(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 104782154 A
(43)申请公布日 2015.07.15

(21)申请号 201280076307.9
(22)申请日 2012.10.09
(85)PCT国际申请进入国家阶段日
2015.04.08
(86)PCT国际申请的申请数据
PCT/IB2012/055448 2012.10.09
(87)PCT国际申请的公布数据
WO2014/057305 EN 2014.04.17
(71)申请人 诺基亚技术有限公司
地址 芬兰埃斯波
(72)发明人 S·奥尔特曼斯 R·林霍尔姆
(74)专利代理机构 北京市中咨律师事务所 11247
代理人 宛丽宏 杨晓光
(51)Int.Cl.
*H04W 12/00*(2006.01)
*H04L 9/00*(2006.01)

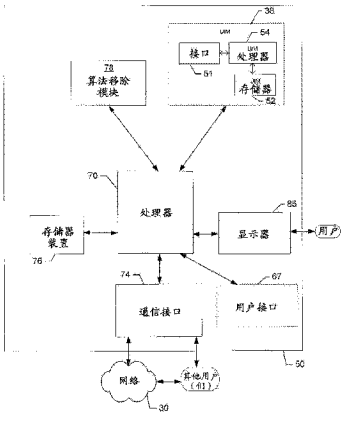
权利要求书5页 说明书13页 附图6页

(54)发明名称

一种用于禁用在装置中的算法的方法和设备

(57)摘要

一种用于使能移除或禁用弱算法的设备可以包括：处理器和包括计算机程序代码的存储器，计算机程序代码可以使得所述设备至少执行包括接收由通信装置利用的一个或多个算法的指示的操作。计算机程序代码还可以使得所述设备确定所述算法中的一个或多个是否被识别为弱算法。计算机程序代码还可以使得所述设备使能向所述通信装置提供消息以指示所述通信设备移除、禁用所述算法中的至少一个检测到的弱算法或向所述检测到的弱算法指派至少一个条件。对应的方法和计算机程序产品也被提供。




