



(12) 发明专利

(10) 授权公告号 CN 1778092 B

(45) 授权公告日 2010.05.12

(21) 申请号 200480010692.2

(22) 申请日 2004.04.23

(30) 优先权数据

03101150.5 2003.04.25 EP

(85) PCT申请进入国家阶段日

2005.10.21

(86) PCT申请的申请数据

PCT/IB2004/050500 2004.04.23

(87) PCT申请的公布数据

W02004/098155 EN 2004.11.11

(73) 专利权人 皇家飞利浦电子股份有限公司

地址 荷兰艾恩德霍芬

(72) 发明人 T·A·M·科维纳亚

F·L·A·J·坎佩曼

(74) 专利代理机构 中国专利代理(香港)有限公

司 72001

代理人 李亚非 刘杰

(51) Int. Cl.

H04L 29/08 (2006.01)

(56) 对比文件

US 5627829 A, 1997.05.06, 说明书第13栏
21-23行, 第12栏59页-第14栏45页, 第14栏
7-22行, 第16栏24-39行, 图7, 11, 12.

审查员 董振兴

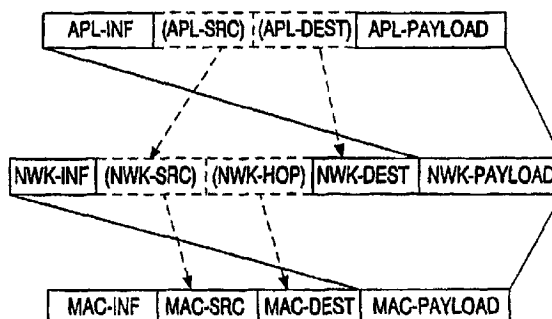
权利要求书 2 页 说明书 6 页 附图 7 页

(54) 发明名称

通信堆栈中的开销降低和地址保护

(57) 摘要

本发明减少了利用分层通信协议进行通信的寻址开销。本发明的改进保持了寻址信息的安全性。



1. 一种利用分层通信模型发送数据的发送方法,包括以下步骤:

在第一层上生成利用密码进行密码保护的第一通信段,该第一通信段包括密码和涉及第一实体的第一地址引用;

在第一层之下的第二层上生成第二通信段,该第二通信段基于第一通信段并进一步包括涉及与第一实体有关的第二实体的第二地址引用;

发送包括第二通信段的数据;

其特征在于:

该发送方法还包括以下步骤:

在已发送数据中至少部分地除去第一地址引用,以及其中在至少部分地除去第一地址引用之前,为第一通信段提供密码保护,并且将所述密码作为已发送数据的一部分发送。

2. 根据权利要求1所述的发送方法,其中仅仅在通信模型中在单个层上提供密码保护。

3. 根据权利要求2所述的发送方法,其中单个层等同于发起消息的层。

4. 根据权利要求1所述的发送方法,其中利用涉及第二地址引用的信息字段来代替第一地址引用。

5. 一种利用分层通信模型接收数据的接收方法,包括以下步骤:

接收包括第二通信段的数据,该第二通信段包括涉及与第一实体有关的第二实体的第二地址引用,并基于利用密码进行密码保护的第一通信段,该第一通信段包括所述密码和涉及第一实体的第一地址引用;和

从第二通信段中检索第一通信段;

其特征在于:

在已接收数据中至少部分地省去第一地址引用,

所述密码是作为已接收数据的一部分接收的,以及

该接收方法还包括在检索第一通信段时恢复第一地址引用的步骤,以及其中在恢复第一地址引用之后,验证第一通信段的密码保护。

6. 根据权利要求5所述的接收方法,其中仅仅在通信模型中在单个层上提供密码保护。

7. 根据权利要求6所述的接收方法,其中单个层等同于发起消息的层。

8. 根据权利要求5所述的接收方法,其中该接收方法利用已接收数据中的信息字段来检索第一地址引用,其中已接收数据中的信息字段替代第一地址引用并涉及第二地址引用。

9. 一种利用分层通信模型进行通信的系统,该系统包括:

发送机装置,其被安排成在第一层上生成利用密码进行密码保护的第一通信段,该第一通信段包括密码和涉及第一实体的第一地址引用,以及该发送机装置进一步被安排成在第一层之下的第二层上生成第二通信段,该第二通信段基于第一通信段并进一步包括涉及与第一实体有关的第二实体的第二地址引用;

通信装置,其被安排成发送包括第二通信段的数据;以及

接收装置,其被安排成接收包括第二通信段的数据,以及进一步被安排成从第二通信段中检索第一通信段;

其特征在于：

该发送机装置被安排成从已发送数据中至少部分地省去第一地址引用，被安排成将所述密码作为已发送数据的一部分发送，以及被安排成在至少部分地省去第一地址引用之前为第一通信段提供密码保护；和

该接收装置被安排成在从已接收数据中检索第一通信段时恢复第一地址引用，以及被安排成在恢复第一地址引用之后验证第一通信段的密码保护。

10. 一种利用分层通信模型发送数据的发送机装置，该发送机装置包括：

第一装置，其被安排成在第一层上生成利用密码进行密码保护的第一通信段，该第一通信段包括所述密码和涉及第一实体的第一地址引用，

第二装置，其被安排成在第一层之下的第二层上生成第二通信段，该第二通信段基于第一通信段并进一步包括涉及与第一实体有关的第二实体的第二地址引用，以及

第三装置，其被安排成发送包括第二通信段的数据，

其特征在于：

在已发送数据中至少部分地除去第一地址引用，将所述密码作为已发送数据的一部分发送，以及在至少部分地省去第一地址引用之前为第一通信段提供密码保护。

11. 一种利用分层通信模型接收数据的接收机装置，包括：

第一装置，其被安排成接收包括第二通信段的数据，该第二通信段包括涉及与第一实体有关的第二实体的第二地址引用，并基于利用密码进行密码保护的第一通信段，该第一通信段包括所述密码涉及第一实体的第一地址引用；以及

