[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04L 9/00 (2006.01)
H04L 12/54 (2006.01)
H04L 9/30 (2006.01)
H04L 9/32 (2006.01)

[12] 发明专利申请公布说明书

[21] 申请号 200780020042.X

[43] 公开日 2009 年 7 月 29 日

[11] 公开号 CN 101496338A

[22] 申请日 2007.4.13

[21] 申请号 200780020042.X

[30] 优先权

[32] 2006.4.13 [33] US [31] 60/791,434

[86] 国际申请 PCT/CA2007/000608 2007.4.13

[87] 国际公布 WO2007/118307 英 2007.10.25

[85] 进入国家阶段日期 2008.12.1

[71] 申请人 塞尔蒂卡姆公司

地址 加拿大安大略省

[72] 发明人 马里努斯·斯特洛伊克

[74] 专利代理机构 深圳中一专利商标事务所

代理人 张全文

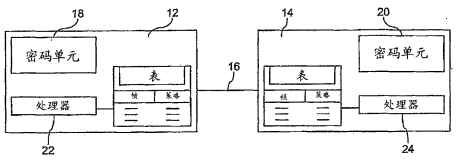
权利要求书 4 页 说明书 14 页 附图 8 页

[54] 发明名称

在电子通信中提供可适用安全等级的方法和装置

[57] 摘要

一种在安全通信系统中通信的方法，其包括以下步骤：在发送者处汇集消息，然后确定帧类型；以及在该消息的帧头中加入该帧类型的指征。 该消息随后被发送到接收者，该帧类型用于执行策略检查。



1.一种在数据通信系统中第一通信者和第二通信者之间通信的方法，包括:

—在上述第一通信者处聚集数据流，该数据流具有至少一个帧，该帧具有帧头和数据;

—在该帧头中整合帧类型的指示；以及

—传送该帧至上述第二通信者以使得该第二通信者根据该帧类型来判断该帧的可接受性。

2.如权利要求 1 所述的方法，进一步包括该第二通信者:

—接收该帧;

—从该帧头确定该帧类型；以及

—关联该帧类型至一个策略，以确定对该帧的至少一个属性而言该帧类型是否可接受。

3.如权利要求 2 所述的方法，进一步包括如果满足该策略则接受该帧，否则拒绝该帧。

4.如权利要求 2 所述的方法，其中该帧头中包括密钥代表，且该策略指出该密钥可接受的帧类型。

5.如权利要求 2 所述的方法，其中该帧头包括安全等级的指示，且该策略指出该安全等级可接受的帧类型。

6.如权利要求 2 所述的方法，其中该策略指出易遭受攻击的帧类型，如果该帧的安全特征的一个或多个组合存在，该方法包括如果发现上述组合其中之一则拒绝该帧。

7.如权利要求 1 所述的方法，包括通过选择安全等级来准备该帧以及在该帧中整合入指示该安全等级的一个或多个安全位。

8.如权利要求 7 所述的方法，包括根据该安全等级进行一下其中之一或二者：加密该数据和对该数据署名。

9.如权利要求 7 所述的方法，其中该安全等级为最低可接受的安全等级，且该最低可接受的安全等级独立于该数据。

10.如权利要求 7 述的方法，其中该安全等级为最低可接受的安全等级，且该最低可接受的安全等级取决于该数据。

11.如权利要求 7 述的方法，其中该安全等级为最低可接受的安全等级，且该最低可接受的安全等级部分取决于该数据，以致该最低安全等级依据该帧类型而变化。

12.如权利要求 2 述的方法，其中该帧包括一个或多个指示安全等级的安全位，且该方法包括该第二通信者提取该安全位以确定该安全等级，其中该策略指出该帧类型对该安全等级而言是否可接受。

13.如权利要求 10 所述的方法，其中该数据经过加密或署名其中之一或二者，该方法包括该第二通信者解密该数据和/或根据该安全位认证该数据。

14.如权利要求 2 所述的方法，其中该策略包括将该帧类型和上述至少一个属性相关联的查询表。

15. 如权利要求 1 所述的方法，其中该帧进一步包括一个或多个位的帧脚，该帧脚含有表示错误码。

16.如权利要求 1 所述的方法，其中该帧头包括密钥识别、对应该密钥识别的密钥表示、安全等级和确定该帧类型的接受性的始发者。

17.一种验证在数据通信系统中第一通信者和第二通信者之间通信的方法，包

括该第二通信者:

—从该第一通信者处接收具有帧头和数据的帧，该帧头包括帧类型的指示;

—从该帧头确定该帧类型；以及

—关联该帧类型与一个策略，以确定对该帧的至少一个属性而言该帧类型是否可接受。

18.如权利要求 17 所述的方法，进一步包括如果满足该策略则接受该帧，否则拒绝该帧。

19.如权利要求 17 所述的方法，其中该帧头中包括密钥代表，且该策略指出对该密钥而言可接受的帧类型。

20.如权利要求 17 所述的方法，其中帧头包括安全等级的指示，且该策略指出对该安全等级而言可接受的帧类型。

21.如权利要求 17 所述的方法，其中该策略指出易遭受攻击的帧类型，如果该帧的安全特征的一个或多个组合存在，该方法包括若发现上述组合其中之一则拒绝该帧。

22.如权利要求 20 所述的方法，其中该安全等级为最低可接受的安全等级，且该最低可接受的安全等级独立于该数据。

23.如权利要求 20 所述的方法，其中该安全等级为最低可接受的安全等级，且该最低可接受的安全等级取决于该数据。

24.如权利要求 20 所述的方法，其中该安全等级为最低可接受的安全等级，且该最低可接受的安全等级部分取决于该数据，以致该最低安全等级依据该帧类型而变化。

25.如权利要求 17 所述的方法，其中该帧包括一个或多个指示安全等级的安

全位，且该方法包括该第二通信者提取该安全位以确定该安全等级，其中该策略指出对该安全等级而言该帧类型是否可被接受。

26.如权利要求 25 所述的方法，其中该数据经过加密或签名其中之一或两者，该方法包括该第二通信者解密该数据和/或根据该安全位认证该数据。

27.如权利要求 17 所述的方法，其中该策略包括该策略包括将该帧类型和上述至少一个属性相关联的查询表。

28.一种在通信系统中的一对通信者之间通信的方法，包括对上述通信者的其中之一豁免与该通信系统相关的安全规则，以使该通信者开始与另一通信者通信。

29.如权利要求 28 所述的方法，其中该另一通信者含有该通信者的状态的指征，且如果该状态指出该通信者被豁免该安全规则，使该通信者开始通信并之后进行初始化，如此通过该初始化之后，该状态改变为指示该通信者遵循该规则。

30.如权利要求 28 所述的方法，其中该数据通信系统为网络，该另一通信者为负责控制对该网络的访问的中间通信者。

在电子通信中提供可适用安全等级的方法和装置

技术领域

【0001】本发明涉及在电子通信中提供可适用安全等级的方法和装置。

背景技术

【0002】电子通信中经常需要防止窃取者中途截取消息。也期望提供消息的真实性的指征，该指征为发送者的可验证的认证。这些目标通常通过密码术的运用来实现。私钥密码术需要在开始通信前共享一个密钥。人们通常更愿意使用公钥密码术，因为其不需要这种共享的密钥。不同地，每个通信者拥有包含私钥和公钥的钥对。该公钥可通过任何便利的方式提供，并不需要保密。