CN 104782154 A

1. 一种方法，包括：

接收由通信装置利用的一个或多个算法的指示；

确定所述算法中的一个或多个是否被识别为弱算法；以及

使能向所述通信装置提供消息，以指示所述通信设备移除、禁用所述算法中的至少一个检测到的弱算法，或向所述算法中的至少一个检测到的弱算法指派至少一个条件。

2. 如权利要求 1 所述的方法，其中确定所述算法是弱算法包括：确定所述弱算法的安全性是不可接受的或者所述安全性易于被攻击。

3. 如权利要求 1 或 2 所述的方法，其中在使能提供消息之前，所述方法进一步包括：

指示所述通信装置执行所述算法中的检测到的第一强算法以便于与网络装置的通信。

4. 如权利要求 3 所述的方法，进一步包括：

响应于检测到所述通信装置执行所述检测到的第一强算法以与网络装置通信，使能向所述通信装置提供数据以更新所述弱算法以便产生第二强算法。

5. 如权利要求 1 至 4 任一项所述的方法，进一步包括：

从所述通信装置接收确认所述通信装置已禁用或移除所述弱算法的消息。

6. 如权利要求 1 或 2 所述的方法，进一步包括：

响应于确定所述通信装置执行所述检测到的强算法以与所述网络装置通信，请求网络实体更新所述弱算法。

7. 如权利要求 1 或 2 所述的方法，其中，所述消息包括基于公钥基础设施的或者用密钥保护安全的命令。

8. 如权利要求 1 或 2 所述的方法，其中，所述条件指定利用局域网使用所述弱算法。

9. 如权利要求 1 或 2 所述的方法，其中：

使得消息的提供能够触发所述通信装置确定网络装置的操作方被批准提供所述消息。

10. 如权利要求 1 或 2 所述的方法，其中：

由所述通信装置利用的算法的指示是响应于经由局域网执行安全性扫描而被接收的。

11. 如权利要求 1 或 2 所述的方法，其中：

所述消息包括至少一个密钥和输入数据，触发所述弱算法确定响应于所述输入数据的执行而生成的输出值指示移除或禁用所述弱算法，引起所述弱算法移除或删除它本身。

12. 如权利要求 11 所述的方法，其中：

所确定的输出包括交织的预确定值和随机值的序列。

13. 如权利要求 11 所述的方法，进一步包括：

响应于接收到指示所述弱算法被删除或移除的一个或多个值，确定所述弱算法已删除或移除它本身。

14. 一种设备，包括：

至少一个处理器；以及

包括计算机程序代码的至少一个存储器，所述至少一个存储器和所述计算机程序代码被配置成，通过所述至少一个处理器，使得所述设备至少执行如下步骤：

接收由通信装置利用的一个或多个算法的指示；

确定所述算法中的一个或多个是否被识别为弱算法；以及

使能向所述通信装置提供消息以指示所述通信设备移除、禁用所述算法中的至少一个

检测到的弱算法，或向所述算法中的至少一个检测到的弱算法指派至少一个条件。

15. 根据权利要求 14 的设备，其中，所述至少一个存储器和所述计算机程序代码被进一步配置成，通过所述处理器，使得所述设备：

通过确定所述弱算法的安全性是不可接受的或者所述安全性易于被攻击，来确定所述算法是弱算法。

16. 如权利要求 14 或 15 所述的设备，其中在使能提供消息之前，所述至少一个存储器和所述计算机程序代码被进一步配置成，通过所述处理器，使得所述设备：

指示所述通信装置执行所述算法中的检测到的第一强算法以便于与所述设备的通信。

17. 如权利要求 16 所述的设备，其中所述至少一个存储器和所述计算机程序代码被进一步配置成，通过所述处理器，使得所述设备：

响应于检测到所述通信装置执行所述检测到的第一强算法以与所述设备通信，使能向所述通信装置提供数据以更新所述弱算法以便产生第二强算法。

18. 如权利要求 14 至 17 任一项所述的设备，其中所述至少一个存储器和所述计算机程序代码被进一步配置成，通过所述处理器，使得所述设备：

从所述通信装置接收确认所述通信装置已禁用或移除所述弱算法的消息。

19. 如权利要求 14 或 15 所述的设备，其中所述至少一个存储器和所述计算机程序代码被进一步配置成，通过所述处理器，使得所述设备：

响应于确定所述通信装置执行所述检测到的强算法以与所述设备通信，请求网络实体更新所述弱算法。

20. 如权利要求 14 或 15 所述的设备，其中，所述消息包括基于公钥基础设施的或者用密钥保护安全的命令。

21. 如权利要求 14 或 15 所述的设备，其中，所述条件指定利用局域网使用所述弱算法。

22. 如权利要求 14 或 15 所述的设备，其中所述至少一个存储器和所述计算机程序代码被进一步配置成，通过所述处理器，使得所述设备：

使能提供消息，所述消息触发所述通信装置确定所述设备的操作方被批准提供所述消息。

23. 如权利要求 14 或 15 所述的设备，其中所述至少一个存储器和所述计算机程序代码被进一步配置成，通过所述处理器，使得所述设备：

响应于经由局域网执行安全性扫描，接收由所述通信装置利用的算法的指示。

24. 如权利要求 14 或 15 所述的设备，其中：

所述消息包括至少一个密钥和输入数据，从而触发所述弱算法确定响应于所述输入数据的执行而生成的输出值指示移除或禁用所述弱算法，引起所述弱算法移除或删除它本身。

25. 如权利要求 24 所述的设备，其中：

所确定的输出包括交织的预确定值和随机值的序列。

26. 如权利要求 24 所述的设备，其中所述至少一个存储器和所述计算机程序代码被进一步配置成，通过所述处理器，使得所述设备：

响应于接收到指示所述弱算法被删除或移除的一个或多个值，确定所述弱算法已删除或移除它本身。

27. 一种包括至少一个计算机可读存储介质的计算机程序产品，所述计算机可读存储介质具有存储在其中的计算机可执行程序代码，所述计算机可执行程序代码包括：

被配置成接收由通信装置利用的一个或多个算法的指示的程序代码指令；

被配置成确定所述算法中的一个或多个是否被识别为弱算法的程序代码指令；以及

被配置成使能向所述通信装置提供消息以指示所述通信设备移除、禁用所述算法中的至少一个检测到的弱算法或向所述算法中的至少一个检测到的弱算法指派至少一个条件的程序代码指令。

