[19]中华人民共和国国家知识产权局

[51]Int.Cl[7]
H04L 9/14

[12]发明专利申请公开说明书

[21]申请号 99118815.2

[43]公开日 2000年4月19日

[11]公开号 CN 1250994A

[22]申请日 1999.9.13 [21]申请号 99118815.2

[30]优先权

[32]1998.9.14 [33]US [31]09/153,272

[71]申请人 朗迅科技公司

地址 美国新泽西

[72]发明人 C·A.·维斯霍里克

[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

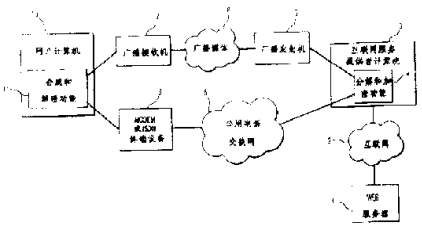
代理人 于 静

权利要求书2页 说明书3页 附图页数1页

[54]发明名称 宽带数据消息的安全传输

[57]摘要

提供信息的安全传输的一种方法。信息的大部分通过非安全信道如终接着许多 接收站的广播媒体来传输。然而,剩余数据通过有保护的信道如由电话连接建 立的点到点信道来传输。当仅获得上述信息的大部分时,对整个信息的截取是 非常困难的。如果在选取经安全信道传输的数据信息的特定比特位时,使用了 加密方法,那么对整个信息的截取就变得更加困难。如果通过安全信道传输的 数据自身能改变加密算法,则对整个信息的截取就变得越发地困难。



ISSN1008-4274

权 利 要 求 书

1. 用来传输数据的装置包括:

用来传输大量数据的非安全连接;

用来传输剩余数据的安全连接;

用来把数据信号分解成表示大量数据的第一种信号和表示剩余数据的第二种信号的装置;

用来把第一种信号和第二种信号合成为表示整个数据的合成信号的装置;

其中上述用来分解数据的装置通过上述非安全连接传输大量数据,及通过上述安全连接传输剩余数据。

2. 权利要求 1 的装置,其中:

第一种信号通过可被多个接收机接收的广播连接来传输;和

第二种信号通过仅可被一个接收机接收的点到点连接来传输。

3. 权利要求 1 的装置,其中上述的分解装置包括生成经加密的第二种信号的装置。

4. 权利要求 3 的装置,其中上述生成经加密信号的装置包括根据由该第二种信号传输的数据内容来生成经加密的信号的装置。

5. 权利要求 1 的装置,其中分解数据信号的装置根据第二种信号所传输的数据的内容执行分解。

6. 一种可靠地传输和接收数据的方法,包括步骤:

将表示上述数据的数据信号分解为表示大量数据的第一种信号和表示剩余数据的第二种信号;

通过没有保护的媒体传输第一种信号;

通过有保护的媒体传输第二种信号;

接收第一种信号和第二种信号;和

将第一信号和第二种信号合成为表示上述数据的合成信号。

7. 权利要求 6 的方法,其中传输第一种信号的步骤包括:

通过可被多个接收机接收的广播媒体传输第一种信号;和

其中传输第二种信号的步骤包括通过仅可被一个接收机接收的连接

传输第二种信号的步骤。

8. 权利要求 6 的方法，其中上述分解上述数据信号的步骤包括对上述第一种信号的数据进行加密的步骤。

9. 权利要求 8 的方法，其中上述对上述第一种信号的数据进行加密的信号步骤包括按第二种信号所传输的数据的内容所决定的方式进行加密。

10. 权利要求 6 的方法，其中上述分解上述数据信号的步骤包括根据由第二种信号所传输的数据的内容分解数据信号的步骤。

说　　明　　书

宽带数据消息的安全传输

本发明涉及能以一种实际无法被截取的方式传输数据消息的方法和装置。

随着因特网（Internet）的日益使用，特别是因特网被日益用来传输宽带数据信号，更加迫切地需要避免这些消息的未经授权的截取。利用被可靠地传输到某个目的地的解密钥的各种方法已经被提出。一条已被用相应的加密钥进行了加密并经一种可被截取媒体传输的消息，就需要由有上述解密钥的、被授权的接收者或者没有上述解密钥的、未被授权的接收者进行解密。各种加密方法已经被提出，但是现代计算机的不断增加的性能使得未经授权的解密变成日益增多的盗窃行为。来自因特网的大多数信息会通过一个共享的媒体，诸如同轴电缆、光纤或无线地广播给许多目的地，该共享媒体具有这样的特征：未经授权的接收者能够很容易地截取并不是传给它们的原始信号。因此，现有的技术存在的一个问题是难于避免被广播给许多目的地的、未经加密的信号被一个不需要该信息的目的地的接收者非法地截取，甚至被截取的经加密的信息也可能被并不需要该信息的那些用户解密。

