于解密、使用哪些解密算法以及怎样应用解密算法。

从文件草案 EN 301 192 V1.1.1 欧洲标准“数字视频广播(DVB);用于数据广播的 DVB 规范”中知道用于广播数据业务的传输系统。这种已知的传输系统例如可以在有线电视(CATV)网络环境中实现。在这种环境中，发射机 10 包括 CATV 网络的头端，接收机 14 包括终端用户的机顶盒、电视机或个人计算机(PCs)。数字信号 12 包含多路复用信号 12，后者可以以 MPEG-2 传送流的形式实现。MPEG-2 传送流是许多所谓业务的多路复用。这样的业务可包含音频/视频流、交互式应用程序(例如以 MHEG-5 格式)、其它类型的数据(例如 IP 分

组)或这些成分的组合。通常，头端 10 向机顶盒 14 发送几个传送流 12。这样，大量业务(或频道)能通过头端 10 广播到许多机顶盒 14。

机顶盒 14 可以调谐到特定的传输流 12，然后可从传输流 12 检索信息。这样的机顶盒通常只有一个调谐器并因此一次只能接收单一传输流 12。当用户想要看电视节目时，或想要运行交互式应用程序时，或想要访问其它类型的数据时，机顶盒 14 调谐到相应的传输流 12，并从那个时刻正被广播的业务中检索和/或处理所需要的数据。

图 2 示出数据分组的结构图，该数据分组被包含在第一段中。DVB 已定义了用于数据广播的 6 个协议栈。这些协议栈之一是所谓的多协议封装(multi-protocol encapsulation)或 MPE。在这种情况下，在数据分组和 MPEG 段之间存在着一对一的映射。并且 MPEG 段通常以几个 MPEG-2 传送流分组的形式发送。MPEG 段具有特定的类型，如协议层 *DSM-CC 专用数据*和 *DVB 多协议封装*所定义的。在图 2 所示的结构图中，数据分组是 IP 分组，它包含 IP 首标 22、ESP 首标 24 和加密的 IP 有效载荷或数据字段 26。数据字段 26 可依靠改变的解密密钥 48 来解密。ESP 首标包含所谓的安全参数索引(SPI)字段。MPE 段首标 20 表明数据分组被嵌入到 MPE 段。ECSs 也可嵌入到相同的结构中。包含 ECM 的分组称为解密分组。解密分组最好被包括在与包含数据分组的第一段链接的第二段中。第一和第二段依靠第一和第二段的至少一部分而链接在一起，所述一部分对所述两段来说是相同的。通过把加密的数据分组和与其有关的解密分组集中在链接在一起的部分中，接收机利用滤出所有包含所述相同部分的分组的单个滤波器可以容易地获得所述数据分组和解密所述数据分组所需的解密分组。所述相同的部分最好被包括在所述部分首标 20 中。例如，在文件草案 EN 301 192 V1.1.1 欧洲标准“数字视频广播(DVB)；用于数据广播的 DVB 规范”中，表 3 中定义的 MPE 段首标 20 的 table_id 和/或 MAC_address 部分可以用以这一目的。

图 3 示出 SPI 字段结构图的例子。这是用于因特网的所有不同 IP

解密方法的仅有强制字段，因此这一字段是不变的。其目的是标识(与目的地址一道)接收机 14 应当使用哪些密钥和算法解密数据。在本实施例中，SPI 字段的开始 14 位被用来存储 ECM 流参考符号 30，后者提供 ECM 流和加密的数据之间的关联。第 15 位用来存储表示密钥变化的信息 32。依靠这一信息 32，可以在传输系统中使控制字的变化同步。当用以加密数据的控制字改变其值时，同步位 32 相应改变其值。这允许接收机 14 准确地确定何时开始使用新控制字值。SPI 字段的第 16 位 34 被保留将来使用。SPI 字段的最后 16 位被用来存储传输系统使用的有条件访问系统的标识符 36。

表明解密密钥变化的信息 32 也可以存储在多位计数器中。

对于接收机 14 中的智能卡来说，处理 ECM 是花费时间的。因此为了避免对加密数据的扩大缓冲的需要，在实际使用相应的控制字之前的一些时候应发送新 ECM。在接收机 14 还使用旧控制字解密数据时，它必须存储新控制字。通常将相同的 ECM 发送几次，以便减少业务访问时间。为了将业务解密，首先必须将 ECM 解码，以便获得控制字。如果没有传输误差，ECM 包含单一控制字就足够了。可是如果 ECMs 包含两个连续的控制字，则可得到更健全的系统。如果在 ECM 中有两个或更多连续的控制字，重发相同的 ECM 在由于传输误差而可能丢失 ECM 时增加了接收到控制字的可能性。