28. 如权利要求 27 所述的计算机程序产品，进一步包括：

被配置成通过确定所述弱算法的安全性是不可接受的或者所述安全性易于被攻击来确定所述算法是弱算法的程序代码指令。

29. 如权利要求 27 或 28 所述的计算机程序产品，进一步包括：

被配置成指示所述通信装置执行所述算法中的检测到的第一强算法以便于与网络装置的通信的程序代码指令。

30. 如权利要求 29 所述的计算机程序产品，进一步包括：

被配置成响应于检测到所述通信装置执行所述检测到的第一强算法以与所述网络装置，使能向所述通信装置提供数据以更新所述弱算法以便产生第二强算法的程序代码指令。

31. 如权利要求 27 至 30 任一项所述的计算机程序产品，进一步包括：

被配置成使得从所述通信装置接收确认所述通信装置已禁用或移除所述弱算法的消息的程序代码指令。

32. 如权利要求 27 或 28 所述的计算机程序产品，进一步包括：

被配置成响应于确定所述通信装置执行所述检测到的强算法以与所述网络装置通信，请求网络实体更新所述弱算法的程序代码指令。

33. 如权利要求 27 或 28 所述的计算机程序产品，其中，所述消息包括基于公钥基础设施的或者用密钥保护安全的命令。

34. 如权利要求 27 或 28 所述的计算机程序产品，其中，所述条件指定利用局域网使用所述弱算法。

35. 如权利要求 27 或 28 所述的计算机程序产品，进一步包括：

被配置成使能提供消息的程序代码指令，所述消息触发所述通信装置确定网络装置的操作方被批准提供所述消息。

36. 如权利要求 27 或 28 所述的计算机程序产品，进一步包括：

被配置成响应于经由局域网执行安全性扫描，使得接收由所述通信装置利用的算法的指示的程序代码指令。

37. 如权利要求 27 或 28 所述的计算机程序产品，其中：

所述消息包括至少一个密钥和输入数据，从而触发所述弱算法确定响应于所述输入数据的执行而生成的输出值指示移除或禁用所述弱算法，引起所述弱算法移除或删除它本身。

38. 如权利要求 39 所述的计算机程序产品，其中：

所确定的输出包括交织的预确定值和随机值的序列。

39. 如权利要求 37 所述的计算机程序产品，进一步包括：

被配置成响应于接收到指示所述弱算法被删除或移除的一个或多个值，确定所述弱算法已删除或移除它本身的程序代码指令。

40. 一种设备，包括：

用于接收由通信装置利用的一个或多个算法的指示的装置；

用于确定所述算法中的一个或多个是否被识别为弱算法的装置；以及

用于使能向所述通信装置提供消息以指示所述通信设备移除、禁用所述算法中的至少一个检测到的弱算法或向所述算法中的至少一个检测到的弱算法指派至少一个条件的装置。

41. 根据权利要求 40 的设备，进一步包括：

用于通过确定所述弱算法的安全性是不可接受的或者所述安全性易于被攻击来确定所述算法是弱算法的装置。

42. 如权利要求 40 或 41 所述的设备，进一步包括：

用于指示所述通信装置执行所述算法的检测到的第一强算法以便于与所述设备的通信的装置。

43. 如权利要求 42 所述的设备，进一步包括：

用于响应于检测到所述通信装置执行所述检测到的第一强算法以与所述设备通信，使能向所述通信装置提供数据以更新所述弱算法以便产生第二强算法的装置。

44. 如权利要求 40 至 43 任一项所述的设备，进一步包括：

用于从所述通信装置接收确认所述通信装置已禁用或移除所述弱算法的消息的装置。

45. 如权利要求 40 或 41 所述的设备，进一步包括：

用于响应于确定所述通信装置执行所述检测到的强算法以与所述设备通信，请求网络实体更新所述弱算法的装置。

46. 如权利要求 40 或 41 所述的设备，其中，所述消息包括基于公钥基础设施的或者用密钥保护安全的命令。

47. 如权利要求 40 或 41 所述的设备，其中，所述条件指定利用局域网使用所述弱算法。

48. 如权利要求 40 或 41 所述的设备，进一步包括：

用于使能提供消息的装置，所述消息触发所述通信装置确定所述设备的操作方被批准提供所述消息。

49. 如权利要求 40 或 41 所述的设备，进一步包括：

用于响应于经由局域网执行安全性扫描，接收由所述通信装置利用的算法的指示的装置。

50. 如权利要求 40 或 41 所述的设备，其中：

所述消息包括至少一个密钥和输入数据，从而触发所述弱算法确定响应于所述输入数据的执行而生成的输出值指示移除或禁用所述弱算法，引起所述弱算法移除或删除它本身。

51. 如权利要求 50 所述的设备，其中：

所确定的输出包括交织的预确定值和随机值的序列。

52. 如权利要求 50 所述的设备，进一步包括：

用于响应于接收到指示所述弱算法被删除或移除的一个或多个值，确定所述弱算法已删除或移除它本身的装置。

# 一种用于禁用在装置中的算法的方法和设备

## 技术领域

[0001] 本发明的示例实施例通常涉及无线通信技术，并且特别地涉及用于提供通信协议以用于禁用或移除在通信装置中的算法的方法和设备。

## 背景技术

[0002] 现代通信时代已经带来了有线和无线网络的极大扩张。计算机网络，电视网络和电话网络正在经历由消费者需求驱动的前所未有的技术扩张。无线和移动联网技术已经解决了相关的消费者需求，同时提供了信息传输的更大的灵活性和直接性。