第二装置，其被安排成从第二通信段中检索第一通信段，

其特征在于：

在已接收数据中至少部分地省去第一地址引用，

所述密码是作为已接收数据的一部分接收的，以及

在检索第一通信段时恢复第一地址引用，以及在恢复第一地址引用之后验证第一通信段的密码保护。

通信堆栈中的开销降低和地址保护

技术领域

[0001] 本发明涉及一种利用分层通信模型发送数据的发送方法,包括以下步骤:在第一层生成包括涉及第一实体的第一地址引用(reference)的第一密码保护的通信段(fragment);在第一层之下的第二层生成第二通信段,该第二通信段是基于第一通信段并进一步包括涉及与第一实体有关的第二实体的第二地址引用;以及发送包括第二通信段的数据。

[0002] 本发明还涉及一种利用分层通信模型接收数据的接收方法,包括以下步骤:接收包括第二通信段的数据,该第二通信段包括涉及与第一实体有关的第二实体的第二地址引用,并基于包括涉及第一实体的第一地址引用的第一密码保护的通信段;以及从第二通信段中检索第一通信段。

[0003] 本发明还涉及一种利用分层通信模型进行通信的系统,该系统包括:发送机装置,其被安排成在第一层生成包括涉及第一实体的第一地址引用的第一密码保护的通信段,并进一步被安排成在第一层之下的第二层生成第二通信段,该第二通信段是基于第一通信段并进一步包括涉及与第一实体有关的第二实体的第二地址引用;通信装置,其被安排成发送包括第二通信段的数据;以及接收装置,其被安排成接收包括第二通信段的数据,并进一步被安排成从第二通信段中检索第一通信段。

[0004] 本发明还涉及一种利用分层通信模型发送数据的发送机装置,该发送机装置被安排成在第一层生成包括涉及第一实体的第一地址引用的第一密码保护的通信段;进一步被安排成在第一层之下的第二层生成第二通信段,该第二通信段是基于第一通信段并进一步包括涉及与第一实体有关的第二实体的第二地址引用;以及进一步被安排成发送包括第二通信段的数据。

[0005] 本发明还涉及一种利用分层通信模型接收数据的接收机装置,该接收机装置被安排成接收包括第二通信段的数据,该第二通信段包括涉及与第一实体有关的第二实体的第二地址引用,并基于包括涉及第一实体的第一地址引用的第一密码保护的通信段;以及进一步被安排成从第二通信段中检索第一通信段。

[0006] 本发明进一步涉及一种用于携带根据分层通信模型生成的数据的信号,所述数据是根据包括第一层和位于第一层之下的第二层的分层通信模型生成的,其中在第一层生成包括涉及第一实体的第一地址引用的第一密码保护的通信段,在第二层生成第二通信段,该第二通信段包括涉及与第一实体有关的第二实体的第二地址引用并且是基于第一通信段的。

[0007] 本发明还涉及一种利用分层通信模型实施通信的发送机计算机程序产品,该发送机计算机程序产品被安排成在第一层生成包括涉及第一实体的第一地址引用的第一密码保护的通信段;进一步被安排成在第一层之下的第二层生成第二通信段,该第二通信段是基于第一通信段并进一步包括涉及与第一实体有关的第二实体的第二地址引用;以及进一步被安排成发送包括第二通信段的数据。

[0008] 本发明还涉及一种利用分层通信模型实施通信的接收机计算机程序产品,该接收

机计算机程序产品被安排成接收包括第二通信段的数据,该第二通信段包括涉及与第一实体有关的第二实体的第二地址引用,并基于包括涉及第一实体的第一地址引用的第一密码保护的通信段;以及进一步被安排成从第二通信段中检索第一通信段,其中在第一层生成包括涉及第一实体的第一地址引用的第一通信段,以及在第一层之下的第二层生成第二通信段,该第二通信段包括涉及与第一实体有关的第二实体的第二地址引用并且是基于第一通信段的。

背景技术

[0009] 在通信协议中,通常使用诸如 OSI 参考模型之类的分层模型。这样的模型包括一组层,每层位于不同的抽象层上。这样的模型从底到顶可以包括:物理层 (PHY)、媒体接入控制层 (MAC)、网络层 (NWK) 以及应用层 (APL)。通常,一帧(在不同装置上的相同 OSI 层之间交换的信息段)由报头和净荷 (payload) 组成。在 OSI 堆栈中层 n 上的一个或多个帧作为下一个较低层 n-1 上的一个或几个帧的净荷来通过物理方式发送。最低层经由例如有线或无线连接来实施物理通信。在通常设置中,单个装置可能在 OSI 堆栈的不同层上具有不同的地址。不同层上的帧通常分别包括源地址、目的地址,有时还有跳地址 (hopaddress)。这由于包括多个地址信息而导致在最低层上发送的物理帧中的大量开销。这在诸如具有有限物理帧长度的通信协议之类的受约束应用中或在低功率应用中呈现过多开销的问题。

发明内容

[0010] 本发明的目的是提供一种发送方法,在该方法中,在基本保持所含信息及其密码保护的同时,降低物理帧的大小。

[0011] 该目的是通过根据本发明的发送方法来实现的,该方法的特征在于,该发送方法还包括至少部分地消除已传送数据中的第一地址引用的步骤,以及其中在至少部分地消除第一地址引用之前,为第一通信段提供密码保护。

[0012] 该方法提出第一地址引用被省去的第一通信段的保护。需要密码保护其帧的某一层可以生成用于每帧的消息完整性代码 (MIC)。通过利用例如 CBC-MAC 模式的分组密码 (参见 Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone, Handbook of Applied Cryptography, p353) 可以生成任意字符串上的 MIC。在帧保护的情况下, CBC-MAC 的输入将是待保护的帧,可能加有指示帧长度的数字前缀。在发送帧之前,将确定后的 MIC 添加到该帧的净荷上。

[0013] 在一些(受约束的)实施中,较低层假定由较高层发起的消息还受到该较高层的密码保护,因此较低层将不对该消息进行任何加密操作。利用基于范例 (paradigm) “发起消息的层负责密码保护”的该方法,密码开销被降低到每个物理消息最多一个 MIC。但这意味着,在上述实例中,较高层不能依赖较低层对已在较高层中省去且仅仅出现在较低层中的地址引用进行密码保护。

