(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 1522527 B
(45)授权公告日 2010.04.28

(21)申请号 02813475.3

(22)申请日 2002.06.25

(30)优先权数据
60/302,957 2001.07.03 US
10/124,088 2002.04.15 US

(85)PCT申请进入国家阶段日
2004.01.02

(86)PCT申请的申请数据
PCT/SE2002/001267 2002.06.25

(87)PCT申请的公布数据
WO03/005675 EN 2003.01.16

(73)专利权人 艾利森电话股份有限公司
地址 瑞典斯德哥尔摩

(72)发明人 L·-E·约恩松 G·佩尔捷

(74)专利代理机构 中国专利代理(香港)有限公司 72001
代理人 栾本生 陈霁

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

(56)对比文件
CELLATOGLU A ET AL:."Robust header compression forreal-time services in cellular networks".SECOND INTERNATIONAL CONFERENCE ON 3G MOBILE COMMUNICATION TECHNOLOGIES.2001,124-128.
SVANBRO K ET AL:."Wireless real-time IP services enabled byheader compression".VTC2000-SPRING. 2000 IEEE 51ST2.2000,21150-1154.

审查员 程东

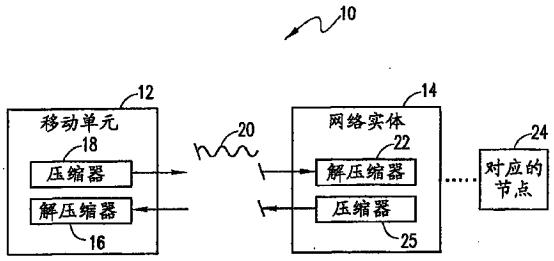
权利要求书 2 页 说明书 6 页 附图 2 页

(54)发明名称

隐式分组类型识别

(57)摘要

在一种用于在压缩器和解压缩器之间的链路上传输分组的系统(10)中,一种方法被提供用于隐式分组类型识别。包括至少第一和第二特性的一组隐式分组传输特性被选择,并且所述压缩器(18,25)被操作分别将所述第一和第二传输特性分配给第一和第二分组类型的分组。所述解压缩器(16,22)被操作检测由所述解压缩器(16,22)接收的分组的传输特性,从而识别被接收的分组为第一或第二分组类型。有用地,无标题分组(26)10包括所述分组类型之一。



CN 1522527 B

1. 一种在压缩器和解压缩器之间通过链路传输分组的系统中的隐式分组类型识别的方法，包括以下步骤：

选择一组隐式分组传输特性，至少包括第一和第二可区别地不同的传输特性；

操作所述压缩器，以便将所述第一传输特性分配给第一分组类型的分组，并且将所述第二特性分配给不同于所述第一分组类型的第二分组类型的分组，以使所述解压缩器能够检测被所述解压缩器接收的分组的所述传输特性，并从而识别接收的分组为第一或第二分组类型。

2. 如权利要求 1 所述的方法，其中：

所述第一分组类型包括无标题的分组。

3. 如权利要求 1 所述的方法，其中：

所述第一分组类型包括无标题的分组，而所述第二分组类型包括具有标题的分组。

4. 如权利要求 1 所述的方法，其中：

所述选择步骤包括在所述压缩器和所述解压缩器之间的预先协商。

5. 如权利要求 1 所述的方法，其中：

所述选择步骤包括为所述第一和第二分组类型选择不同的分组尺寸。

6. 如权利要求 1 所述的方法，其中：

所述选择步骤包括为所述第一和第二分组类型选择不同组的信道编码组合。

7. 如权利要求 1 所述的方法，其中：

所述选择步骤包括为所述第一和第二分组类型选择多路复用选项来创建不同的逻辑信道。

8. 如权利要求 1 所述的方法，其中：

所述选择步骤包括利用加密算法选择一组加密密钥，并且所述压缩器将不同的加密密钥分配给所述第一和第二分组类型。

9. 如权利要求 1 所述的方法，其中：

所述选择步骤包括选择 N 个不同的分组传输特性，用于分别识别 N 个不同分组类型的分组。

10. 如权利要求 1 所述的方法，其中：

所述系统被配置成根据从包括 [VJ]、[IPHC]、[CRTP]、[LLA] 和 [ROHC] 的一组标题压缩 / 解压缩方案中选择的方案来压缩和解压缩分组标题。

11. 一种在压缩器和解压缩器之间通过链路传输分组的系统中的隐式分组类型识别的方法，其中压缩器和解压缩器分别在传输之前压缩分组标题和在传输之后解压缩分组标题，该方法包括以下步骤：