[0003] 当前和未来联网技术继续促进信息易于传输以及对用户而言的便利性。由于电子通信装置的现在普遍存在的性质，所有年龄和教育水平的人都在利用电子装置来与其他个体或联系人通信、接收服务和/或共享信息、媒体和其他内容。一个在其中有需求增加信息传送容易性的区域涉及向通信设备的服务递送。服务可以是促进通信装置功能性的特定应用或算法的形式。通信装置所使用的一些算法可以是为算法的使用提供安全的加密算法。

[0004] 目前，许多机器和装置利用机器类型通信。这些机器和装置（例如，传感器，致动器，和计量仪）中的一些可以用户无人值守并且可能不便于用户交互。机器类型通信可以允许机器和装置运转寿命长。例如，许多计量装置预计可用超过二十年。这种长寿命可能造成有关于通信装置的算法安全性的一些问题。例如，目前很难将弱算法从正被所部署的装置使用中移除，并且这个问题通常是通过逐步淘汰来解决，其中，新的设备仅仅具有较强的算法和不再是弱的算法，于是通过自然更换，装置群体迁移向较新的算法（对于移动装置而言，典型的更换周期是 2-3 年）。弱算法可能是不安全的算法，其可被作为攻击目标。在许多情况下，设备的寿命要比能够安全地支持的算法长得多。无法充分地确保在设备的长寿命上面的算法可能是由于随着时间的推移的技术进步，这可能使得强力攻击要更多的计算运算。此外，由于随着时间推移的技术进步，与加密算法相关联的加密密钥可能不足够强以防止黑客违反算法的安全性。

[0005] 目前，一些现有的解决方案包括：将两个或更多个算法包含到装置上，使得如果算法之一被确定为弱，有另一种算法使用作为备份的算法。目前，这种方法常常是不成功的，因为弱算法可能未被永久禁用。

[0006] 当弱算法仍然可用时，系统可能受到“出价向下攻击”，其中伪装成网络节点的攻击者可以指示它仅支持弱算法（例如，不安全的算法），在这种情况下装置可以遵从并使用弱算法，这可能导致安全漏洞。

## 发明内容

[0007] 据此提供一种方法和设备用于从通信装置自动移除或禁用一个或多个算法。就此方面，示例实施例可以提供使得能够远程禁用或移除在一个或多个通信装置上的弱算法（例如，易于被攻破的加密算法）的通信协议。其中算法可以被禁用或移除的通信设备可以是（但是不是必需）用户无人值守的。如此，从通信装置禁用或移除算法可以被执行，而无

需经由通信装置的用户交互。在一些示例实施例中，通信设备可以不包括用户接口。但是在其他示例实施例中，在用户接口可以被包括在通信装置中。

[0008] 在一个示例实施例中，在通信装置试图通过使用弱算法连接到网络装置的情形中，该弱算法可以被禁用或移除。在一些情形中，通信装置可以联络网络装置，从而提供所支持的算法（例如，安全性算法）的指示（例如，列表）。网络装置可以经由通信信道向通信装置指示使用较强算法用于与网络装置的通信。

[0009] 网络装置还可以确定通信装置所支持的一个或多个弱算法并且指示通信装置移除或禁用所检测到的弱算法。响应于接收到来自网络装置的指令，通信装置可以移除或禁用弱算法。就此方面，可以通过移除可能已过时或陈旧的较不安全的算法，来更新通信装置。

[0010] 在一个示例实施例中，提供了一种用于使能移除或禁用弱算法的方法。该方法可以包括接收由通信装置利用的一个或多个算法的指示。该方法可以进一步包括确定所述算法中的一个或多个是否被识别为弱算法。该方法可以进一步包括使能向所述通信装置提供消息以指示所述通信设备移除、禁用所述算法中的至少一个检测到的弱算法，或向所述算法中的至少一个检测到的弱算法指派至少一个条件。