[0014] 在该实施例中,通过在省去第一地址引用之前计算 MIC 来提供第一地址引用的密码保护。由于复制的信息在较高层中不再可用,因此该信息仍然被包含在 MIC 中并因此得到保护。因此该实施例具有维持密码保护以包含已经省去的地址引用的优点。

[0015] 描述了根据本发明的方法的一个实施例。该实施例具有的优点是,仅仅在通信层

的一个层上添加密码保护,从而降低了开销。

[0016] 描述了根据本发明的方法的一个实施例。该实施例具有如下优点:在其中每个消息通常短得足以适应一帧(即在每个层上的消息比最大允许净荷小)的一个应用中,通过在可能是发起层的最高层上执行操作来使得添加 MIC 的开销最小化。

[0017] 描述了根据本发明的方法的一个实施例。将要省去的复制信息由指示在哪里可以找到该省去数据的较短字段来代替。

[0018] 本发明的另一个目的是提供一种接收方法,其中在基本维持所包含信息及其密码保护的同时,减小物理帧的大小。

[0019] 该目的是通过根据本发明的接收方法来实现的,该方法的特征在于,在接收数据中至少部分地省去第一地址引用,以及该接收方法进一步包括在检索第一通信段时恢复第一地址引用的步骤,以及其中在检索第一地址引用之后,验证第一通信段的密码保护。

[0020] 描述了根据本发明的接收方法的另外的实施例。这些实施例是对上述实施例的补充。

[0021] 根据本发明的系统的特征在于,发送机装置被安排成从已发送数据中至少部分地省去第一地址引用,以及接收装置被安排成在从已接收数据检索第一通信段时恢复第一地址引用。

[0022] 根据本发明的发送机装置的特征在于,发送机装置还被安排成至少部分消除已发送数据中的第一地址引用。

[0023] 根据本发明的接收机装置的特征在于,至少在已接收数据中部分地省去第一地址引用,并且接收机装置还被安排成在检索第一通信段时恢复第一地址引用。

[0024] 根据本发明的信号的特征在于,该信号携带在其中至少部分省去第一地址引用的第二通信段。

[0025] 根据本发明的发送机计算机程序产品的特征在于,发送机计算机程序产品还被安排成在已发送数据中省去第一地址引用。

[0026] 根据本发明的接收机计算机程序产品的特征在于,至少在已接收数据中部分省去第一地址引用,并且接收机计算机程序产品还被安排成在检索第一通信段时恢复第一地址引用。

附图说明

[0027] 下面将通过实例并参考附图来进一步描述本发明的这些和其它方面,其中:

[0028] 图 1 说明一种示例分层通信模型,

[0029] 图 2 显示 NWK 帧和 MAC 帧之间的关系,

[0030] 图 3 显示利用 MIC 的帧保护,

[0031] 图 4 显示只在起始层上的保护,

[0032] 图 5 显示在帧生成期间计算 MIC 并省去已复制数据的过程,

[0033] 图 6 显示多跳设置中的通信,

[0034] 图 7 显示利用本发明的相同通信,

[0035] 图 8 显示利用本发明的相同多跳通信的其它实施例,

[0036] 图 9 显示本发明的递归 (recursive) 实施例,以及

[0037] 图 10 显示在较高层利用子寻址的本发明的实施例。

具体实施方式

[0038] 在所有附图中,相同的参考数字指示相似或相应的特征。附图中指示的一些特征通常用软件实现,因而代表诸如软件模块或对象之类的软件实体。

[0039] 本发明第一实施例将由图 1 中所示的例子来说明。图 1 显示分层通信模型 100 的一个实例,该分层通信模型 100 包括物理层 (PHY) 101、媒体接入控制层 (MAC) 102、网络层 (NWK) 103 和应用层 (APL) 104。实际的通信 105 发生在最低层。实际上,可以使用比这里所示的层更多的层。可以使用不同的通信信道,包括利用光、电和无线技术。

[0040] 图 2 显示了在多跳设置中,在 OSI 堆栈中相邻层上的两个帧 (即 NWK 帧和 MAC 帧) 之间关系的实例。多跳网络中的消息,例如在 NWK 层始发的消息在达到其目的地之前可以被一个或多个中间装置中继。中间装置将应用某一路由算法,以便确定消息随后应发送到哪个装置。下一个中间装置的地址由 NWK-HOP 地址指示,接收装置使用该 NWK-HOP 地址确定它们是否为下一跳以及是否应当向前发送该消息。

[0041] NWK 帧报头包含信息字段 (NWK-INF) 201,该信息字段提供关于例如帧的其余部分的内容的信息。还存在发起消息的装置 (NWK-SRC) 204、它的最终目的地 (NWK-DEST) 202 和净荷 (NWK-PAYLOAD) 205。在多跳设置中,它还将包含下一跳 203 的 NWK 地址 (NWK-HOP),以便接收装置能够确定它应当处理该帧还是丢弃该帧。MAC 层将被用来把 NWK 帧作为净荷 (MAC-PAYLOAD 214) 从当前装置发送到下一跳,因此 MAC 层包含当前装置的 MAC 地址 (MAC-SRC) 213 和下一跳的 MAC 地址 (MAC-DEST) 212。在许多情况下,项 MAC-DEST 和 NWK-HOP 将涉及相同的物理装置,即寻址信息被发送两次。在常规应用中,涉及同一装置的不同层的地址在单个物理帧中出现若干次。在本发明中,从 NWK 帧中省去已复制地址 (在该实例中 :NWK-HOP) 的项,并且 NWK 层依赖 MAC 层中的相应项 (MAC-DEST)。