选择一组隐式分组传输特性，其中所述组的不同特性识别不同类型的分组；

压缩利用相应一个所述特性识别的类型的特殊分组的标题，以使所述特殊分组变成无标题的，又使所述解压缩器能够检测所述相应的特性，并从而识别所述特殊分组为无标题分组类型。

12. 如权利要求 11 所述的方法，其中：

所述选择步骤包括选择多个特定的分组尺寸，以便只供无标题分组使用；和

所述压缩器使用所述特定的分组尺寸之一来只传输无标题分组。

13. 如权利要求 11 所述的方法，其中：

所述选择步骤包括选择一组信道编码组合；以及

所述信道编码组合之一只被分配给无标题分组，而所述信道编码组合中的另一个只被分配给另一指定类型的分组。

14. 如权利要求 11 所述的方法，其中：

所述选择步骤包括选择多路复用选项来创建不同的逻辑信道，只在所述逻辑信道之一上发送无标题分组，并且只在所述逻辑信道的另一个上发送另一指定类型的分组。

15. 如权利要求 12 所述的方法，其中：

所述选择步骤包括利用加密算法选择一组加密密钥，所述密钥之一只被分配给无标题分组，而所述密钥中的另一个只被分配给另一指定类型的分组。

16. 如权利要求 12 所述的方法，其中：

所述选择步骤包括在所述压缩器和所述解压缩器之间的预先协商。

17. 一种用于通过链路发送和接收分组的设备，包括：

压缩器，被配置为将第一传输特性分配给第一分组类型的分组，并将第二特性分配给不同于所述第一分组类型的第二分组类型的分组；以及

解压缩器，被配置为检测被所述解压缩器接收的分组的所述传输特性，并从而识别接收的分组为第一或第二分组类型。

18. 如权利要求 17 所述的设备，其中：

所述压缩器和所述解压缩器预先协商分组特性。

19. 如权利要求 17 所述的设备，其中：

所述第一分组类型包括无标题分组，而所述第二分组类型包括具有标题的分组。

20. 如权利要求 17 所述的设备，其中：

所述压缩器为所述第一和第二分组类型分配不同的分组尺寸。

21. 如权利要求 17 所述的设备，其中：

对于所述第一和第二分组类型，分配不同组的信道编码组合。

22. 如权利要求 17 所述的设备，其中：

对于所述第一和第二分组类型，分配多路复用选项来创建不同的逻辑信道。

23. 如权利要求 17 所述的设备，其中：

所述压缩器将与相关的加密算法有关的一组加密密钥中不同的加密密钥分配给所述第一和第二分组类型。

隐式分组类型识别

[0001] 相关的申请的交叉引用

[0002] 本专利申请要求2001年7月3日提交的共同未决的美国临时申请60/302,957的优先权,并且其中公开的全部内容在此引入作为参考。

[0003] 发明背景

[0004] 在此被公开和要求的发明通常涉及一种方法,用于在一个系统中识别分组类型,该系统中利用分组在链路上传输数据。更特别地,本发明涉及一种上述类型的方法,其中至少一些分组的标题传输前被0字节压缩,因此所述分组是无标题的并且分组类型必须被隐含地识别。甚至更特别地,本发明涉及特别适于供诸如蜂窝和无线链路的窄带链路使用的上述类型的方法。

[0005] 由于互联网的巨大成功,在很多不同种类的链路上利用互联网协议(IP)已经成为有挑战性的任务。然而,因为IP的标题相当大,所以关于诸如无线和蜂窝链路的窄带链路来使用IP可能是困难的。例如,对于由普通协议(IP、UDP、RTP)传送的普通语音数据,所述标题可以代表所述分组的大约70%。这导致十分低效的链路使用。

[0006] 术语标题压缩(HC)指通过点对点链路在每一跳跃基础上最小化在标题中承载的信息所必需的带宽的技术。一般来说,在互联网社会中,HC技术有十多年的历史,并且存在几个通常被使用的协议,诸如RFC 1144(下文中"VJ",1990年2月,I ETF网络工作组在由VanJacobson等编写的题为"Compressing TCP/IP Headers for Low-Speed Serial Links(为低速串行链路压缩TCP/IP)"的IETF RFC 1144的文件中提出);RFC 2507(下文中"IPHC",1999年2月,IETF网络工作组在由Degermark,Nordgren与Pink编写的题为"IP HeaderCompression(IP标题压缩)"的IETF RFC 2507的文件中提出);以及RFC 2508(下文中"CRTP",1999年2月,IETF网络工作组在由Casner和Van Jacobson编写的题为"Compressing IP/UdP/RTPHeaders for Low-Speed Serial Links(为低速串行链路压缩IP/UDP/RTP标题)"的IETF RFC 2508的文件中提出)。