[0011] 在另一示例实施例中，提供了一种用于使能移除或禁用弱算法的设备。该设备可以包括处理器以及包括计算机程序代码的存储器。所述存储器和计算机程序代码被配置成通过处理器使得所述设备至少执行操作，包括：接收由通信装置利用的一个或多个算法的指示。所述存储器和计算机程序代码被进一步配置成通过处理器使得所述设备确定所述算法中的一个或多个是否被识别为弱算法。所述存储器和计算机程序代码被进一步配置成通过处理器使得所述设备使能向所述通信装置提供消息以指示所述通信设备移除、禁用所述算法中的至少一个检测到的弱算法或向所述算法中的至少一个检测到的弱算法指派至少一个条件。

[0012] 在另一示例实施例中，提供了一种用于使能移除或禁用弱算法的计算机程序产品。该计算机程序产品包括至少一个计算机可读存储介质，所述计算机可读存储介质具有存储在其中的计算机可读程序代码。所述计算机可执行程序代码可以包括被配置成接收由通信装置利用的一个或多个算法的指示的程序代码指令。所述计算机可执行程序代码可以包括被配置成确定所述算法中的一个或多个是否被识别为弱算法的程序代码指令。所述计算机可执行程序代码可以包括被配置成使能向所述通信装置提供消息以指示所述通信设备移除、禁用所述算法中的至少一个检测到的弱算法或向所述算法中的至少一个检测到的弱算法指派至少一个条件的程序代码指令。

[0013] 在另一示例实施例中，提供了一种用于使能移除或禁用弱算法的设备。该设备可以包括用于接收由通信装置利用的一个或多个算法的指示的装置。该设备可以包括用于确定所述算法中的一个或多个是否被识别为弱算法的装置。该设备可以包括用于使能向所述通信装置提供消息以指示所述通信设备移除、禁用所述算法中的至少一个检测到的弱算法或向所述算法中的至少一个检测到的弱算法指派至少一个条件的装置。

## 附图说明

[0014] 如此以一般术语描述了本发明的一些示例实施例，现在将对附图进行参考，附图

不一定按比例绘制，并且其中：

[0015] 图 1 是根据本发明示例实施例的系统的示意框图；

[0016] 图 2 是根据本发明示例实施例的设备的示意框图；

[0017] 图 3 是根据本发明示例实施例的网络装置的示意框图；

[0018] 图 4 是根据本发明示例实施例的网络实体的示意框图；

[0019] 图 5 是根据示例实施例的系统的示意框图；

[0020] 图 6 说明了根据本发明示例实施例用于禁用或移除一个或多个算法的流程图；以及

[0021] 图 7 说明了根据本发明另一示例实施例用于禁用或移除一个或多个算法的流程图。

[0022] 具体实现方式

[0023] 现在将在后面参考附图全面描述本发明的一些实施例，其中，本发明的一部分而不是所有的实施例被示出。实际上，本发明的不同实施例可以用不同形式实施，并且不应该被视为限制于在此阐述的实施例。类似的参考数字至始至终指的是类似元件。根据本发明的实施例，在此使用的术语“数据”、“内容”、“信息”和类似术语可以可交换地用来指代能够被发射、接收和 / 或存储的数据。此外，在此使用的术语“示例”不是被提供来传达任何定性评估而只是传达示例的说明。因此，这类术语的使用不应该被视为限制本发明的实施例的范围。

[0024] 另外，在此使用的术语“电路”指的是 (a) 仅硬件的电路实施（例如，采用模拟电路和 / 或数字电路的实施方式）；(b) 电路和（一个或多个）计算机程序产品的结合，其包括存储在一个或多个计算机可读存储器上的软件和 / 或固件指令，它们一起工作以使得设备执行一个或多个在此描述的功能；和 (c) 电路，比如（一个或多个）微处理器或（一个或多个）微处理器的一部分，即使软件或固件物理上不存在，其也需要用于操作的软件或固件。在这里，“电路”的这种定义应用于此术语的所有使用，包括在任何权利要求中。作为又一个示例，在此使用的术语“电路”还包括这样一种实施方式，其包括一个或多个处理器和 / 或部分处理器以及附随的软件和 / 或固件。作为又一个示例，在此使用的术语“电路”还例如包括用于移动电话的集成了应用处理器的电路或基带集成电路，或服务器、蜂窝网络装置、其他网络装置和 / 或其他计算装置中的类似集成电路。

[0025] 在此定义的“计算机可读存储介质”指的是非临时性物理或有形存储介质（例如，易失性或非易失性存储器装置），它可以与指代电磁信号的“计算机可读传输介质”区分。