[0042] 如果一个层直接或者通过像地址查找表一样的某一可逆映射来发起消息或者生成包含将在较低层中复制的信息 (比如地址) 的帧,则较高层将省去已复制的信息,并在一个字段 (例如 NWK-INF 字段) 中指示哪些信息被省去,以及可选地指示可从哪里检索到它。如何指示这些的一个简单实施例是定义一些指示某个项是否被省去的比特。参考图 2,并假定在 NWK 层有时可能省去 NWK-DEST 202、NWK-HOP 203 和 NWK-SRC 204,则 NWK-INF 201 字段将包含三个比特,每个比特涉及多个地址项中的一个,其指示哪个地址项存在 (或被省去)。附加比特或隐含规则可用来确定较低层中的哪些字段将被使用。发起层将在接收端读取 NWK-INF 字段中的比特,并直接或者利用可逆映射 (在许多情况下,这将采取查找表的形式) 从较低层中得到所省去的地址。

[0043] 作为选择,不是省去字段,而是可以用一个较短字段来代替该字段。于是该较短字段将包含某类指针或参考指示符,它们将提供可在哪里找到已省去信息的信息。此外,将可能使用例如 NWK-INF 字段中的比特来指示一个字段是否已被替代。

[0044] 作为选择,不是把比特字段添加到 NWK-INF 字段上,而是可以使用指示已省去字段被短字段替代的不同技术。如果未完全使用例如已省去字段的有效值范围,而开始于特定前缀的保留范围是可用的,则该特定前缀可以用来指示该字段已经被替代。假设将要省去的字段是右边的,并且具有 0x00000000-0xffffffff 的有效值范围,则前缀 0xf... 可以

用来指示该字段已经被例如只有 2 字节的较短字段替代。于是该字段的值应与该前缀一致,从而被限制到范围 0xf000-0xffff。

[0045] 该思想在消息的物理帧大小受到限制的应用中特别有利。这种应用的典型例子是低成本和 / 或低功率无线连接装置的系统,其中所述无线连接装置例如是传感器、家庭安全、楼宇自动化、遥测、玩具、鼠标、键盘等。如果不同 OSI 层上使用的地址相同,在这种情况下,地址之间不必进行变换,则该方法甚至更为有利。

[0046] 在本发明的第二实施例中,对于已经省去的地址保持密码保护。

[0047] 图 3 示出了诸如 NWK 层之类的某一层想要通过对于包括地址信息的每帧生成消息完整性代码 (MIC) 来密码保护其帧的情况。在此情况中, NWK-MIC 306 保护整个 NWK 帧 301...305,而 MAC-MIC 315 保护包括 NWK 帧的整个 MAC 帧 311...314。

[0048] 在一个示例系统中,MAC 帧的典型最大长度可以是 102 字节,并且 MIC 的尺寸可被定义为 4、8 或 16 字节。假定消息通常适合于单个帧,如果在 OSI 堆栈的每层上存在 MIC,则在一帧中将存在 12 至 48 个 MIC 字节,从而导致大约 10-50% 的开销。

[0049] 在一些 (受约束的) 实施中,较低层假定由较高层发起的消息还受到较高层的密码保护,以便降低诸如发送附加 MIC 之类的密码开销。

[0050] 使用该基于范例“发起消息的层负责密码保护”的方法,对于从 NWK 层发起的消息,如图 4 所示每消息将最多有一个 MIC。但这意味着在上述例子中, NWK 层不能依赖 MAC 层来密码保护 NWK-HOP 403 (或 MAC-DEST 412)。

[0051] 然而,受保护信息应该包括在传递期间将被省去的已复制信息。

[0052] 如果发起消息的层仍然需要利用 MIC 来保护已复制信息,则它生成在包括已复制信息的所有相关信息上的 MIC。在计算 MIC 之后,已复制信息从该帧中被消除,并通过可逆映射 (例如查找表) 转换为较低层上的相应信息。当收到该帧时,检索来自较低层的适当信息,并通过使用可逆映射将该适当信息转换成发起层上的适当信息。该信息在适当位置上被插入到帧中,之后核实 MIC。

[0053] 如图 5 所示,在过程步骤 550 中, NWK 层将计算包括 NWK-HOP 的整个帧 501...505 上的 MIC。接着,在过程步骤 551 中,从帧中消除 NWK-HOP (如由叉号 507 表示的),并将该 NWK-HOP 发送给 MAC 层,以用作或者转换为 MAC-DEST。接收装置的 NWK 层把 MAC-DEST 转换成 NWK-HOP,并在检验 NWK-MIC 之前把 NWK-HOP 插入该帧中。

[0054] 如果不但省去地址信息而且还用其它信息来替代地址信息,则如上文所述,通过使已省去信息和替代信息上具有 MIC,也可以可选地保护该其他信息。

[0055] 该实施例具有保持已省去信息的密码保护的附加优点。

[0056] 图 6 显示在根据传统通信方式的多跳设置中从 M1 650 经由 M2 651 到 M3 652 的消息。

[0057] 图 7 显示在本发明的实施例的多跳设置中从 M1 650 经由 M2 651 到 M3 652 的消息。图 7 显示了 NWK-HOP 是通过参考 MAC-DEST 省去的。虚线和叉号 711...712 指示该字段实际上被省去,以便减小帧长。该实施例另外的优点是: NWK 帧不改变在跳之间的后续通信,因而更有可能减少节点中的处理开销。

[0058] 图 8 描述在帧长减小方面实现附加节省的一个实施例。在第一和最后的通信中,字段 NWK-SRC 和 NWK-DEST 也分别被省去。以稍微不规则处理为代价,得到通信规模的进一

步减小。

[0059] 在一个不同的实施例中,本发明被递归地应用。图 9 显示了应用层中的字段可如何参考网络层中的字段,同时这些字段也可能被省去,因为它们参考较低层上的字段。

[0060] 在另一个实施例中,在每个层上寻址是不相同的。我们示出了一个例子,其中 NWK 层使用装置的地址,但是 APL 层例如通过把 5 个比特附加到装置地址 1001、1003 上来对这些装置内的应用寻址。这些比特指定了被寻址装置内的 32 个应用之一。在该实施例中,APL 层上的地址不能完全被省去,因为这 5 个比特在较低层上是不可用的。在较低层上仅仅复制字段 1001、1003 的前缀。因此如图 10 所示,不是省去字段 1010、1011,而是用较短字段 1002、1004 来替代字段 1010、1011。