在 MPE 段的首标 20 中，已经定义所谓的 payload_scrambling_control 字段(两位)，用来表示改变到另一个控制字(见文件草案 EN 301 192 V1.1.1 欧洲标准“数字视频广播(DVB)；用于数据广播的 DVB 规范”中表 3)。对于包含数据的 IP 分组，这些同步位表示内容被加密(11)或没有被加密(00)。对于传送 ECM 的 IP 分组，所述位表示控制字是偶数(01)或非偶数(10)。这些同步位可被最好是硬件滤波器的滤波装置 16 使用，用来滤出多个相同 ECM 情况，以便不必由软件来去除这些相同 ECM 情况。如果使用加密，则滤波装置 16 在(1x)和(x1)之间交替。最初，滤波装置 16 使用滤波器

1x。这意味着当第一控制字(非偶数)已通过滤波装置 16 时开始使用滤波器 x1。第一控制字的第二和进一步的事件被滤波装置 16 滤出。第二控制字(偶数)的第一事件通过滤波装置 16，之后，滤波装置 16 开始使用滤波器 1x。第二控制字的第二和进一步的事件被滤波装置 16 滤出。第三控制字的第一事件现在可以通过滤波装置 16 等等。

说 明 书 附 图

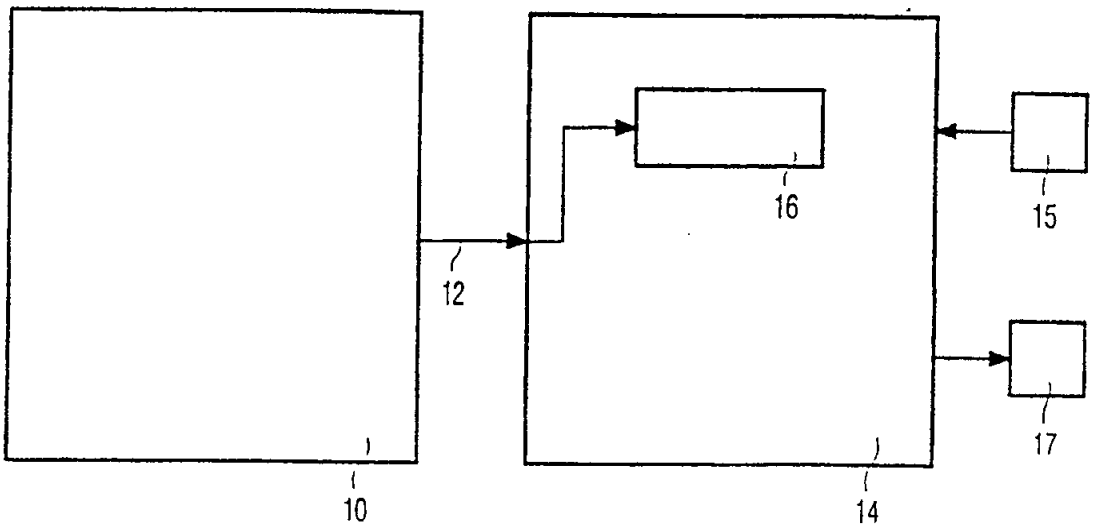


图 1

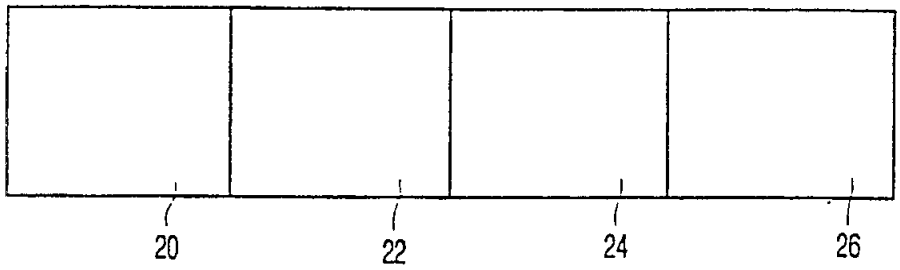


图 2

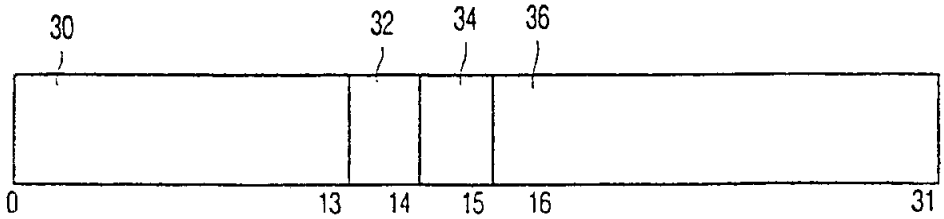


图 3