[0026] 而且，正如在此所指出的，算法可以是可以被执行的计算机指令的集合或子集。就此方面，算法可以包括但不限于：软件应用、计算机代码或者软件应用或计算机代码的一部分。在示例实施例中，算法可以具有安全和认证特性。

[0027] 附加地，正如在所指出的，弱算法可以，但不是必需，是指具有不可接受的安全性（例如，安全水平）或者安全性易受攻击的算法。

[0028] 图 1 说明了通用系统图，在其中，诸如移动终端 10 之类的装置在示例通信环境中被示出。如图 1 所示，根据本发明示例实施例的系统的实施例可以包括能够经由网络 30 彼此通信的第一通信装置（例如，移动终端 10）和第二通信装置 20。在一些情况下，本发明的实施例还可以包括一个或多个附加的通信装置，其中一个在图 1 中被绘出为第三通信装置

25。在一个实施例中，不是使用本发明实施例的所有系统可包括本文说明和/或描述的所有装置。虽然为了示例的目的，移动终端 10 和/或第二和第三通信装置 20 和 25 的实施例可以被示出并且在下文被描述，但是其他类型的终端，诸如传感器、计量装置（例如电表）、交通摄像头、天气传感器、家用 eNodeB(HeNB)（例如，毫微微小区）、便携数字助理 (PDA)、寻呼机、移动电视、移动电话、游戏设备、膝上型计算机、照相机、录像机、音频/视频播放器、无线电、全球定位系统 (GPS) 设备、蓝牙耳机、通用串行总线 (USB) 设备、或前述的以及其他类型的语音和文本通信系统的任何组合可以容易地使用本发明实施例。此外，不移动的设备，诸如服务器和个人计算机也可以容易地使用本发明的实施例。

[0029] 网络 30 可以包括可以经由对应的有线和/或无线接口彼此通信的各种不同节点（其中第二和第三通信装置 20 和 25 可以是示例）、装置或功能的集合。如此，图 1 的说明应该被理解为是系统的某些单元的宽广视图的示例，而不是系统或网络 30 的包罗万象或详细的视图。虽然不是必需的，但是在一个实施例中，网络 30 可以能够支持依照如下任何一个或多个的通信：第一代 (1G)，第二代 (2G)，2.5G，第三代的通信 (3G)，3.5G，3.9G，第四代 (4G) 移动通信协议，长期演进 (LTE)，高级 LTE(LTE-A) 和/或类似物。在一个实施例中，网络 30 可以是点对点 (P2P) 网络。

[0030] 一个或多个通信终端，诸如移动终端 10 和第二和第三通信装置 20 和 25 可以是经由网络 30 彼此通信，并且每一个均可以包括一个或多个天线，用于向基站发送信号以及用于从基站接收信号，基站例如可以是这样一个基站，其是一个或多个蜂窝或移动网络的一部分，或者是可以耦合到诸如局域网 (LAN)、城域网 (MAN) 和/或诸如互联网之类的广域网 (WAN) 之类的数据网络的接入点。接着，诸如处理元件（例如，个人计算机，服务器计算机等）之类的其他装置可以经由网络 30 耦合到移动终端 10 和第二和第三通信装置 20 和 25。通过将移动终端 10 和第二和第三通信装置 20 和 25（和/或其他装置）直接或间接连接到网络 30，可以使得移动终端 10 和第二和第三通信装置 20 和 25 能够例如根据包括超文本传输协议 (HTTP) 的众多通信协议和/或类似物而与其他装置进行通信或彼此通信，从而分别执行移动终端 10 以及第二和第三通信装置 20 和 25 的各种通信或其他功能。

[0031] 此外，移动终端 10 以及第二和第三通信装置 20 和 25 可以按照例如射频 (RF)、近场通信 (NFC)、蓝牙 (BT)、红外 (IR) 或多种不同有线或无线通信技术的任何技术进行通信，所述通信技术包括局域网 (LAN)、无线 LAN(WLAN)、全球微波互联接入 (WiMAX)、无线保真 (WiFi)、超超宽带 (UWB)、Wibree 技术和/或类似物。这样，可以使得移动终端 10 以及第二和第三通信装置 20 和 25 能够通过多种不同接入机制中的任何机制而与网络 30 进行通信以及彼此通信。例如，诸如 LTE、宽带码分多址 (W-CDMA)、CDMA2000、全球移动通信系统 (GSM)、通用分组无线业务 (GPRS) 和/或类似物之类的移动接入机制，以及诸如 WLAN、WiMAX 和/或类似物之类的无线接入机制，以及诸如数字用户线 (DSL)、电缆调制解调器、以太网和/或类似物之类的固定接入机制，均可以被支持。

