[19]中华人民共和国国家知识产权局

[51]Int. Cl[7]
H04L 9/08 H04Q 11/04

[12]发明专利说明书

[21] ZL 专利号 96197989.5

[45]授权公告日 2003 年 1 月 1 日

[11]授权公告号 CN 1097904C

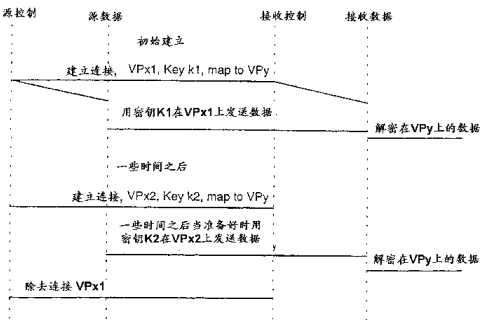
[22]申请日 1996.10.24 [21]申请号 96197989.5
[30]优先权
[32]1995.11.4 [33]GB [31]9522639.5
[86]国际申请 PCT/GB96/02597 1996.10.24
[87]国际公布 WO97/17781 英 1997.5.15
[85]进入国家阶段日期 1998.4.29
[73]专利权人 马科尼通讯有限公司
地址 英国英格兰考文垂
[72]发明人 R·J·普罗托尔
[56]参考文献
CN1054693A 1991. 9.18 H04L9/14
CN1054693A 1991. 9.18 H04L914
EP0660570A2 1995. 6.28 H04L2906
EP0660570A2 1995. 6.28 H04L29/06,
H04Q11/04
COMMUNICATIONS OF THE ACM VOL. 38, NO. 2 1995. 2. 1 secure communications in atm networks daniel stevenson, nathan hillery and
COMMUNICATIONS OF THE ACM VOL38 NO2 1995. 2. 1 SECURE COMMUNICATIONS IN ATM NETWORKS DANIEL STEVENSON NATHAN HILLERY AND
审查员 张 蔚
[74]专利代理机构 中国专利代理(香港)有限公司
代理人 栾本生 王忠忠

权利要求书 1 页 说明书 3 页 附图 2 页

[54]发明名称 加密密钥管理

[57]摘要

在具有一组虚拟通道或电路的异步传输模式电信网络中,可更新在源和接收机之间发送数据所用的加密密钥,最初发送数据采用第一加密密钥,通过该组虚拟通道或电路的第一个,并通过该组虚拟通道或电路的第二个建立连接,通过这个连接将第二加密密钥从源送到接收机,接着通过该组虚拟通道或电路的第二个,采用第二加密密钥发送数据。



ISSN1008-4274

1．在具有一组虚拟通道的异步传输模式（ATM）电信网络中，一种用于更新在源和接收机之间发射的数据所用的加密密钥的方法，其特征在于：最初发射数据采用第一加密密钥，通过该组虚拟通道的第一个，并通过该组虚拟通道的第二个建立连接，通过该连接将第二加密密钥从源发送到接收机，接着通过该组虚拟通道的第二个，采用第二加密密钥发射数据。

2．在具有一组虚拟电路的异步传输模式（ATM）电信网络中，一种用于更新在源和接收机之间发射数据所用的加密密钥的方法，其特征在于：最初发射数据采用第一加密密钥，通过该组虚拟电路的第一个，并通过该组虚拟电路的第二个建立连接，通过该连接将第二加密密钥从源发送到接收机，然后，通过该组虚拟电路的第二个采用第二加密密钥发射数据。

加密密钥管理

本发明涉及在采用比如虚拟通道或虚拟电路的异步传送模式（ATM）系统中的加密密钥的更新，使得用很简单的方法更新和管理加密密钥，而不存在通常的信息发射机与接收机之间的同步变化问题。

如图 1 所示，将数据加密，经过一系统发送，然后在另一端解密，如果加密密钥是不变的，则是直进式的。然而，对于一个必须工作相当长时间的系统，常常需要改变其密钥。在现有的系统中，通过经系统发送新的密钥做到了这一点，在终点预装第二密钥，并给出某个转接信号。则接收机必须能以精细地控制方式不丢失数据地保持两个密钥，且在它们之间很快变化。同步两端之间的转接是实际的问题。

在文章“proceedings of the Sympsium of NetwoRk and Distributed system Security” San Diego, UsA, Feb. 1995, pages 17-30 中，描述了一个以 MCNC 设计的实验密钥捷变密码系统。该系统与 ATM 本地和广域网络是兼容的。该系统以对终端用户透明的，并与现存的公用网络标准兼容的方式，建立和管理主机之间的安全连接。