【0003】密码算法中有很多变化以及确定该精密运算的各种参数。无线通信的标准中，惯常为每种帧类型提前设定好这些参数。然而，这种方式限制了这些参数的灵活性。

【0004】当一个装置与其它若干装置通信时，常常需要针对每一通信设立各自的参数。

【0005】本发明的一个目的为消除或减轻上述不足之处。

发明内容

【0006】一方面，本发明提供一种在数据通信系统中第一通信者和第二通信者之间通信的方法，该方法包括：在上述第一通信者处聚集数据流，该数据流具有至少一个帧，该帧具有帧头和数据；在该帧头中整合帧类型的指示；以及传送该帧至上述第二通信者以使得该第二通信者根据该帧类型来判断该帧的可接受性。

【0007】另一方面，本发明提供一种验证在数据通信系统中第一通信者和第二通信者之间通信的方法，包括该第二通信者：从该第一通信者处接收具有帧头和数据的帧，该帧头包括帧类型的指示；从该帧头确定该帧类型；以及关联该帧类型与一个策略，以确定对该帧的至少一个属性而言该帧类型是否可接受。

【0008】再一方面，本发明提供一种在数据通信系统的一对通信者之间通信的方法，包括对上述通信者的其中之一豁免与该通信系统相关的安全规则，以使该通信者开始与另一通信者通信。

附图说明

【0009】以下将以将结合附图的方式对本发明的一个实施例进行描述，其中：

【0010】图 1 为通信系统的示意性表示；

【0011】图 2 为图 1 所示的通信系统中交换的信息帧的示意性表示；

【0012】图 3 为图 2 所示的帧的帧控制部分的示意性表示；

【0013】图 4 为图 1 中的发送者所执行的方法的示意性表示；

【0014】图 5 为图 1 中的接收者所执行的方法的示意性表示；

【0015】图 6 为该通信系统的一个实施例中的网络的示意性表示；

【0016】图 7 为该通信系统的一个实施例的示意性表示；

【0017】图 8 为该通信系统的另一实施例的示意性表示；

【0018】图 9 为另一帧的示意性表示；

【0019】图 10 为利用图 9 中的帧，发送者所执行的方法的示意性表示；

【0020】图 11 为利用图 9 中的帧，接收者所执行的方法的示意性表示；

【0021】图 12 为另一通信系统的示意性表示；及

【0022】图 13 为图 12 中的通信者所执行的方法的示意性表示。

具体实施方式

【0023】请参阅图 1，通信系统 10 包括一对由通信线路 16 所连接的通信者 12、14。每一通信者 12、14 包括各自的密码单元 18、20。

【0024】每一通信者 12、14 可包括处理器 22、24。每个处理器可连接至显示器及用户输入装置，例如键盘、鼠标或其它适合的装置。如果该显示器是触摸感应式的，则该显示器自身可作为用户输入装置使用。计算机可读存储介质（图未示）连接至每一处理器，以为处理器 22、24 提供指令来命令和/或设置处理器 22、24 来执行与每一通信者 12、14 的操作相关的步骤或运算，下文将进一步解释。该计算机可读介质可包括硬件和/或软件，例如（仅以举例的方式）：磁盘（Magnetic Disk）、磁带（Magnetic Tape）、光读取介质（如 CD-ROM）及半导体存储器（如 PCMCIA 卡）。在每种情形下，该介质可为便携的形式，例如小视盘（Small Disk）、软盘（Floppy Diskette）、盒式磁带（Cassette），或该介质可为相对较大或不可移动的形式，例如支持系统中所提供的硬盘驱动器（Hard Disk Drive）、固态记忆卡（Solid State Memory Card）或随机存储器（RAM）。应当指出，上述列举示例介质既可单独使用也可结合使用。

【0025】为了在通信者 12、14 之间传输数据，分组流 30 根据已定义的协议在至少一个通信者处被汇集。该分组流 30 在图 2 中示意性表示，且由一个或多个帧 31 组成，每个帧 31 具有帧头（Header）32 和数据（Data）34。在某些协议中，该分组自身可被组织成一个帧，该具有帧头 32a 和由单独的帧的组成的数据 34a。该帧头 32 由位串组成并在该位流中指定位置包含有控制信息。

【0026】每一帧头 34 中包含安全控制位 33，该安全控制位 33 包括安全模式位 35 和完整性等级位 36、37。

【0027】在本实施例中，安全模式位 35 用于指出是否加密。完整性等级位 36、37 一起用于指出使用的是四个完整性等级（例如 0、32、64、128 位密钥长度）

中的哪一个。该安全模式位 35 可用于指示操作的可选模式，例如认证，位长可增加（或减少）以适应不同的组合。应当意识到，在该位流 30 的每一帧 31 中提供安全位允许该安全等级建立在逐帧的基础上，而不是建立在一对通信者的基础上，因此，在组织通信中提供更好的灵活性。

【0028】为了保障安全，可使用某些最低安全等级。这些等级应通过一个已议定的规则由所有的通信者决议。该规则可为静态或动态。

【0029】在操作中，通信者 12 执行图 4 中由数字 100 所表示的步骤，以发送信息至通信者 14。首先，在步骤 102 中该通信者 12 准备数据和帧头。然后，在步骤 104 中选择安全等级。该安全等级通过考虑接收者必需的最低安全等级、该接收者的性质和被传送的数据的类型来确定。如果安全等级含有加密，则在步骤 106 中该通信者 12 加密数据。如果该安全等级含有认证，则在步骤 108 中该通信者 12 对该数据签名。然后，在步骤 110 中该通信者 12 将指征该安全模式及安全等级的位加入该帧控制中。在步骤 112 中该通信者 12 发送该帧至通信者 14。

【0030】一旦收到该帧，该通信者 14 执行图 5 中由数字 120 所表示的步骤。在步骤 122 中，该通信者 14 首先接收该帧。然后，在步骤 124 中提取该安全位。如果模式安全位 34 指出已加密，则在步骤 126 中该通信者 14 解密该数据。如果该安全位指出需认证，则在步骤 126 中验证该签名。最后，在步骤 128 中该通信者 14 检查该安全等级以确保其满足预设的最低安全等级要求。在步骤 130 中，如果加密或认证中任一失败，或该安全等级不满足最低要求，则该通信者 14 拒绝该消息；如果该加密和认证成功，且该安全等级满足最低要求，则该消息被接受。

【0031】应当意识到，提供安全位和可调的安全等级为保护该通信中的每一帧带来灵活性。因此该发送者能够决定哪些帧应该加密但不需认证。由于认证通常增加消息的长度，这在带宽非常珍贵的受限环境下节约资源。

【0032】在另一实施例中，该通信者 12 希望以不同的最低安全要求分别发送相同消息给多个接收者 14。在这种情况下，该通信者 12 选择足够高的安全等级以满足全部的要求。该通信者 12 随后如图 4 中所示以该安全等级来汇集并发送消息。由于满足每一接收者的最低要求，该消息将被他们每一个所接受。应当意识到，相较分别处理每一接收者的要求而言，本实施例更有效率。

【0033】在另一实施例中，使用不同的安全位长。实际位长不限于任何数值，而是可针对任何给定的应用而预先确定。该安全位应指出运算参数，这些安全位可被用于确定密钥的长度为 40 位或 128 位、所使用的密钥的版本或者该加密系统中的任何其它参数。