[0032] 在示例实施例中，第一通信装置（例如，移动终端 10）可以是移动通信装置，诸如例如无线电话或其他装置，诸如个人数字助理 (PDA)、移动计算装置、照相机、录像机、音频/视频播放器、定位设备、游戏设备、电视设备、无线电设备、传感器、计量装置、交通摄像头、天气传感器、HeNB（例如，毫微微小区）或各种其他类似的设备，或它们的结合。第二通信装置 20 和第三通信装置 25 可以是移动或固定通信装置。然而，在一个示例中，第二通信装

置 20 和第三通信装置 25 可以是服务器，远程计算机或终端，诸如例如个人计算机 (PC) 或膝上型计算机。

[0033] 在示例实施例中，网络 30 可以是被布置成智能空间的自组织或分布式网络。因此，装置可以进入和 / 或离开网络 30 并且网络 30 中的装置可以能够基于其他装置的入口和 / 或出口来调整操作，以考虑相应的装置或节点及其相应能力的增或减。

[0034] 在示例实施例中，移动终端以及所述第二和第三通信装置 20 和 25 可以使用能够采用本发明实施例的设备 ( 例如，图 2 的设备 2)。

[0035] 图 2 说明了根据本发明示例实施例用于禁止或移除一个或多个弱算法的装置的示意框图。现在将参考图 2 描述本发明的示例实施例，在其中，设备 50 的某些元件被示出。图 2 的设备 50 可以被使用在例如移动终端 10( 和 / 或第二通信装置 20 或第三通信装置 25) 上。或者，设备 50 可被实施在网络 30 的网络设备上。然而，可替换地，设备 50 可以被实施在移动和固定的各种其它装置 ( 诸如例如上面列出的任何设备 ) 上。在一些情况下，实施例可以被使用在设备的组合上。因此，本发明的一个实施例可以完全实施在单个装置 ( 例如，移动终端 10) 处、由处于分布式方式中的多个装置 ( 例如，P2P 网络中的一个或多个装置 ) 来实施或者通过处于客户机 / 服务器关系中的装置来实施。此外，应该指出的是，下面描述的装置或元件可以不是强制性的并且因此一些装置或元件可以在某个实施例中被省略。

[0036] 现在参考图 2，设备 50 可以包括如下装置或以其他方式与如下装置通信 :处理器 70、可选用户接口 67、通信接口 74、存储器装置 76、显示器 85、可选用户识别模块 (UIM)38 以及算法移除模块 78。存储器装置 76 可以包括例如易失性和 / 或非易失性存储器。例如，存储器装置 76 可以是电子存储装置 ( 例如，计算机可读存储介质 )，其包括被配置来存储可以由机器 ( 例如，计算设备如处理器 70) 取回的数据 ( 例如，比特 ) 的栅极。在示例实施例中，存储器装置 76 可以是非临时性的有形存储装置。存储器装置 76 可以被配置来存储信息，数据，文件，应用程序 ( 例如，算法 )，指令等，用于使得设备能够按照本发明示例实施例执行各种功能。例如，存储器装置 76 可以被配置来缓冲输入数据以用于由处理器 70 进行处理。附加地或替换地，存储器装置 76 可以被配置来存储用于由处理器 70 执行的指令。作为又一替换，存储器装置 76 可以是存储信息和 / 或媒体内容 ( 例如，图片，音乐，和视频 ) 的多个数据库之一。

[0037] 处理器 70 可以以许多不同的方式来实施。例如，处理器 70 可以实施为各种处理装置中的一个或多个，例如协处理器、微处理器、控制器、数字信号处理器 (DSP)、具有或不具有随附 DSP 的处理电路，或者包括集成电路的各种其他处理装置，诸如 ASIC( 特定应用集成电路 )、FPGA( 现场可编程门阵列 )、微控制器单元 (MCU)、硬件加速器、专用计算机芯片等。在示例实施例中，处理器 70 可以被配置来执行存储于存储器装置 76 中的或者处理器 70 以其他方式可访问的指令。这样，无论是通过硬件或是软件方法或者通过它们的组合来配置，处理器 70 均可以代表当被相应配置时能够根据本发明实施例执行操作的实体 ( 例如，被物理地实施于电路中 )。因此，例如，当处理器 70 被实施为 ASIC、FPGA 等时，处理器 70 可以是用于实施本文所描述的操作的专门配置的硬件。可替换地，作为另一示例，当处理器 70 被实施为软件指令的执行器时，指令可以专门配置处理器 70 以在指令被执行时执行本文描述的算法和操作。然而，在某些情况下，处理器 70 可以是特定装置 ( 例如，移动终端或网络装置 ) 的处理器，适于通过处理器 70 被用于执行本文所描述的算法和操作的指令进