[0007] 标题压缩利用这样一个事实,即在一个流量内,标题中的一些字段不改变,或者有小的和/或可预测的值的改变。因此,标题压缩方案最初只发送静态信息,而改变的字段随着它们的绝对值或者按照与分组到分组的差值被发送。当然,完全随机的信息必须在根本没有任何压缩的情况下被发送。所述标题压缩方案通常可以被实现为一种状态机,与压缩有关的挑战性任务是保持所述压缩器和解压缩器状态(被称为上下文)彼此一致,同时将所述标题开销保持得尽可能低。

[0008] 显然,在把通过无线的IP上的话音(VoIP)(VoIPoW)作为对于电路交换话音的经济可行的替代中,标题压缩十分重要。用于这个目的的标题压缩解决方案已经被IETF的健壮标题压缩(ROHC)工作组开发。这些解决方案在2001年7月由Bormann等人的题为"RobustHeader Compression(健壮标题压缩)"的IETF RFC 3095的文件中被提出。所述ROHC RTP标题压缩方案已经被设计在一个任意的链路层上有效地压缩所述IP/UDP/RTP标题。除协商外,ROHC RTP压缩只要求由所述链路层提供成帧和误差检测,而诸如分组类型识别的所有其它的功能则由所述ROHC方案自己处理。

[0009] 最近的标题压缩中的工作还包括创立用于 IP/UDP/RTP 分组的 0 字节标题压缩方案。例如，这个类型的方案在2002年4月由Jonsson等编写的题为“A Link-Layer Assisted ROHC Profile for IP/UDP/RTP（用于 IP/UDP/RTP 的链路层辅助 ROHC 概括）”的 RFC 3242 的文件（下文中“LLA”）中被描述。这些方案使用由较低层提供的功能以便通过在正常操作期间为大多数分组完全消除标题来提高压缩效率。当它们中的一些信息可以通过由所述辅助层提供的功能推断时，这些无标题分组可以被发送。这个信息包括识别分组类型的标题字段。

[0010] 尽管现在无标题分组可以被诸如 LLA 的方案提供，但是在使用所述 ROHC 技术被压缩的所有标题中仍然需要分组类型标识符，因此需要一个最小的八位组标题尺寸。因此，在空中接口上没有明确地使用附加比特的情况下，提供分组类型识别成为问题，并且直到这个问题被解决，才不会阻碍 0 字节标题压缩方案的使用。为了完全消除所述标题，分组类型标识符必须通过其它装置被提供，当“自由”链路层比特不可用时并且当所述附加比特传输不可能时被使用。

发明内容

[0011] 本发明通过在其中分组标题已经通过压缩被完全消除因此压缩后的分组是无标题分组的设备中提供分组类型识别来克服了上面提出的现有技术的问题。更特别的，在本发明的实施方案中，在不需要在所述空中接口或其它传输链路上传输附加比特的情况下，通过使用由所述物理层提供的功能，分组类型识别被隐含地进行。根据本发明，建议了几个解决方案用于创立标题压缩方案，这些方案能够完全压缩完所述标题，当所述链路不能提供一个明确的分组类型标识符时有用。下文中详细描述每一个解决方案。

[0012] 可以预料，本发明的实施方案可以被有利地与上述分别被称作 [VJ]，[IPHC]，[CRTP] 和 [ROHC] 的标题压缩方案一起使用。此外，可以预料，通过把本发明的一个实施方案和诸如 [LLA] 的 0 字节标题压缩方案结合起来可以取得十分重要的优点。然而，本发明决不限于此。在此使用专业术语标题压缩、标题压缩器和标题解压缩器是用来强调本发明的宽范围。

[0013] 本发明的一个实施方案涉及一种隐式分组类型识别方法，该方法供一种被配置在传输链路上传输至少最初被提供标题的分组的系统来使用，其中所述系统包括分别在传输前压缩标题和在传输后解压缩标题的压缩器和解压缩器。所述方法包括建立和选择一组隐式分组传输特性的步骤，其中不同的特性识别不同类型的分组。所述压缩器被操作来压缩特殊分组的标题，所以所述特殊分组变成无标题的，所述特殊分组是被所述特性中的相应一个特性识别的一种类型的分组。所述特殊分组根据相应的传输特性被传输，并且所述解压缩器被操作来检测所述相应的特性并且由此识别所述特殊分组的分组类型。应该强调，本发明的实施方案可以被用于识别 N 个不同的分组类型，其中 N 是一个正整数。