密码单元支援在 ATM 协议层的硬件加密和解密。该系统是 SONET 兼容的并以 OC－12C 速率（622Mbps）全双工操作。对于每个安全连接商定单独的加密密钥。每个密码单元能管理 65000 多个有源安全连接。可以所谓的“bum-in-the fibre”保密入口方式，或以直接的 ATM 主机接口来连接密码单元。通过以证书为基准的系统来实施叉电鉴别和通路控制。

根据本发明，在具有一组虚拟通道的异步传输模式（ATM）电信网络中，提供一种用于更新在源和接收机之间发送数据所用的加密密钥的方法，最初发射数据采用第一加密密钥，通过该组虚拟通道的第一个，并通过该组虚拟通道的第二个建立连接，通过这个连接将第二加密密钥从源发送到接收机，接着通过该组虚拟通道的第二个采用第二加密密钥发射数据。

还提供：一种在具有一组虚拟电路的异步传送模式（ATM）电信网络中，一种用于更新在源和接收机之间发送数据所用的加密密钥的方法，最初发射数据采用第一加密密钥，通过该虚拟电路组的第一个，

并通过该虚拟电路组的第二个建立连接，通过这个连接将第二加密密钥从源送到接收机。接着，通过该虚拟电路组的第二个，采用第二加密密钥发射数据。

在 ATM 网络中，能够建立多个虚拟通道（VPS）或虚拟电路（VCS），除非它们被实际使用了，用光了，无网络资源。不是具有两个密钥的复杂性和精细地控制转接，其基本的想法是建立具有新密钥的第二 VP/VC，并且当准备好时，以选择发送器在新的 VP/VC 上开始发送数据。无需复杂的转接机构，当新 VP/VC 使用期间，可简单地将老的的一个去掉。

在图 2 中示出了操作的顺序。

该实施例对用户加密 VP（VPY），最初建立在经过 ATM 传输的

VPX1 上，并用密钥 K1 加密。后来为该密钥需要更新的，使用 VPX2 和密钥 K2 建立第二连接。将它建立之后，当选择时发送器可即开始在新 VP 上发送数据，随后可将老的 VP 断开。这种实施例加密 VPS，对于虚拟电路其结构是同样的。

可将这个程序如下地扩展到双向的情况，当源要改变所用的密钥时，它建立它的数据处理器，以便在新的 VP 上处理新的密钥，然后它告诉接收机，当得到变化信息，它准备好时，它开始新的 VP，当它到达时，前端设备用新的密钥简单地开始接收在新 VP 上的数据。

如果 ATM 传输是在如接入网等闭路系统中，上述的程序是足够的。在开放网络中，有另外两个需要考虑的事情:

该网络将或者必须建立（和管辖）在它们的全频带要求上并进而提供整个网络的两个电路，或者管辖两个电路一起的通信量的总和。每个选择都不是特别复杂的。

只要保证两个电路之间信元序列的完整性，基本的机构就好了。如果信元顺序完整性不可能，则可应用其它的方法，比如以足够转接时间保持通信量的加密器，提供给变化中的最坏情况。

可将这种密钥控制的方法实际应用到任何分组网络。具体地说，对于 提供密钥的频繁更新而没有复杂的转换协议和其它的复杂性，这是一个很实际的方法。这很适合存取系统将保密程序送给选择数目的用户，对已签购该程序的那些用户给予密钥以便加密它。现在，在这种环境中，可要求频繁地改变密钥，这种机构使改变密钥很容易。