[0061] 替代是可能的。在以上的描述中,“包括”不排除其他元件或步骤,“一种”或“一个”不排除多个,并且单个处理器或其他单元也可以实现权利要求所述的若干装置的功能。实际通信包括利用光、电、无线、微波或任何其他合适技术在不同装置或装置的部分之间进行的实际通信,或者甚至包括处理系统内的软件部件之间或者处理系统之间的通信。

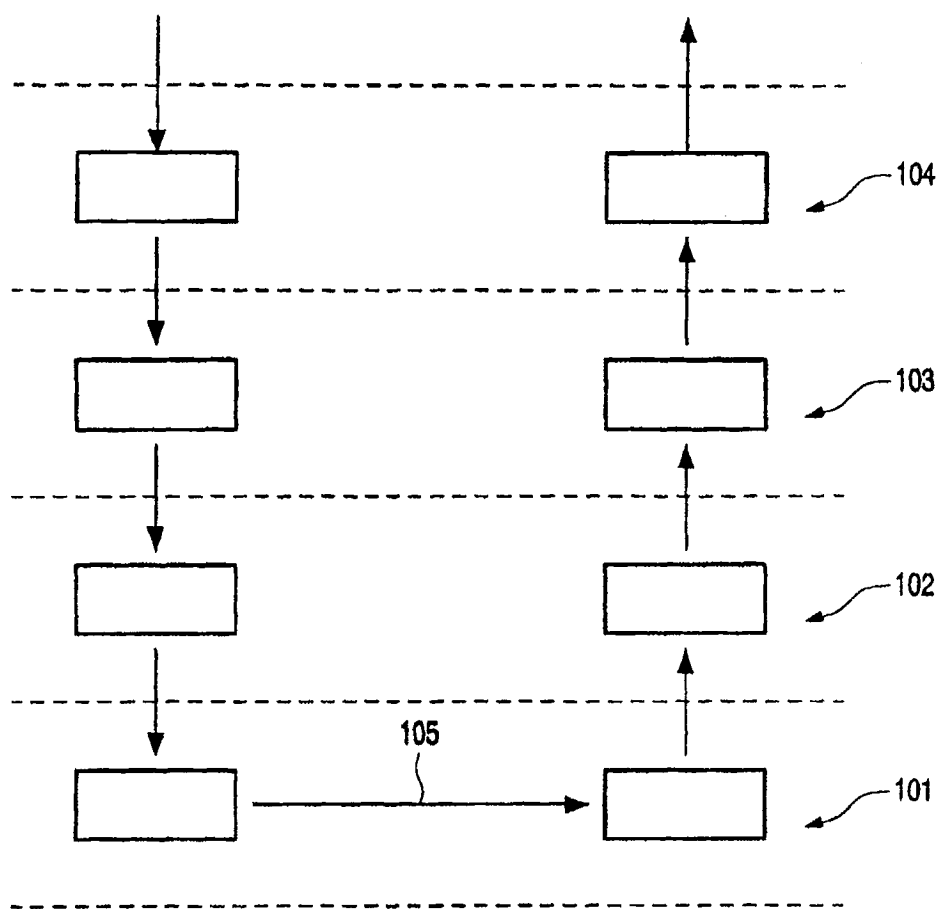
100

图 1

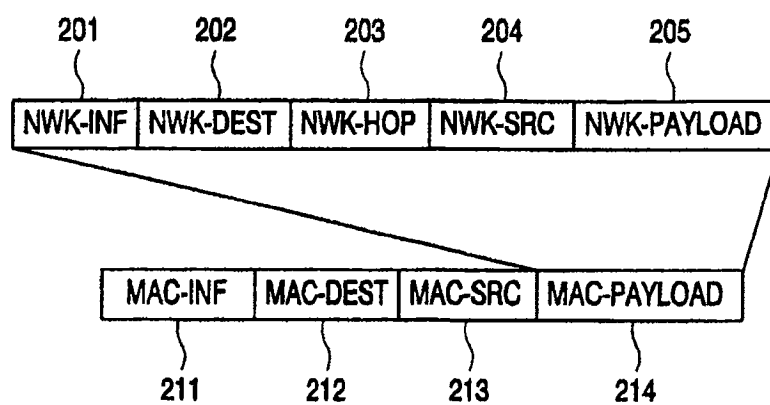


图 2

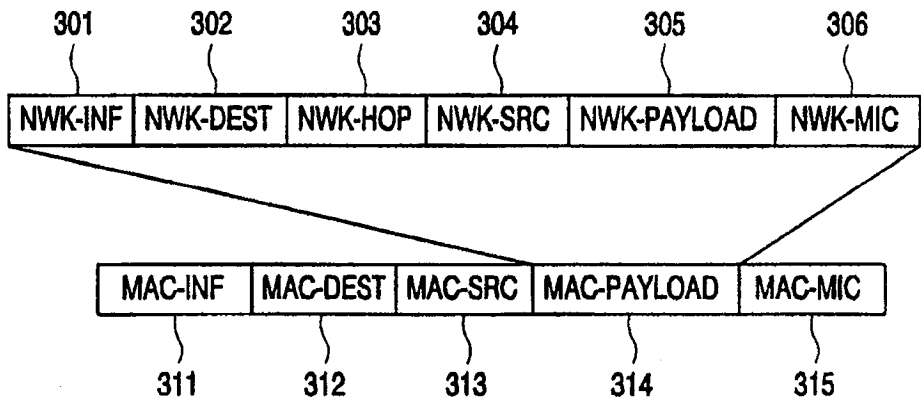


图 3