【0034】应当意识到，在上述实施例中，可使用网络堆栈来组织通信者之间的通信。因此参看图 6，通信者 A 的网络堆栈用数字 130 表示，通信者 B 的网络堆栈用数字 140 表示。这些网络堆栈被分成几层并具有类似的结构。网络堆栈 130 包括应用层（Application Layer，APL）132、网络层（Network Layer，NWK）134、消息认证层（Message Authentication Layer，MAC）136 和物理层（Physical Layer，PHY）138。该网络堆栈 140 包括用类似标号方式表示的类似组成部分。

【0035】该发送者决定他如何保护有效负载（Payload）（以及在哪保护它，即哪一层）。对 APL 层而言，安全性是透明的，其作用仅为指出数据保护的等级（即安全服务：无、机密、数据认证或两者皆有）。实际的密码处理则被指派到下面的层。

【0036】基于接收到的帧和本地维护的状态信息，该接收者决定是否接受被保护的有效负载。该密码处理（在与发送者相同的层进行）的结果，包括透明传送的保护等级的信息，被传送到应用层，该应用层决定所提供的保护等级是否充分。该接收者可基于该“充分性测试”向原始发送者确认该帧的正确接收。

【0037】该确认（ACK），如果有，被传送回至发送者并被传送到适当的层（如果被保护的消息在 APL 层被发送，则 ACK 应返回至那一层；当然，对下面的层而言类似）。

【0038】该发送者A决定其想要使用SEC所指示的保护等级来保护有效负载m（考虑自身安全需求和，可能的话，那些预期的接收者的安全需求）。该有效负载 m 和期望的保护等级 SEC 然后被传送到负责实际密码处理的下一层（例如图中的 MAC 层）。（该传送的消息可包括辅助该帧处理的附加状态信息，例如预期的接收者、分片信息等。应注意，如果进行密码处理的层与有效负载 m 所在的层相同，指派到下一层进行密码处理仅仅是概念性的步骤。）

【0039】密码处理包括利用该期望的保护等级 SEC 所指示的密码处理来保护有效负载 m 和（可能的话）相关信息（如帧头）。用于保护该信息的密钥来自该发送者和该预期的接收者之间所维护的共享密钥材料（Keying Material）。在密码处理之后，在图 6 中用[m]K, SEC 来表示的该被保护的帧被传递到至预期的接收者 B。

【0040】利用该监测到的保护等级SEC'所指示的密码处理，且利用该发送者和该预期接收者之间所维持的共享密钥材料所得到的密钥，该预期的接收者从该接收到的被保护的帧中获取该有效负载 m'。该获取到的有效负载 m'和该监测到的保护等级SEC'被传递到与该发送者发出该有效负载相同的层，在这里判断该监测到的保护等级的充分性。如果满足或超过期望的保护等级 SEC_0，该监测到的保护等级 SEC'被认为足够，这里参数 SEC_0 可能为固定的预先商议的保护等级，该保护等级独立于或取决于在此讨论的获取到的有效负载 m'。（在取决于消息方式下定义 SEC_0 将允许细粒度的访问控制策略，但通常会增加存储和处理的需求。）

【0041】上述方式在期望的保护等级和监测到的保护等级可进行比较的环境下工作，例如这组保护等级为一个偏序（Partial Ordering）的环境或（一组保护等

级其中之一）进行隶属测试（Membership Test）的环境。一个示例是包含加密和/或认证的组合的情形下，将加密的自然排序（Natural Ordering）（不加密< 加密，Encryption OFF< Encryption ON）和认证的自然排序（按照数据认证字段的长度递增来排序）的笛卡尔乘积（Cartesian product）进行排序。此外，如果这组保护等级具有最高等级，则该发送者可使用该最高保护等级来确保（未被改变的）消息总能通过充分性测试。在另一示例中，将该被观测的保护等级与 SEC_0 比较，这里 SEC_0 为一组保护等级，而不仅仅是最低保护等级。在这种方式下，如果 SEC_0={None, Auth-32, Auth-64, Auth-128}且 SEC=Auth-32，则该充分性测试通过；反之如果 SEC_0 和上面相同且 SEC=Auth-32+机密（Confidentiality，例如加密），则该充分性测试失败。

【0042】在以上实施例中，每一发送者预先与每一预期的接收者商议该最低期望保护等级 SEC_0。因此，这种方式可能不如预期那样适用于某些应用场合且该 SEC_0 参数的每一改变都可能带来额外的协议开销（Protocol Overhead）。这些不足可利用从接收者到发送者的确认（ACK）机制作为该 SEC_0 信息的反馈通道来克服。这通过在每一确认信息中加入关于期望保护等级的指示信息来完成。该信息可随后被原始发送者核对以更新其接收者的期望的最低保护等级，而不管这是否取决于消息。

【0043】在另一实施例中，示出一种同步安全等级的方法。参看图 7，该通信系统的另一实施例总体用标号 160 表示。该系统包括一个发送者 162（发送者 A）和在标记为 G 的组内的接收者 168。该发送者 A 包括参数 SEC_A 164 和 SEC_G 166。

【0044】发送者 A 想要安全传递消息 m 至设备组 G。该发送者 A 访问该二个参数，即（1）想要保护该信息的最低等级 SEC_A（一般而言，SEC_A 可能取决于其发送信息所至的组和该信息本身，故适当的标记为 $SEC_A(m,G)$）；（2）该接收者的组 G 期望的最低保护等级 SEC_G（如果该等级取决于该发送者和该信息

本身，适当的标记为 $SEC_G(m,A)$）。这里，一个组的最低期望等级为所有组员的最低期望等级的最大值。

【0045】初始化:

【0046】发送者 A 假定每一参数 SEC_G 被设置为最高保护等级（针对与其安全通信的每一组 G）。

【0047】操作方法:

【0048】发送者 A 确定其想要保护该消息 m 的最低保护等级 SEC_A。应用于该消息 m 的实际保护等级 SEC 同时满足自身的充分性测试（即 $SEC \geq SEC_A$）和该组 G 的最低期望等级（即 $SEC \geq SEC_G$）。

【0049】该组 G 中的每一接收者 B（即 $B \in G$）在其安全确认消息中指出在该特定时刻的最低期望保护等级（针对发送者 A 和消息 m）。

【0050】A 更新该参数 SEC_G，使其与接收反馈回的每一确认信息中指出的所有最低保护等级一致（即在所有响应的设备 B 中：$SEC_G \geq SEC_B$）。

【0051】应注意到，上述流程发送消息的保护等级同时满足该发送者的需求和接收者的期望，并能适应随时间的变化。可选择地，该发送者可仅考虑其自身的保护需求，其代价为可能发送的消息会因充分性不够（因为低于期望保护等级）而被一个或多个接收者拒绝。

【0052】上述流程可被归纳为任一网络拓扑中装置间的状态信息的大概自同步过程，这里关于状态信息的反馈信息可能在沿从接收者到发送者的反馈路径上就被部分处理，而不是仅由发送者自己处理（在上述示例中，拓扑图为具有根部 A 和树叶（接收者）的树，且该同步涉及一个特殊的安全参数）。