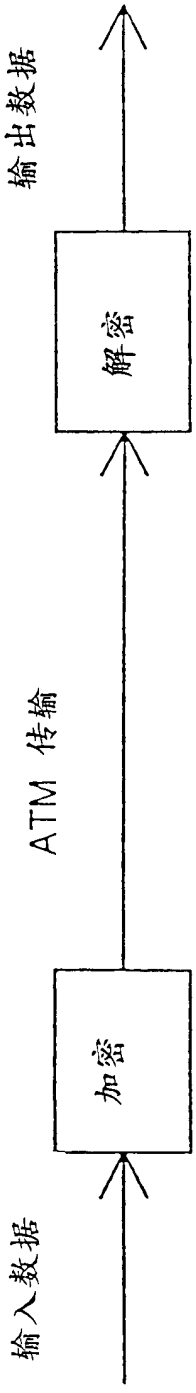


图 1

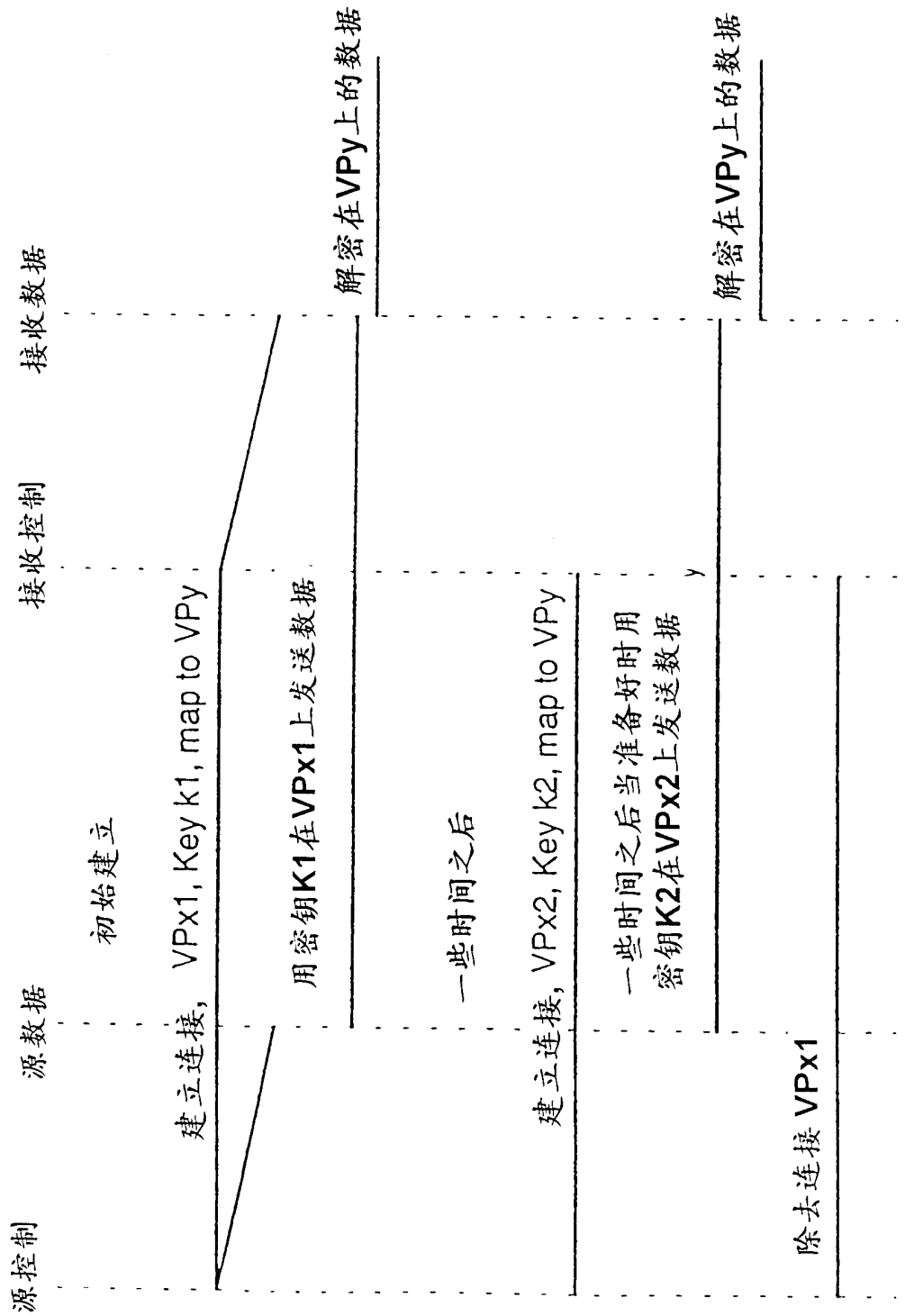

源控制
源数据
接收控制
接收数据
初始建立
建立连接, VPx1, Key k1, map to VPy
用密钥K1在VPx1上发送数据
解密在VPy上的数据
一些时间之后
建立连接, VPx2, Key k2, map to VPy
一些时间之后当准备好时用
密钥K2在VPx2上发送数据
y
解密在VPy上的数据
除去连接 VPx1

图 2