[0014] 如在此被使用的，术语“隐式分组传输特性”指一种与通过一个链路从所述压缩器侧到所述解压缩器侧传输无标题和被压缩的标题分组有关的特性或机制，其中所述隐式特性可以为不同的分组类型而被改变并且不需要任何附加比特。

附图说明

[0015] 图 1 是说明根据本发明的一个实施方案的一种使用标题压缩和隐式分组识别的系统的示意图。

[0016] 图 2 是说明表示本发明的一个实施方案的传送信道设备的示意图。

[0017] 图 3-4 是共同表示本发明的另一个实施方案的与分组加密有关的示意图。

[0018] 典型实施方案的详细描述

[0019] 参考图 1，其中显示了系统 10，它在从移动单元 12 到网络实体 14 传输诸如话音或语音信息的信息中使用本发明的一个实施方案。在移动单元 12 被产生的语音数据根据惯例分组化所述数据，给各个分组提供标题并且传递所述分组到移动单元 12 的压缩器 18。压缩器 18 还按照在此被进一步描述的来压缩所述标题并且操作。压缩之后，分组同样按照在下文中被描述的在无线链路 20 上被传输到网络实体 14 的解压缩器 22 并且被处理。链路 20 有用地可以是一个双工链路，它具有以传统方式被从解压缩器 22 传输到压缩器 18 的反馈分组。这使所述压缩器和解压缩器能够在所述分组在链路 20 上被发送之前预先协商分组传输的特性或机制。然而，虽然双工链路通常使得事情变得简单并且诸如可以为标题压缩改进性能，但是链路 20 也可以是一个单工链路。即使所述数据传输是单工的，以双工方式执行协商仍是可能的，否则可以脱机进行协商。如在此被使用的，在所述压缩器和解压缩器之间协商或预先协商指一个传统过程，其中所述压缩器和解压缩器彼此来回地通信，以便关于将被在无标题分组和其它分组类型的传输和隐式识别中使用的特性和机制及其特定值而达成一致。

[0020] 图 1 还显示了一个对应的节点 24，它也可以是一个被链接到网络实体 14 的移动单元。对应的节点 24 通常未被直接连接到网络实体 14，而是通过节点网络被间接地连接。网络实体 14 被提供一个压缩器 25，移动单元 12 被提供一个相应的解压缩器 16。压缩器 25 和解压缩器 16 处理到移动单元 12 的输入业务量，也就是来自相应的通信节点 24 的输入业务量。

[0021] 在本发明的第一实施方案中，压缩器 18 和解压缩器 22 协商将被用于识别无标题分组的一个或几个特定的分组尺寸。因为 0 字节标题压缩，所以这是可能的，以便提供无标题分组，只在有某些特性的特定链路上是有用的，并且只对于适合所述链路特性的应用程序是有利的。所述特定分组尺寸之一应该是预期的最小尺寸。当一个分组被发送到所述压缩器时，所述压缩器决定使用哪个分组类型。如果所述分组的有效负荷有一个是被协商的分组尺寸之一的尺寸，并且所述分组不需要标题，则所述压缩器发送没有标题的所述分组。另外，包括一个隐式分组类型标识符的标题被附加到被发送的有效负荷。

[0022] 解压缩器 22 总是把任何特定的被预协商尺寸的分组作为没有标题的分组处理，并且利用上下文信息和链路同步来解压缩所述标题。如已知的，上下文信息是从在相同的分组流或流量中先前被发送的分组中接收的信息。如果被传输到所述解压缩器的分组不是所述特定尺寸之一，则所述分组作为具有包括分组类型标识符和其它被压缩的标题字段的被压缩的标题的普通分组被处理。

[0023] 在实现上述实施方案中，所述压缩器必须确保如果具有正常被压缩标题的分组的尺寸匹配无标题分组的任何特定的被预协商的尺寸，则填充字符必须被附加到所述分组，以便它的尺寸将不再匹配被预协商的尺寸。这对于在所述解压缩器侧避免任何模糊是必要

的。

[0024] 在本发明的第二实施方案中，多组信道编码组合被用于提供隐式分组类型识别。如本领域已知的，传送信道和传送格式组合是某些标准化可配置的物理层的特征。每个传送信道(TC)的特征是一个特定的信道编码方案，并且在所述物理层传送格式组合(TFC)是传送信道的组合并且当一个物理子信道建立时被定义。每个TFC可以被配置符合于一个分组格式以便在它的不同部分上应用不同的信道编码。使用这些定义并且假定一个物理层使用上述概念，不同的传送格式组合的组可以被预先识别并且被用于隐式分组类型识别。也就是说，一个特殊的TFC标识符值可以被用于指定一个被要求用于每个特殊分组类型传输的信道编码组合。