本发明解决了上述问题，并且对以前的技术进行了改进，其方法是将源传输到目的地的数据的一部分从广播媒体中抽取出来，通过一个较安全和专用的媒体，诸如电话连接来传输；然后将通过广播媒体接收到的数据与从广播媒体中抽取出来并经安全媒质传输的数据组合起来，以便得到完整的数据消息。这种方法的优点是使得解密基本上是不可能的，因为接收方不可能访问数据消息的全部数据。在许多种情况下，安全连接作为一个上游连接用来控制数据消息源；使用此上游连接作为一个双向连接方式就能很方便地形成一个独立的下游连接来传输已被从广播媒体中抽取出来的数据。

根据本发明的一个实施例，将数据中有规律的和重复的部分从广播

媒体抽取出来，并且通过安全媒体传输之前，首先对所有数据进行加密。这种方法的优点是使得部分解密更加困难。

图 1 是一个方框图，描述申请者的发明的原理。

图 1 是一个方框图，描述本发明的操作过程。数据信息源 1 诸如一个 Web 服务器，通过因特网向因特网服务提供者（ISPN）计算机 3 发送数据消息。该计算机包含用来实现分解和加密功能 4 的软件和硬件。随后被分解的信号一部分被传送给广播发射机 5，而另一部分被传输给点到点的公用电话交换网 8。大部分数据去往广播发射机 5，该广播发射机通过广播媒质 6（例如同轴电缆、光纤、无线信道和由这些媒体任意组合而成的媒体）传输此数据。广播接收机 7 从广播媒体中接收该数据信号的广播部分。公用电话交换网 8 向调制解调器或者综合业务数字网（ISDN）终端设备 9 传输非广播部分的数据。广播接收机 7 和调制解调器或 ISDN 终端设备的输出被传输给一个包含合成和解密功能 11 的用户计算机 10，该计算机将这两个信号合成以便重新组成原始数据信号。

从用户计算机到 ISP 计算机再到数据源的连接是在用户计算机和数据源之间建立连接的过程中建立起来的。该数据源由一个 URL（统一资源定位器）码识别。这就使得此方法非常实用，因为不需要额外的连接。

为了使这种方法更加安全，通过安全信道传输的数据能够被用来指明该分解的方法。例如，假设每第 19 位比特通过安全信道传输；最初，通过安全信道所接收到的第一个比特可能被插入到由安全信道和非安全信道两者所接收到的 19 比特的第 10 个比特的位置上。然后，如果那个比特为 0，那么通过安全信道所接收到的下一个比特就可能被插入到通过安全信道和非安全信道所传输的下一个 19 比特组的第 11 个比特位置上。如果通过安全信道所接收到的那个比特是 1，那么通过安全信道所接收到的下一个比特将被插入到通过安全信道和非安全信道所传输的下一个 19 比特组的第 9 个比特位置上。因此，安全信息实际上指明了安全和非安全信息之间的分解的方法，这大大地增加了成功地截取和解密被传输的信息的难度。当然，该分解和合成操作是同步的。

另外或附加地，整个消息的各个段能够被加密。使用简单的加密方法，在传输之前，改变每个段中的比特的顺序；然后，解密过程将所接

收到的每个段的比特重新排列为原来的顺序，把通过安全信道所接收到的比特插入到每个段的固定位置上。

另外，加密方法本身可能受到安全信道的内容的影响。例如，如果安全信道信号是 1，那么对于通过非安全信道的相应段或后续段的数据，使用第一种加密算法；如果安全信道信号是 0，那么使用第二种加密算法。也可以使用基于安全信道的 n 比特的多种加密算法。

根据安全信道的内容进行加密和分解的方法能够合二为一。例如，在通过非安全信道传输经加密的段之前，可将上述的分解方法放在加密操作之前进行。然后，非安全信道的内容在接收机中被解密，并且把通过安全信道所接收到的比特根据上述的插入方式插入到适当的位置。

除根据前面描述的通过安全信道传输的数据的分解和/或加密的两种技术之外，所有消息能够被加密，因此，使截取者的任务进一步复杂了。甚至不加密，如果信道仍是安全的，并且分解周期与该数据的各子段的周期（例如 1 字节长）不相同，那么仅仅基于广播信道信息的信息的解密应该仍是非常困难的。