【0053】如图 8 中所示，A 发送以安全保护等级 SEC 保护的有效负载至 B1-B4 构成的设备组。接收者 B1-B4 以期望的保护等级（在图中以整数 1、3、2、5 所示，这里这些整数以保护等级递增的顺序编号）提供反馈给发送者 A。该反

馈经由中间节点C1和C2被传送回A，这些节点在代表二个组返回给发送者A压缩的认证信息之前收集组G1、G2中的各设备其各自的反馈并加以处理。该这些中间设备所提供的压缩反馈为A提供满足所有接收者期望的最低保护等级的信息，该信息与不经中间处理就传送给A的情形中的信息相同。（这里，我们假定中间设备在计算中不存在欺骗。）

【0054】在另一实施例中，通信中的每一帧的结构如图9中所示并大体上用数字170表示。该帧170主要包括帧头172、有效负载174和帧脚176。该帧脚176通常包括代表错误码的一个或多个位。该有效负载174包括该特定帧170中将被传送的数据，即消息。

【0055】一个示范性的帧头172a在图9详细示出。该帧头172a包括密钥标识（Key Identifier）178、密钥代表（Representation）180、帧类型182、安全等级184（如之前一样）和信息始发者（例如发送者12）的指示186。

【0056】该帧头172a的每一部分包含表示传送的某一属性的一个或多个位或包括一条信息。该密钥标识178和该密钥代表180通常用于确定使用什么密钥和如何使用该密钥，例如广播或单播通信。

【0057】该帧类型182提供关于在该特定帧172a中什么传送类型将被发送的指征。典型的帧类型182包括数据帧、指令帧、确认帧和信标帧。数据类型的帧传输数据，指令类型的帧传输指令，确认类型的帧传输反馈信息给发送者，例如接收者对帧已被适当接收的确认，以及信标帧通常将传送以时间间隔分割开。

【0058】为了提供安全，除了为接收者14提供最低安全等级外，该发送者12在帧头172a中加入了帧类型182。该帧类型182被该接收者14用于执行策略检查（Policy Check）以确定该安全等级、密钥、密钥用法等是否适合被传输的帧的类型。例如，对通常需要高安全性保护的帧类型而言，安全性不够将遭到拒绝。

【0059】在操作中，该发送者 12 执行图 10 中数字 200 所示的步骤来发送信息给接收者 14。首先，根据上述步骤 102-110 该发送者 12 在步骤 202 中和准备该帧。应当了解，这些步骤也包括帧头 172a 的准备以包括图 9 中所示的位的代表。在步骤 204 中，该发送者确定该帧类型 182 并在帧头 172a 中包括一个或多个位以指示该帧类型 182。在步骤 206 中，该发送者 12 随后发送该帧 170 至接收者 14。

【0060】一旦接收到该帧 170，该接收者 14 执行图 11 中数字 208 所示的步骤。首先在步骤 210 中该接收者 14 接收该帧，然后在步骤 212 中执行上述讨论的步骤 124-126。然后在步骤 214 中，该接收者 14 从帧头 172a 中提取帧类型 182。随后在步骤 216 中，为了执行策略检查，该帧类型 182 被与策略相关联。具体而言，该接收者访问指示每一帧类型的一个或多个策略的查询表（Look-up Table）。在步骤 218 中该接收者 14 确定该策略是否满足，且在步骤 220 中基于该策略是否满足来拒绝或接受该帧 170。

【0061】该策略检查包括该帧类型 182 与某些其它数据的相关性，优选的是包含在该帧内的数据。例如，该策略可包括密钥类型和帧类型之间的某些相关性，以致基于该密钥 160 代表，根据该密钥是否适用于该特定帧类型 182 该帧被接受或拒绝。结果，为了要满足策略，需要某种类型的密钥（或密钥用法）。如果该密钥不是正确的类型，则该帧 170 不被接收者 14 所接受。如果单个帧头 32a 被用于图 2 中所示的多个帧 34a，则该策略将同样应用于该信息内的余下的帧。

【0062】在另一示例中，该策略基于该帧 170 内包含的安全等级 184 来设置，例如上文所讨论的最低安全等级 SEC_0。该帧 170 包含某一在发送者 12 准备该帧头 172 时已被包含的最低安全等级，且该最低安全等级与该特定帧类型相关联。如果该安全等级 184 适于该帧类型 162，则在步骤 220 中该帧 170 被接收者传送，如果不是该帧 170 被拒绝。应当理解，该策略可适用于将该帧内任何适当的信息与该帧类型 182 相关联。

【0063】为了防范更易于遭受攻击的安全特征的组合，上述原则使得安全检查适用于各种信息、各种帧类型等。例如，当帧类型不使用加密而特别容易受到攻击时，策略可造成接收者因未经加密仅需认证而拒绝该帧。

【0064】一般而言，存在三种安全等级检查，其具有不同粒度等级。第一种是 SEC_0 独立于消息的情况。在这种情况下，该最低安全等级只设置一次，本地仅需存储一个数值来执行策略检查。然而，由于对所有消息和消息类型仅有一个最低安全等级，当 SEC_0 独立于信息时提供最小粒度。

【0065】第二种是 SEC_0 完全取决于消息的情况。由于每个信息具有其自身的最低安全等级，在这种情况下提供高粒度等级。然而，这需要将所有消息和所对应的最低安全等级的列举存储在本地的表格中。

【0066】第三种是 SEC_0 部分取决于消息的情况，也就是如图 9-11 所讨论的消息被分成不同的类型（例如按照帧的类型），且每一种消息类型被分配一个最低安全等级。这种情况平衡了空间竞争需求和基于最低安全等级执行策略检查的粒度。通常，消息/帧类型的数量显著减少，并因此在表格中实现的可行性增加。

【0067】在图 12 所示的另一实施例中，网络 N 包括通过中间通信者 C 通信的一个或多个通信者（例如 A、B）。通信者 A 利用上述任何原则通过网络传输帧 150 至信者 C。当通信者 A 首先希望接入网络 N 时，他们没有密钥因而不能被认证以在网络 N 中通信。初始化程序的大体步骤在图 13 中示出。该通信者 C 首先在步骤 224 中获得 A 想要加入网络 N 的指示。该指示可通过适当的注册程序来提供。在步骤 226 中，通信者 C 在一个指示状态的表中加入 A，并将通信者 A 的状态设置为“豁免”。该豁免状态需要进行初始化程序，因而直到在网络 N 中被初始化后，通信者 A 才能安全通信。

【0068】在步骤 228 中，通信者 A 发送帧至中间通信者 C。在步骤 230 中，通信者 C 检查该表格。在这第一次通信中，该通信者 A 的状态为豁免且密钥交换

或其它初始化程序在步骤232中执行，且通信者A的状态在步骤234中变为“非豁免”（或豁免指示被移除，设为零等）。通信者A遵循正常的安全规则发送帧至通信者C。在步骤230中，通信者A的状态将从此之后被定为非豁免且在步骤236中应用正常的安全规则，例如通过检查安全等级、帧类型等。应当理解，A也可豁免C从而角色互换，且A允许C与之通信（例如，这里A为另一网络的一部分）。

【0069】在图12所示网络N的示例实施中，上述最低安全等级测试考虑该帧150和该始发者186。在这种情况下，该发送者为通信者A且该接收者为通信者B。最低安全等级的检查将因此为检查是否SEC ≥ SECB(m,A)。如果最低安全等级独立于始发者A，如前文所述，上述安全等级检查归结为检查是否SEC ≥ SECB(m)。与之前的安全等级测试一样，也有存储空间的考虑（情形1）。