[0025] 参考图2，它显示了一个例子，其中传送信道基于代表信道编码要求的四个不同的可能类型的比特分类被配置。所述类型包括被压缩标题的八位组(CH八位组)和三个任意的比特类型(Cls A比特，Cls B比特以及Cls C比特)。这涉及在一个可配置的物理层上IP/UDP/RTP/AMR音频业务量信道编码要求。

[0026] 如果多个分组都要求同样的编码组合，则它们全部可以用相同的TFC标识符被识别，并且所述分组的不同部分在每个传送信道上被发送。这允许某些TFC标识符唯一地与一个特殊分组类型相联系。例如，还参考图2，具有被压缩的标题的分组共同地被表示为分组类型1，或PT1。因此，图2表示有标题的分组将使用TFC标识符值[000,001,010]。在图2中共同地被表示为PT2的无标题分组将使用TFC值[011,100]。

[0027] 上述可配置的物理层概念要求某些假定以便与用于VoIP的任何标题压缩器机制一起工作。更特别的，假定所述被要求的TFC已经被在所述物理层定义，一个信道被提供用于所述不同的被压缩的标题尺寸(包括用于最大预期的被压缩的标题尺寸的一个)，无标题分组要求的全部传送格式是可用的，以及所得到的有关的分组流量的TFC标识符组对于所述标题压缩层是可用的。此外，假定所述物理层给所述解压缩器提供所述TFC标识符以及所述被接收的分组。

[0028] 在用于所述第二实施方案的标题压缩设置中，所述压缩器识别一个或几个应当被用于无标题分组的TFC标识符。所述压缩器还与所述解压缩器关于这些标识符应当被用于所述无标题分组而达成一致意见。如上面描述的，所述压缩器确保所有被压缩的标题被使用TFC标识符传递到所述物理层。

[0029] 如在所述压缩器和所述解压缩器之间同意的，如果所述被接收的分组有一个被包括在被分配到无标题分组的标识符组中的TFC标识符，则所述解压缩器把被接收的分组作为无标题分组来对待。如果所述解压缩器承认被接收的是无标题分组，则它利用上下文信息和链路同步来解压缩所述标题。如果被接收分组的TFC标识符不在这个组内，则所述分组被作为具有包括一个分组类型标识符和其它标题字段的被压缩标题的普通分组来处理。应该注意，所述压缩器必须确保包括0字节尺寸标题的每个被压缩的标题正好匹配被定义的用于分组被为其传递的所述TFC标识符的被压缩标题信道的TFC。如果不是这种情况，则压缩器必须使用填充字符以便产生适合于将被用于所述相应的分组的TFC的被压缩的标题。定义适当的TFC组的职责属于所述物理层。

[0030] 所述隐式分组类型识别发明的第三实施方案通过使用由基础层提供的创立不同的逻辑信道的多路复用选项来区别不同的分组类型。例如，这个实施方案可以通过使用不

同的业务选项、不同的业务量类型或特定的 QoS 参数被实现。

[0031] 根据这个过程，所述压缩器使用来自较低层的可用的多路复用选项之一来创立两个逻辑信道。所述压缩器和解压缩器协商两个逻辑信道中的哪一个将被仅仅用于属于一个单独流量的无标题分组，并且协商哪个信道将被用于具有被压缩标题的分组。所述压缩器随后确定哪个分组类型用于特殊分组（有或没有标题）并且在适当的逻辑信道上发送所得到的分组到所述解压缩器。

[0032] 所述解压缩器总是把在被识别用于无标题分组的逻辑信道上接收的分组作为无标题分组来对待，并且利用上下文信息和链路同步来解压缩所述标题。否则，所述分组被作为一个具有包括分组类型标识符和其它标题字段的被压缩标题的普通分组来处理。

[0033] 本发明的另一个实施方案指向一种技术，该技术在所述物理层上使用一对加密密钥以便产生用于所述标题压缩层的分组类型标识符。在执行保证当使用一对不一样的密钥时被加密值的唯一性的加密操作之前，这种方法重新使用现有的物理层 CRC 值。因此这种方法在所述物理层上，在所述物理层 CRC 计算和所述物理层成帧操作之间操作。如本领域技术人员已知的，CRC 是循环冗余码的首字母缩写词，它是一类通过发现多项式除法的余数来产生奇偶检验比特的线性误差检测码。所述加密操作使用一种不应该促使分组尺寸扩展的加密算法。因此，一种可用的加密方法可以被使用，它使用不促使尺寸扩展的附加流密码和比特方式的异或操作。所述加密算法也不应该通过解密传播比特误差，这意味着解密之前和之后错误比特的数量相同。