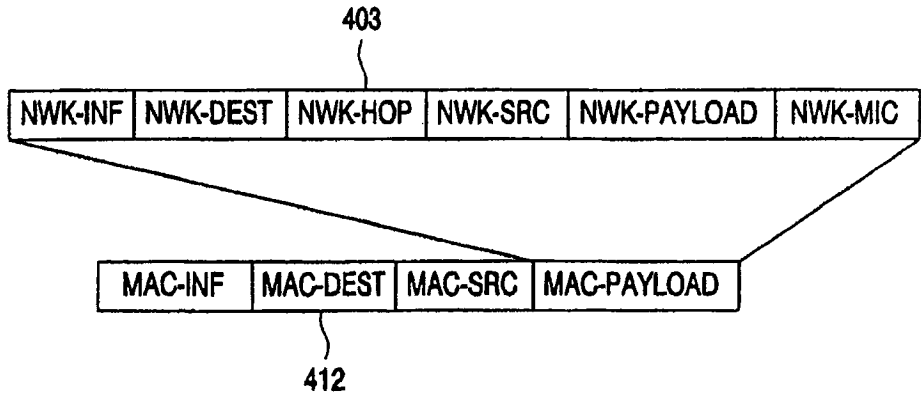


图 4

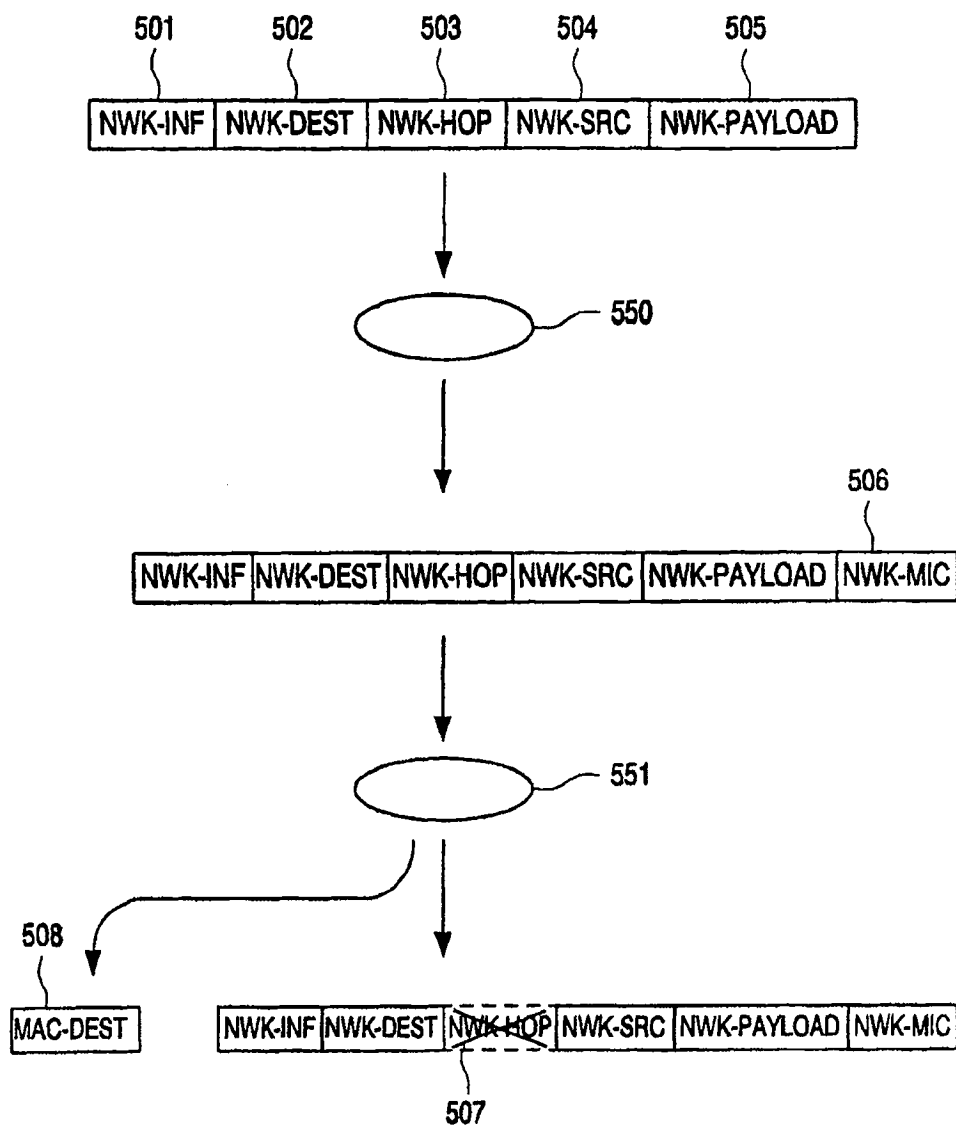


图 5

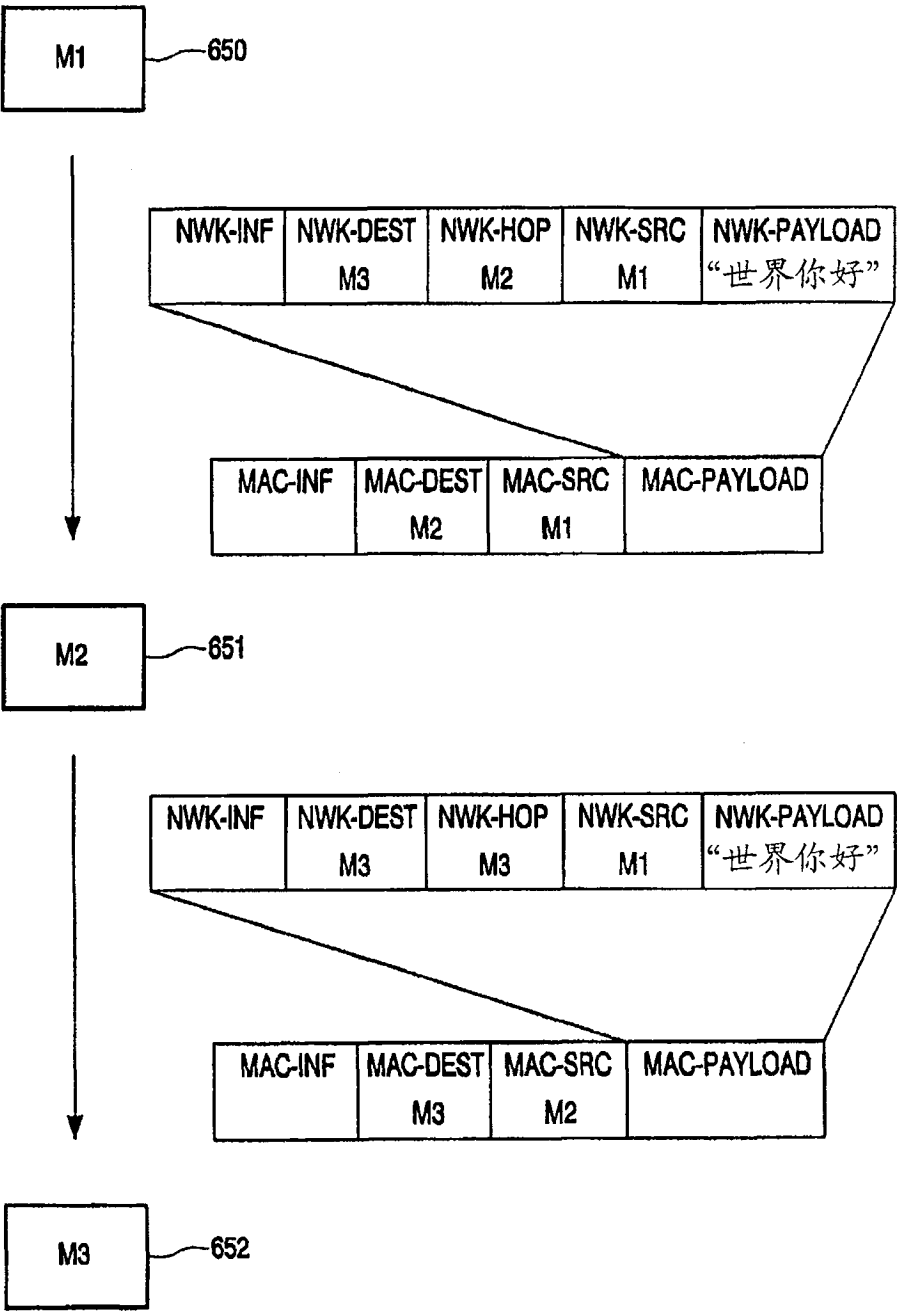


图 6

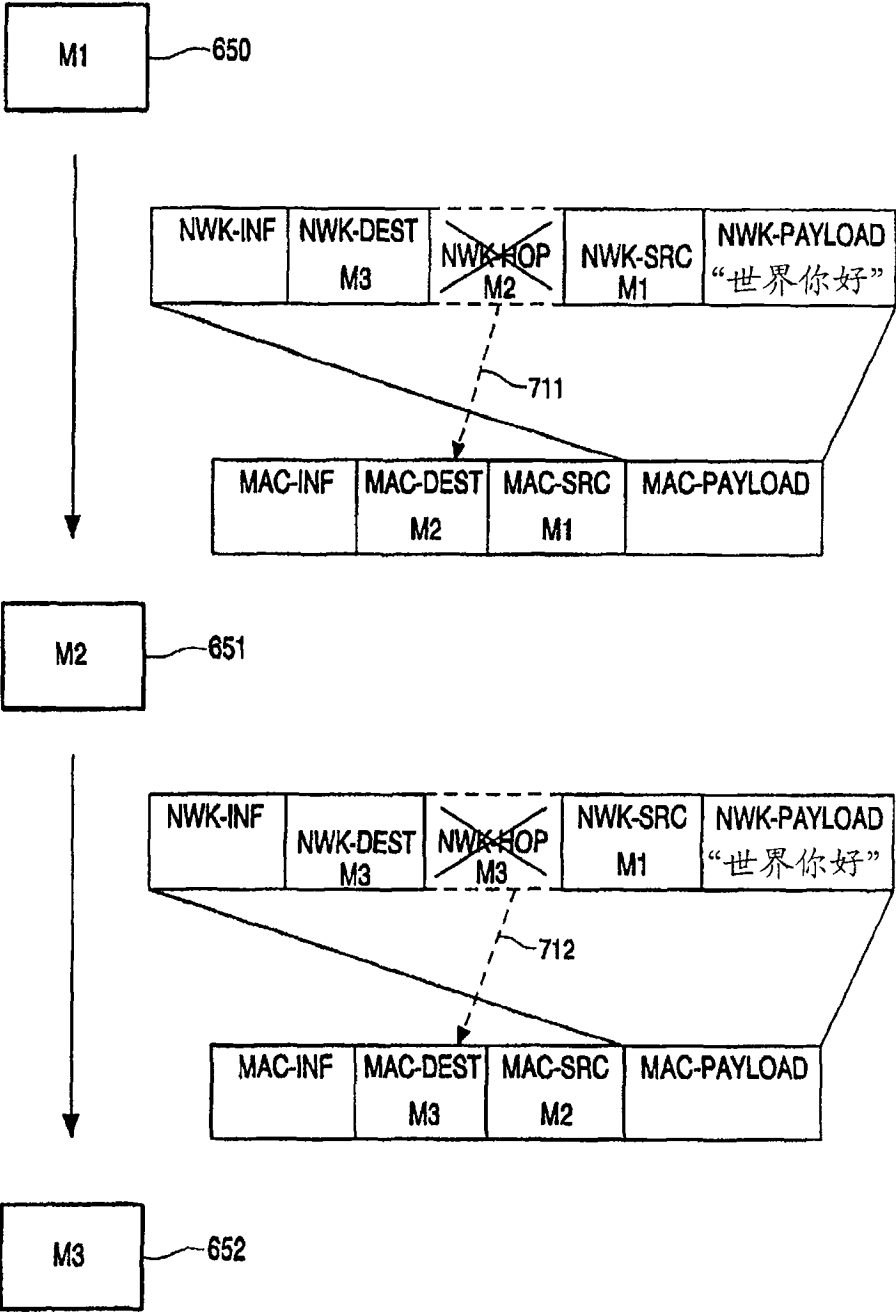