【0070】如果该最低安全等级完全依赖于该始发者A，则列出最低安全等级表（如上文所述，依据帧m、m的帧类型或是否取决于消息），不同的是为每一始发者（情形2）。如果最低安全等级独立于始发者A，除了当始发者在一组明确列举出豁免的装置（例如表中由“ExemptSet”（豁免组）表示的）中之外，该ExemptSet之外的装置执行单一最低安全等级表（可能依据帧类型等），此外，为该ExemptSet中的每一成员列举其各自的最低安全等级表（情形3）。因此，如果通信者（和与之相关的装置）为该ExemptSet表的部分，适用情形2；如果没有装置在该ExemptSet表中，适用情形1。

【0071】如果通信者在该ExemptSet表中，使用独立于该ExemptSet中的该特定装置的一个最低安全等级表，则情形3可更易于执行。这要求，不在该ExemptSet表中的装置只需要执行一个安全等级表，而在该ExemptSet表中的装置执行一个表（情形4）。

【0072】情形4的进一步优化为，对在该ExemptSet表中的所有装置而言，该可能依赖于消息或消息类型（如上文所述）的最低安全等级被设置为针对在

ExemptSet之外的所有装置的最低安全等级或者被设置为针对所有在ExemptSet之内的所有装置的一个预先指定值。由于这将导致只有两种选择（例如：针对每帧、帧类型、全部），这可用布尔（Boolean）参数来指示。

【0073】总之:

【0074】$SEC \geq SEC_B(m,A))$，这里

- 如果A不是ExemptSet的成员，$SEC_B(m,A))=SEC_B(m)$。
- 如果A是ExemptSet的成员且消息m的重写参数OverrideSEC(m)设置为假（FALSE），$SEC_B(m,A))= SECB\ (m)$。
- 如果A是ExemptSet的成员且消息m的重写参数OverrideSEC(m)设置为真（TRUE），$SEC_B(m,A))= ExemptSEC_B(m)$。

【0075】总的来说，最实际的情况下 $ExemptSEC_B(m)$被设置为“不安全”。

【0076】应当注意到，如果一些装置已被接收者 B 标示出属于 ExemptSet（且ExemptSECB(m)被设置为“不安全”），有一种情形允许这些尚未有密钥的装置（例如，因刚加入该网络且尚需建立密钥，如经由密钥协商（Key Agreement）或密钥传输协议（Key Transportation Protocol）或个人身份号码（PIN）或其它机制）“绕过（by-pass）”该最低安全等级检查（即该安全检查始终成功）。

【0077】绕过最低安全等级检查可能取决于该接收到的消息 m、该消息 m 的帧类型（如果 m 的帧类型包括在该被传输的帧中，该消息对接收者可见——通常 m 的帧类型和其它帧控制信息并未加密），或取决于可通过重写参数OverrideSEC(m)设置的参数。

【0078】也应当注意到，接收者对 ExemptSet 的操作有效地约束该最低安全等级检查的操作（一个装置加入该组可能允许绕过或降低安全要求，同时一个装置从该组中的排除恢复普通的最低安全等级检查并使其（再次可能）适用于在此讨论的始发装置）。

【0079】因此，上述提供了在该系统的寿命期限内考虑通信者（及其装置）的过渡行为的弹性机制，并易于推进一个装置从还没有密钥的某初始阶段到已建立密钥并能严格遵守正常的最低安全等级策略的阶段。

【0080】该重写参数 OverrideSEC(m)允许精细调节“绕过”该最低安全等级检查并使这取决于接收到的消息 m（或消息类型——显然在付出表格实现成本的情况下可使粒度尽可能精细化）。例如，在一个装置加入网络并尚需建立一个密钥的情况下，可仅对始发装置 A 最低需求的消息或消息类型而言将重写参数 OverrideSEC(m)设为真（TRUE），以建立与接收装置 B（或与网络内的某些其它装置 T，一旦该密钥被建立该装置 T 即通知 B），因而限制装置 A 的可允许行为但并不排除所有形为。这也可用于任何其它初始化程序或设立程序并不应限于密钥设立。

【0081】同样，接收者 B 对重写参数 OverrideSEC(m)的操作允许对安全控制策略进行非常灵活且低耗的精调。例如，通过将所有的重写参数设为假（FALSE），有效地关闭与没有密钥的装置的所有网络操作（由于所有给接收者 B 的密码不安全的消息将最终被拒绝）——所谓的秘密行动模式——而将所有的重写参数设为真（TRUE），可能导致该最低安全等级测试被有效地绕过从而允许不安全的信息不受限制地流向装置 B。