[0034] 在这个实施方案中，一对加密密钥首先在所述物理链路的压缩器和解压缩器侧之间交换。因为预期在所述物理层另一个加密层将被使用，所以所述密钥交换不必被保密。在所述密钥交换之后，每个加密密钥被分配给不同的分组类型流量。例如，一个密钥可以被分配表示无标题分组，而另一个密钥可以表示具有被压缩的标题的普通分组。一个分组在所述链路的压缩器侧使用被分配给它的分组类型的密钥被加密。所述被加密的分组以及在所述未被加密的分组上被所述物理层以传统方式计算的 CRC 值通过所述链路被发送到所述解压缩器侧。一旦在所述解压缩器侧接收，则被接收的分组就对于每个密钥被解密并且一个 CRC 值在由所述 CRC 覆盖的普通数据上被计算，使用每个被解密的分组替代被接收的加密分组。每个被计算的 CRC 值符合于所述被交换密钥之一。它们之一将等于从所述链路压缩器侧接收的 CRC 值，从而识别符合于适当的逻辑信道的密钥，并且因此也识别所述被接收的分组的分组类型。

[0035] 图 3 和图 4 显示这个过程的一个例子，用于两个不同的分组类型。参考图 3，在物理链路 20 的压缩器侧，显示了一个无标题分组 26，或分组类型 1。在功能块 28，一个 CRC 值通常首先由所述物理层计算以便提供一个 CRC1 的 CRC 值，块 30。在成帧和传输之前，在功能块 32，所述分组 26 使用被分配给这个分组类型流量的密钥 (eKey1) 被加密以便提供被加密的分组 (ePacket)34。CRC1 和 ePacket 34 随后通过所述物理媒体 20 被发送到所述解压缩器侧。在功能块 36 和 38 上，在接收端分别用 eKey1 和 eKey2 对 ePacket 34 解密，从而产生最初未知类型的分组 40 和 42，(？分组 1) 和 (？分组 2)。随后为每个被解密的 40 和 42 计算 CRC 值，产生的 CRC 值 CRC1 和 CRC2 分别在 44 和 46 被显示。这些值随后被与被接收的 CRC 值比较，在块 30 被显示。在这种情况下，CRC 值 44(CRC1) 等于被接收的 CRC 值，因此识别所述分组类型为 PT1。

[0036] 参考图 4，显示了适用于诸如被压缩的标题分组（CH 分组）或分组类型 2 的不同分组类型的分组 48 的相同过程。一个 CRC 值在功能块 50 被计算以便提供一个 CRC2 的 CRC 值 52。使用被分配给 PT2 的密钥 (eKey2) 对于分组 48 进行加密以便提供加密分组 (ePacket)56。CRC2 和 ePacket 56 随后在链路 20 上被发送，在功能块 58 和 60，ePacket56 分别被用 eKey1 和 eKey2 解密。未知类型 62 和 64 的分组从所述解密被产生，并且分别被用于计算是 CRC1 的 CRC 值 66 以及是 CRC2 的 CRC 值 68。通过比较所述 CRC 值和所述被传输的 CRC 值 52，确定分组 48 是 PT2。

[0037] 图 3 和图 4 中表示的过程可以被简要地概括如下：

[0038] 1. 在所述标题压缩子层下，所述链路的两侧协商一对加密密钥以及一个加密算法的使用并且给每个密钥分配一个逻辑值。

[0039] 2. 所述压缩器随后决定使用哪个标题和分组类型并且发送使用符合于所述被选择的分组类型的密钥所得到的加密的分组。

[0040] 3. 在所述发送端时，所述 CRC 值根据惯例在通常的 CRC 覆盖范围上被计算。

[0041] 4. 将被传输的分组随后使用分配给它的分组类型进行加密。由此产生的被加密的值以及符合于所述未被加密的数据的 CRC 值随后在所述物理信道上被发送。

[0042] 5. 在接收端时，所述 CRC 值被提取，所述被接收的分组使用两个密钥被解密，并且随后一个 CRC 值在所述通常的 CRC 覆盖范围上通过每个被解密的值被计算。这产生两个新的值，CRC1 和 CRC2。被接收的 CRC 随后被与新的被计算的值 CRC1 和 CRC2 比较，并且匹配所述被接收值的值指示哪个加密密钥被使用，从而识别所述分组类型。

[0043] 6. 对于无标题 / 标题区别的情况，所述解压缩器总是把所述被接收的分组和被识别用于无标题分组的逻辑信道作为无标题分组来处理，并且利用上下文信息和链路同步来解压缩所述标题。否则，所述分组被作为具有一个含有分组类型标识符和其它标题字段的被压缩的标题的普通分组来处理。