图 7

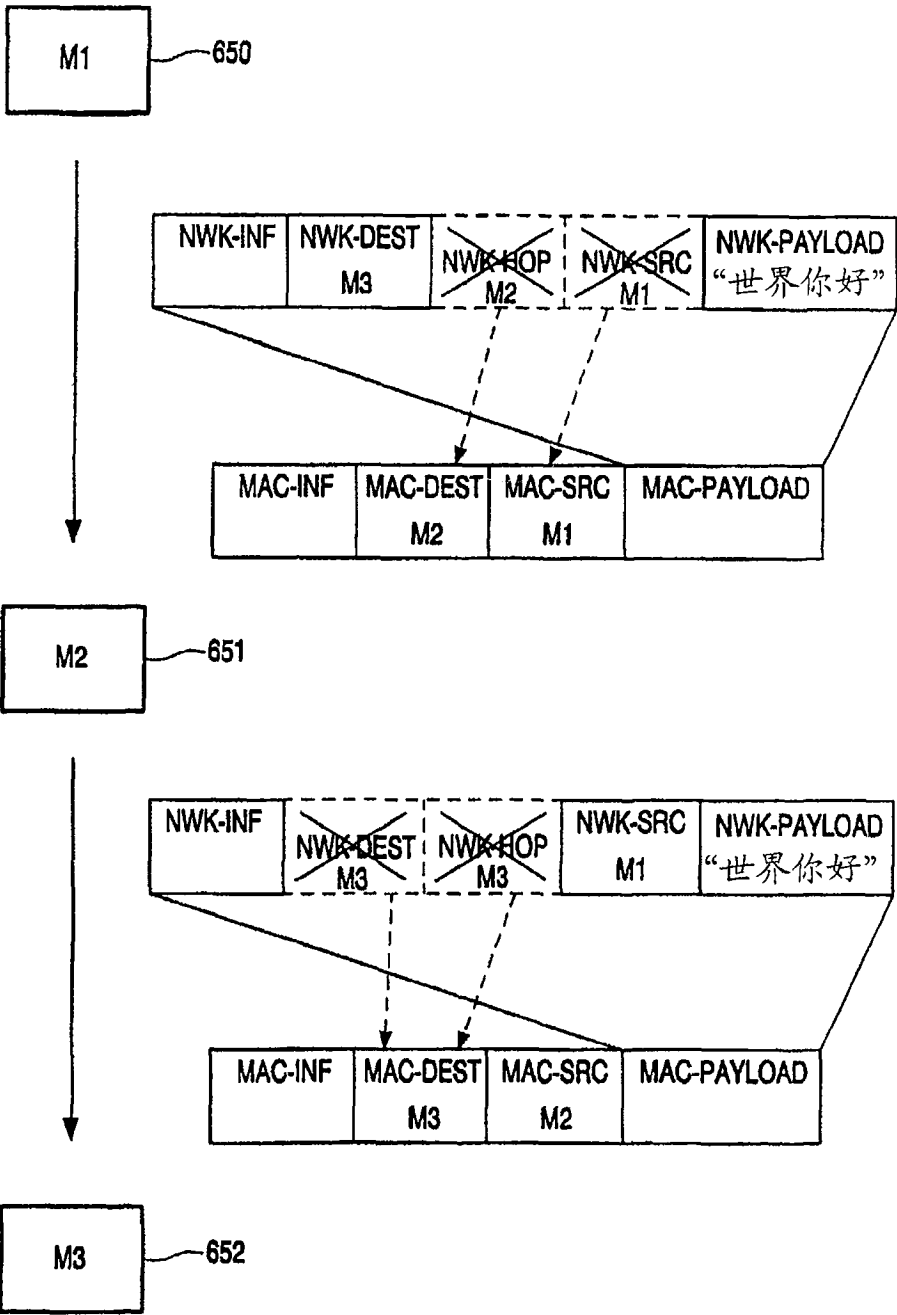


图 8

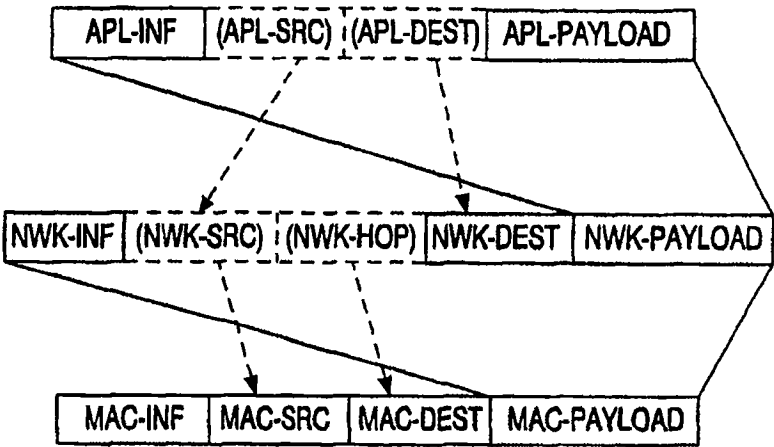


图 9

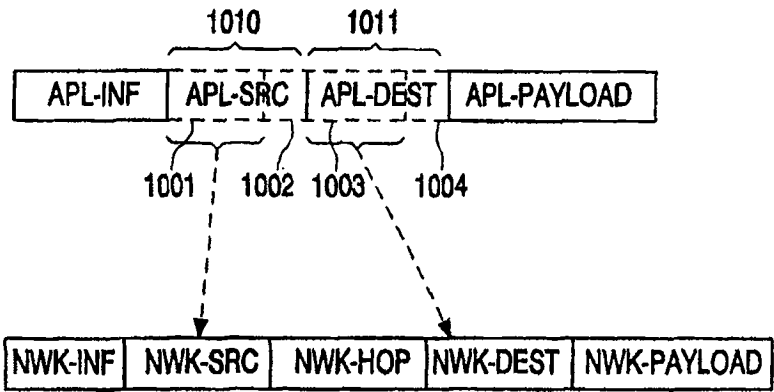


图 10