【0082】应当意识到，该安全规则提供灵活性不仅可适用于在逐帧的基础上而且适用于基于帧类型，使得策略检查可确定是否某些安全规则或密钥类型可用于特定的帧类型。

【0083】尽管本发明已参照一些具体的实施例来描述，但本领域的技术人员在不脱离本发明的精神与本发明的权利要求所记载的范围的前提下可作出各种修改。

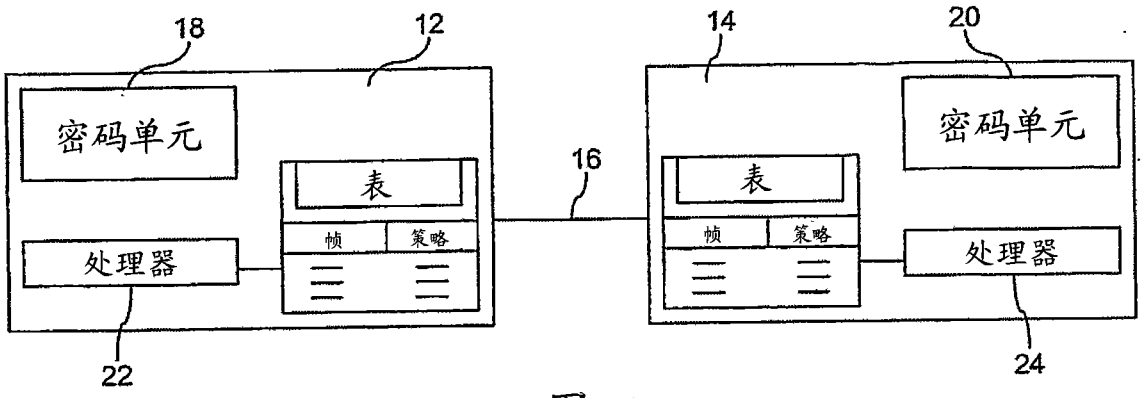

18
12
14
20
密码单元
表
16
密码单元
帧
策略
帧
策略
处理器
处理器
22
24

图 1

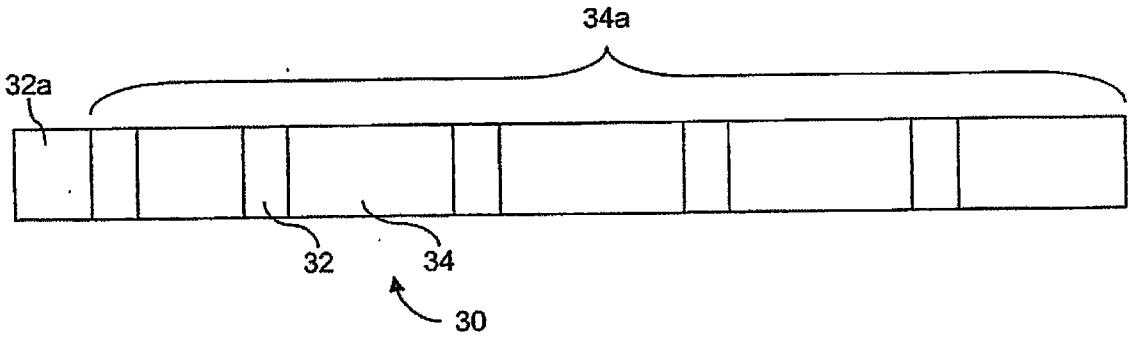

34a
32a
32
34
30

图 2

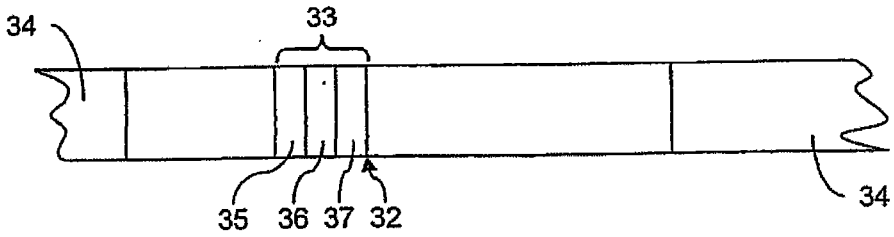

34
33
35
36
37
32
34

图 3

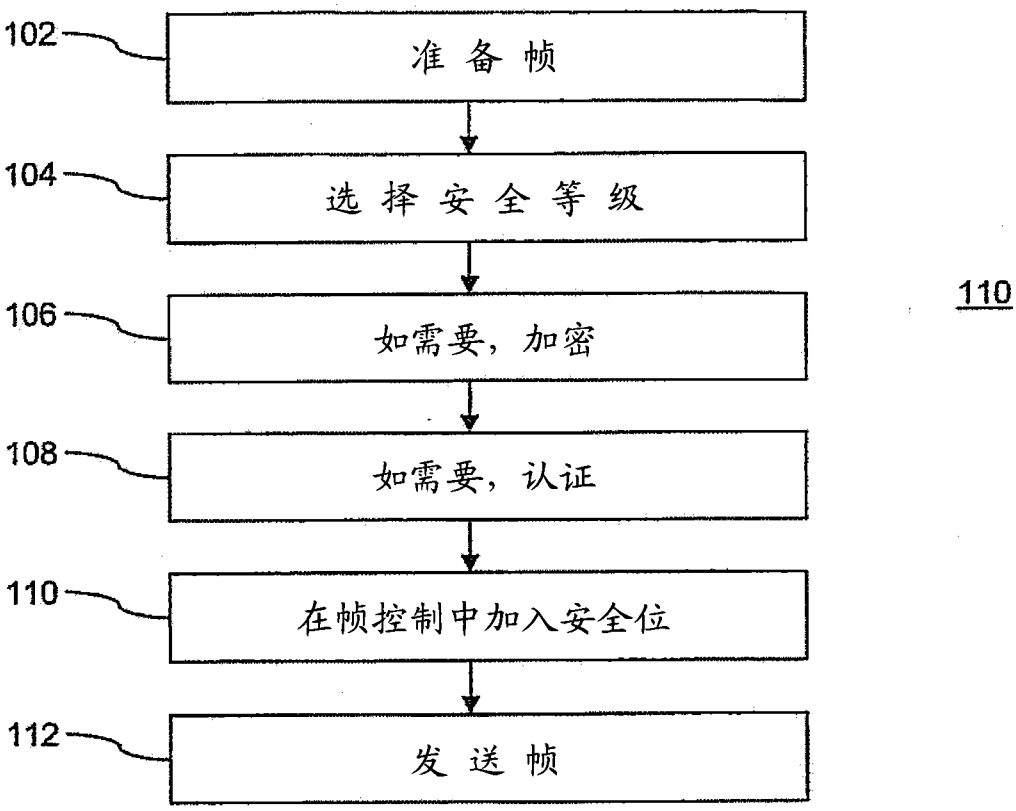

102
准 备 帧
104
选 择 安 全 等 级
106
如需要，加密
108
如需要，认证
110
在帧控制中加入安全位
112
发 送 帧
110

图 4

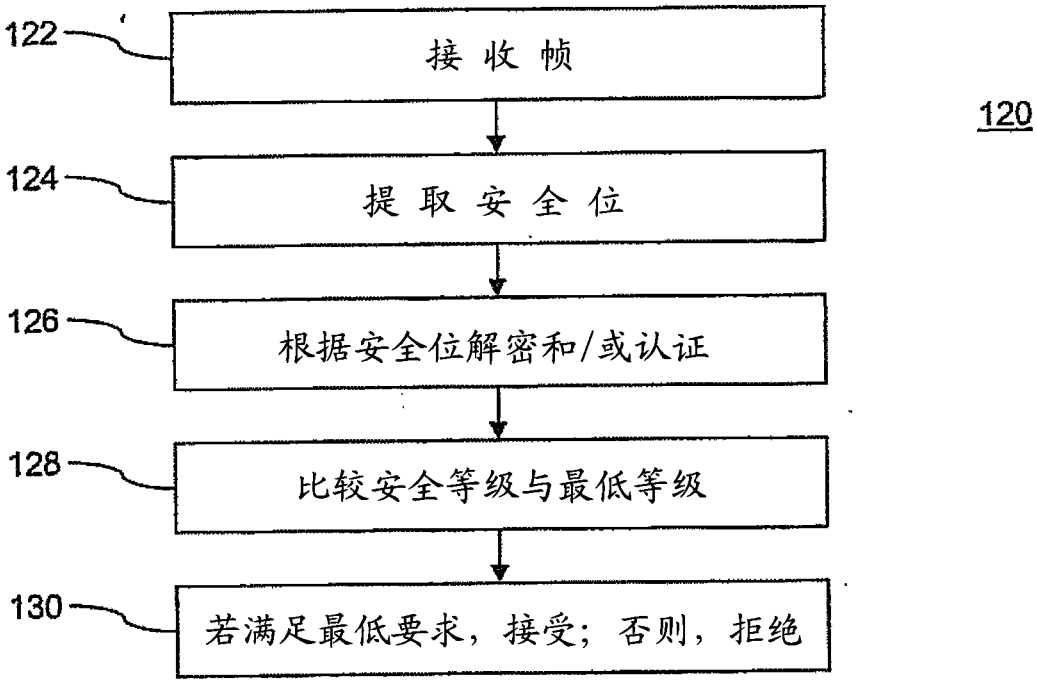

122
接 收 帧
120
124
提 取 安 全 位
126
根据安全位解密和/或认证
128
比较安全等级与最低等级
130
若满足最低要求，接受；否则，拒绝

图 5

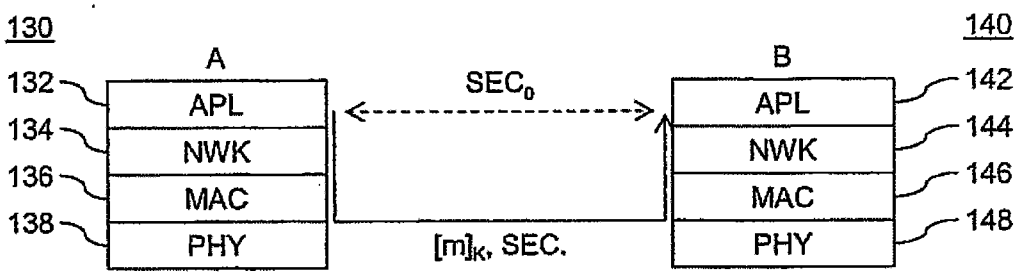

130
140
A
B
132
134
136
138
142
144
146
148
APL
NWK
MAC
PHY
APL
NWK
MAC
PHY
SEC0
[m]K, SEC.