[0044] 应该注意，也可以建议一对不同的 CRC 多项式，但是这种多项式不能保证对于任何日期，使用所述相同的数据但是不同的多项式的 CRC 计算时，总是只有一个唯一的值被产生。

[0045] 显然，按照上述示教，本发明的很多修改和变化是可能的。因此应该理解，在被公开的概念的范围内，本发明可以被以不同于已经被特别描述的方式实践。

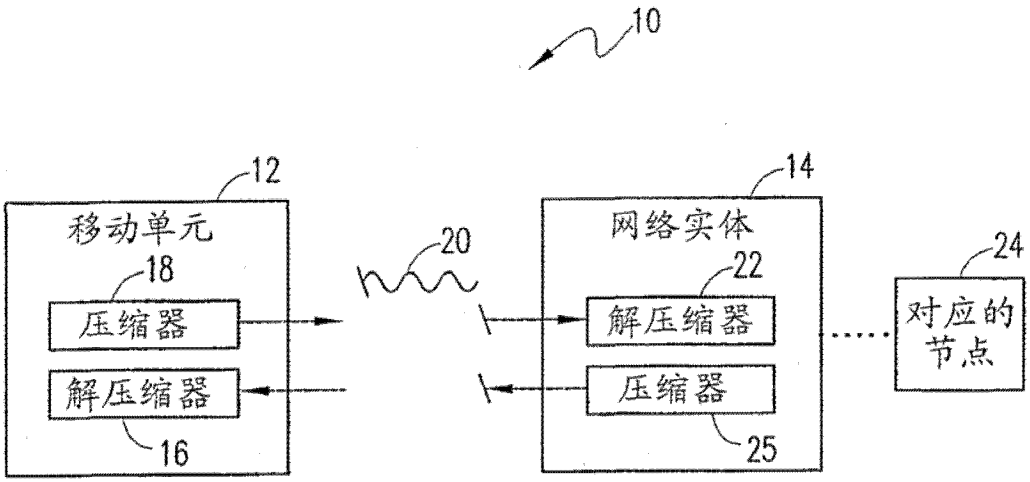

10
12
移动单元
18
压缩器
解压缩器
16
20
14
网络实体
22
解压缩器
压缩器
25
24
对应的节点

图 1

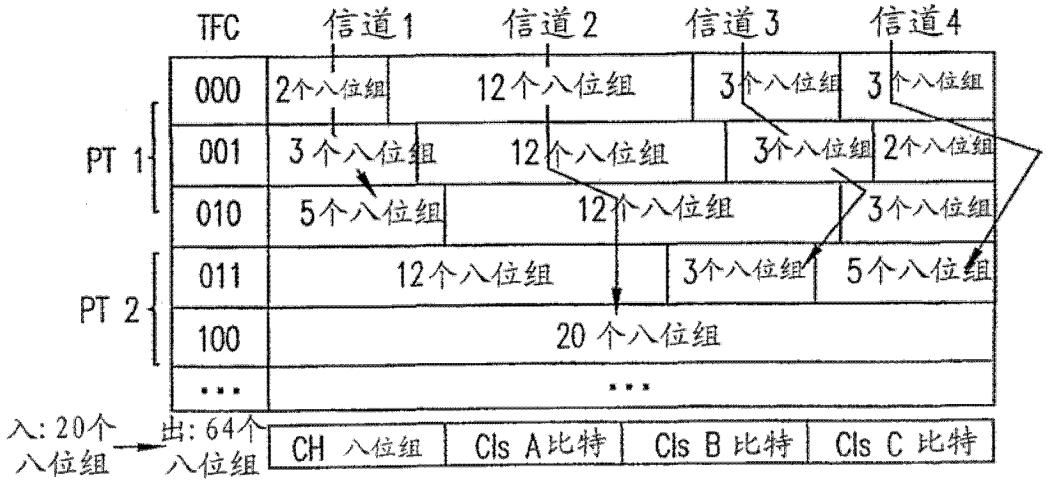

TFC
信道1
信道2
信道3
信道4
000
2个八位组
12个八位组
3个八位组
3个八位组
PT 1
001
3个八位组
12个八位组
3个八位组
2个八位组
010
5个八位组
12个八位组
3个八位组
PT 2
011
12个八位组
3个八位组
5个八位组
100
20个八位组
...
...
入: 20个八位组
出: 64个八位组
CH 八位组
Cls A比特
Cls B 比特
Cls C 比特