本发明的首选实施例的许多变动对于那些本领域中一般技术人员来说将是显而易见的。本发明仅由后附的权利要求书所限定。

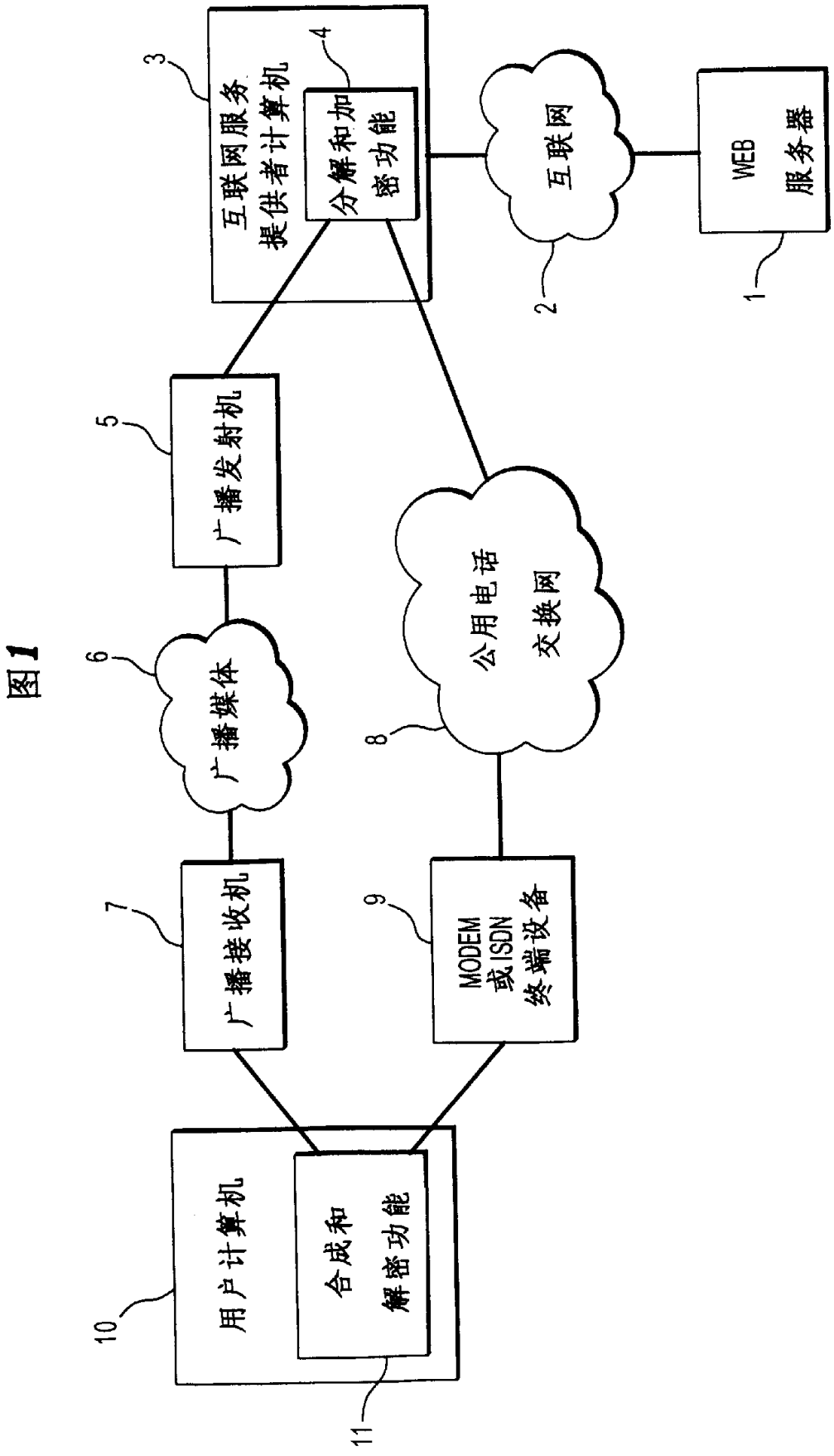

互联网服务
提供者计算机
3
分解和加
密功能
4
互联网
2
WEB
服务器
1
广播发射机
5
广播媒体
6
公用电话
交换网
8
广播接收机
7
MODEM
或ISDN
终端设备
9
用户计算机
10
合成和
解密功能
11

图 1