图 6

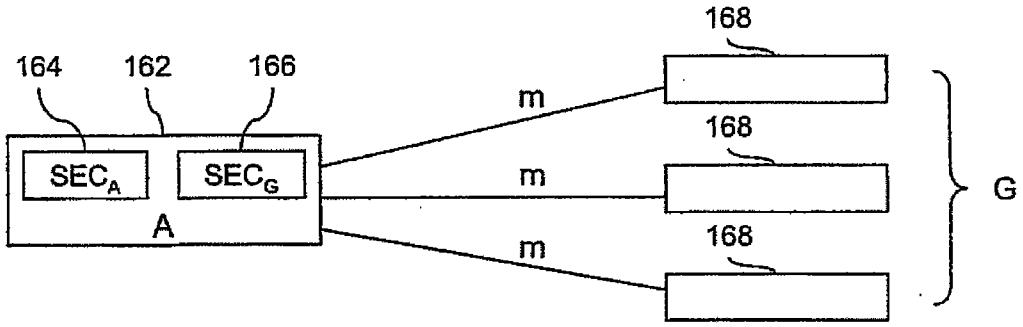

164
162
166
168
168
168
m
m
m
SECA
SECG
A
G

图 7

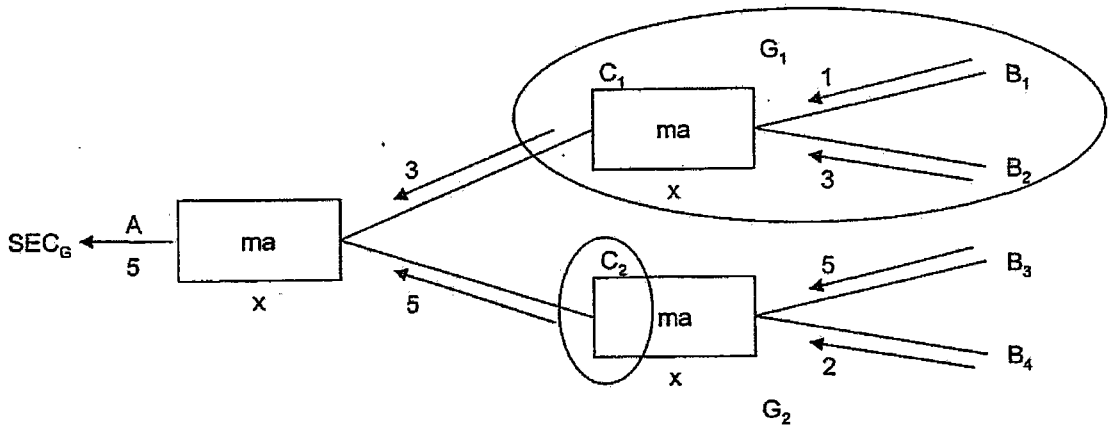


图 8

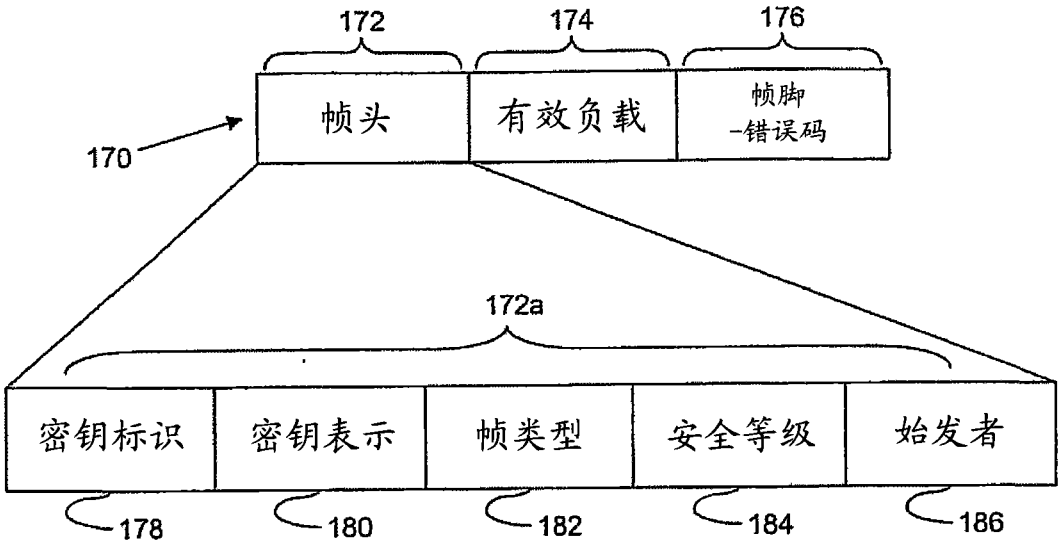

172
174
176
帧头
有效负载
帧脚
-错误码
170
172a
密钥标识
密钥表示
帧类型
安全等级
始发者
178
180
182
184
186

图 9

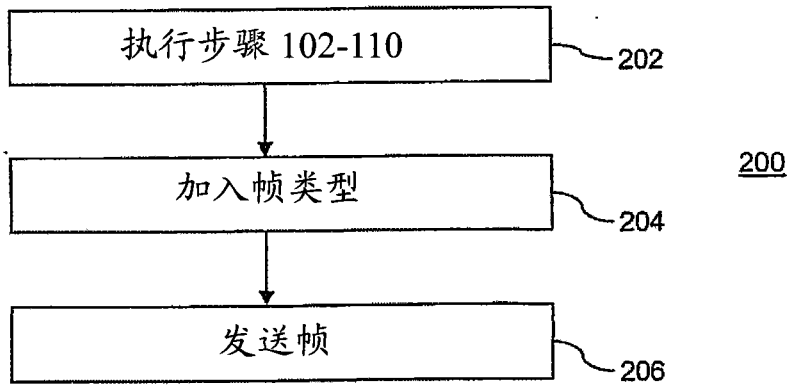

执行步骤 102-110
202
加入帧类型
204
200
发送帧