图 2

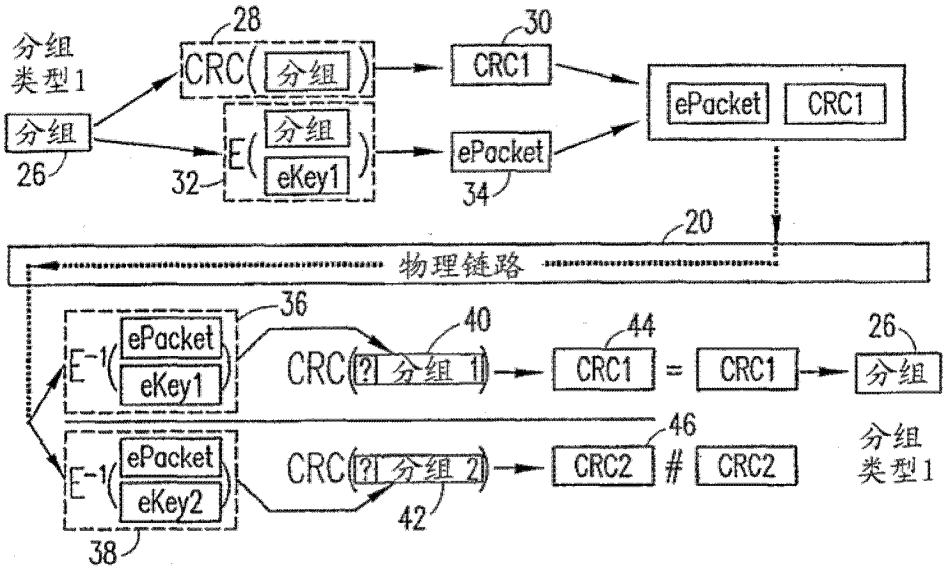

分组
类型1
分组
26
CRC(分组)
28
E(分组 eKey1)
32
CRC1
30
ePacket
34
ePacket CRC1
20
物理链路
E-1(ePacket eKey1)
36
CRC(?| 分组 1)
40
CRC1 = CRC1
44
26
分组
E-1(ePacket eKey2)
38
CRC(?| 分组 2)
42
CRC2 # CRC2
46
分组
类型1

图 3

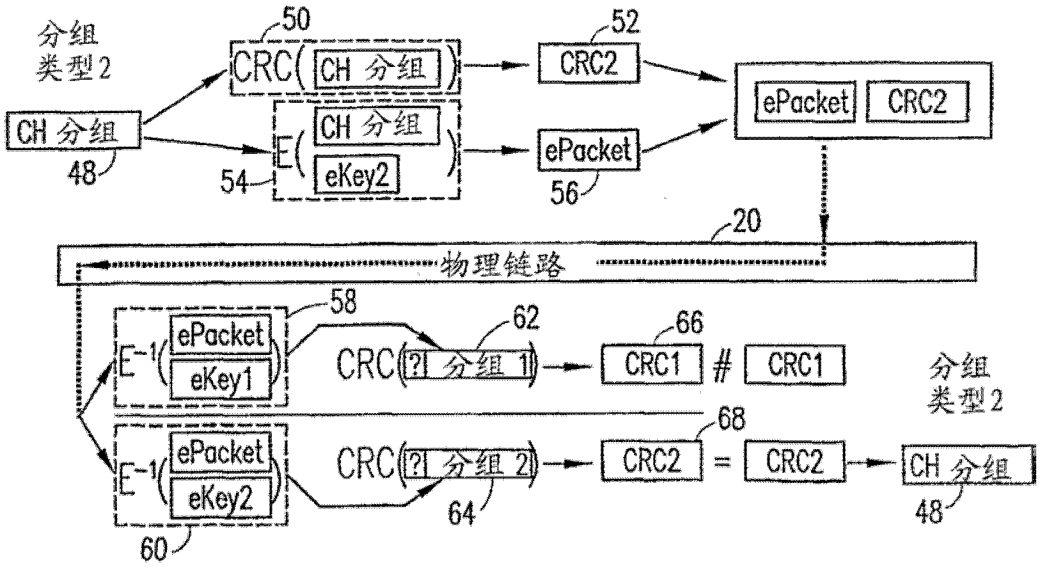

分组
类型2
CH 分组
48
CRC(CH 分组)
50
E(CH 分组 eKey2)
54
CRC2
52
ePacket
56
ePacket CRC2
20
物理链路
E-1(ePacket eKey1)
58
CRC(?| 分组 1)
62
CRC1 # CRC1
66
分组
类型2
E-1(ePacket eKey2)
60
CRC(?| 分组 2)
64
CRC2 = CRC2
68
CH 分组
48

图 4