206

图 10

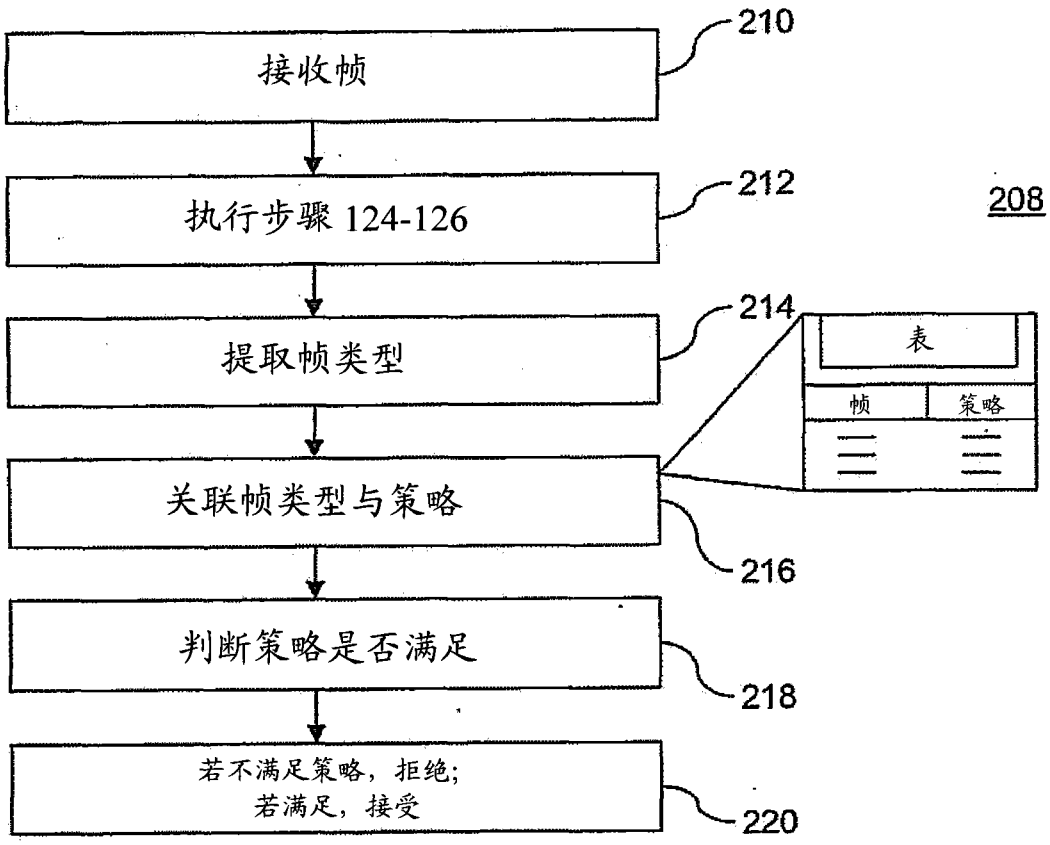

接收帧
210
执行步骤 124-126
212
208
提取帧类型
214
表
帧
策略
关联帧类型与策略
216
判断策略是否满足
218
若不满足策略，拒绝；
若满足，接受
220

图 11

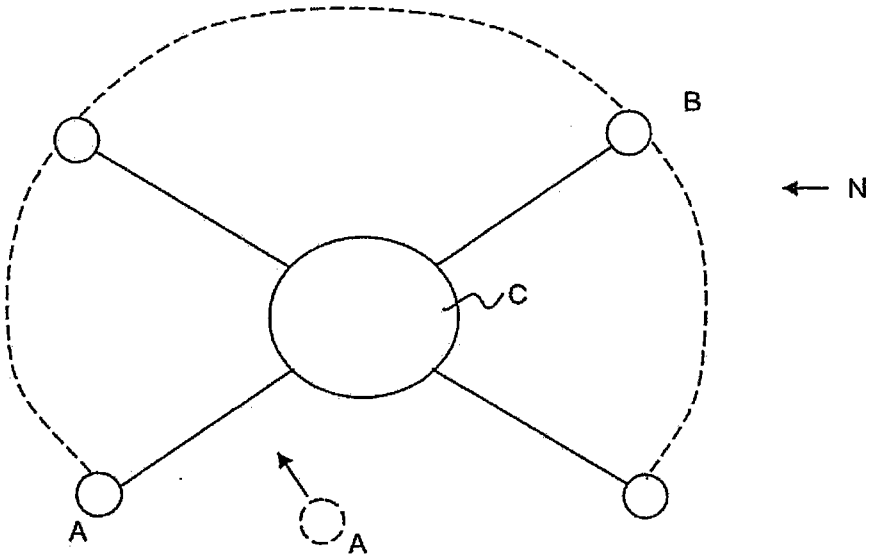

B
N
C
A
A

图 12

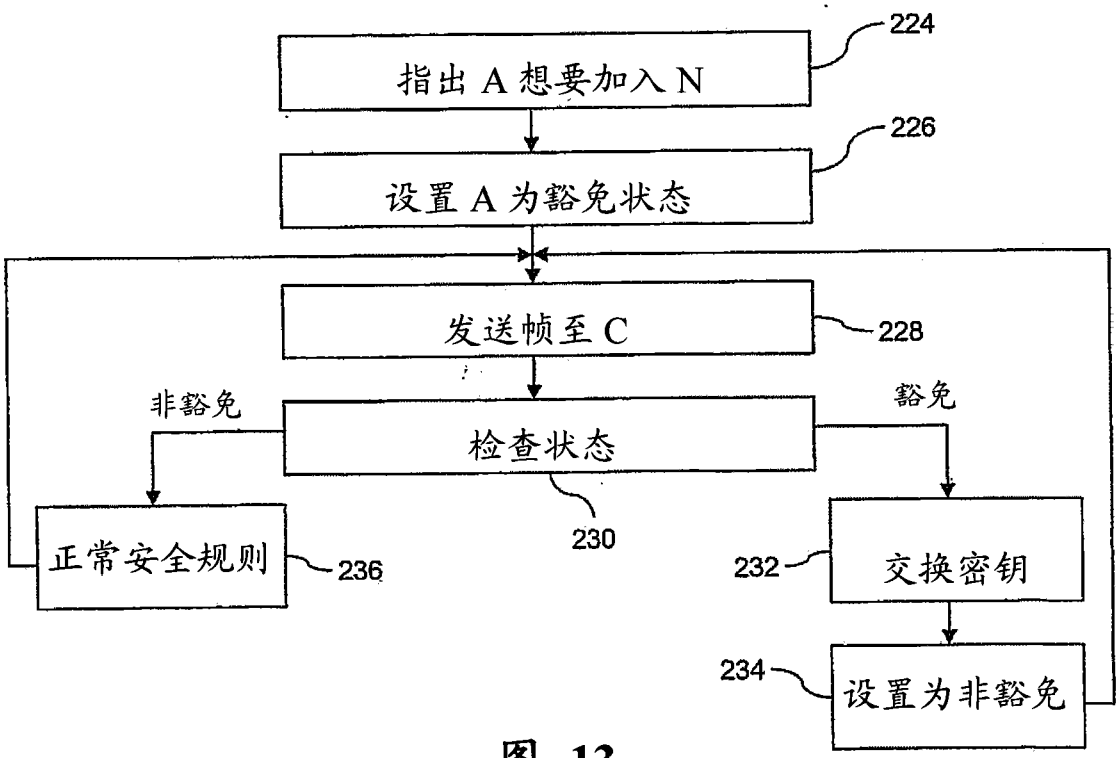

224
指出 A 想要加入 N
226
设置 A 为豁免状态
发送帧至 C
228
非豁免
豁免
检查状态
230
正常安全规则
236
232
交换密钥
234
设置为非豁免

图 13