一步配置而使用本发明的实施例。除了其他方面之外，处理器 70 还可以包括被配置来支持处理器 70 的操作的时钟、算术逻辑单元 (ALU) 和逻辑门。

[0038] 在示例实施例中，处理器 70 可以被配置来操作连接性程序，例如浏览器，Web 浏览器等。就此方面而言，连接性程序可以使得设备 50 例如根据无线应用协议 (WAP) 发射和接收 Web 内容，例如基于位置的内容或任何其它合适的内容。

[0039] 同时，通信接口 74 可以是任何装置，例如以硬件、计算机程序产品或者硬件和软件的组合来实施的装置或电路，被配置来从网络和 / 或与设备 50 通信的任何其它装置或模块接收数据和 / 或向它们发送数据。就此方面而言，通信接口 74 可以包括例如天线（或多个天线）和支持硬件和 / 或软件，用于使得能够与无线通信网络（例如，网络 30) 通信。在固定环境中，通信接口 74 可以替换地或者还支持有线通信。这样，通信接口 74 可以包括通信调制解调器和 / 或其他硬件 / 软件，用于支持经由电缆、数字用户线 (DSL)、通用串行总线 (USB)、以太网或其他机制的通信。

[0040] 可选用户接口 67 可以与处理器 70 通信以接收在用户接口 67 处用户输入的指示和 / 或向用户提供可听、可视、机械或其他输出。这样，用户接口 67 可以包括例如键盘，鼠标，操纵杆，显示器，触摸屏，麦克风，扬声器或其他输入 / 输出机制。在示例实施例中，其中该设备被实施为服务器或某些其他网络装置，用户接口 67 可以受限、远程定位、或消除。处理器 70 可以包括用户接口电路，其被配置成控制诸如例如扬声器、振铃器、麦克风、显示器和 / 或类似物之类的用户接口中的一个或多个元件的至少一些功能。处理器 70 和 / 或包括处理器 70 的用户接口电路可以被配置成通过存储在处理器 70 可访问的存储器（例如，存储器设备 76，和 / 或类似物）中的计算机程序指令（例如，软件和 / 或固件）控制用户接口的一个或多个元件的一个或多个功能。

[0041] 在示例实施例中，处理器 70 可以被实施为、包括或者以其他方式控制算法移除模块。算法移除模块 78 可以是任何装置，例如按照软件操作或者以硬件或者硬件和软件的组合来实施的装置或电路（例如，在软件控制下操作的处理器 70，实施为专门被配置成执行本文描述操作的 ASIC 或 FPGA 的处理器 70，或者它们的组合），从而配置该装置或电路来执行算法移除模块 78 的对应功能，如下所述。因此，在使用软件的示例中，执行该软件的装置或电路（例如，在一个示例中为处理器 70) 形成与此类装置相关联的结构。

[0042] 在示例实施例中，算法移除模块 78 可以与网络装置（例如，图 3 的网络装置 90) 通信，并且可以向网络装置提供设备 50 所支持以及所使用的算法的指示（例如，列表）。响应于指示的接收，网络装置可以确定设备 50 所使用的算法的任何算法是否是弱算法（例如，较不安全的算法）。在网络装置识别设备 50 的一个或多个弱算法的情形中，网络装置可以向算法移除模块 78 发送消息以指示算法移除模块 78 移除或禁用该弱算法。响应于从网络装置接收到该消息，（例如，该消息可以是特定挑战序列的形式作为被禁用算法的输入，输出被解码为移除消息），设备移除模块 78 可以移除或禁用设备 50 的弱算法。就此方面而言，如下面更充分描述的那样，设备 50 可以利用被网络装置指定的强算法（例如，更安全的算法）。

[0043] 设备 50 可以进一步包括可选 UIM 38。UIM 38 可以包括存储器装置（例如，UIM 存储器 52)、处理器（例如 UIM 处理器 54) 以及被配置来与处理器 70 或其他装置通信的接口 51。UIM 38 可以是智能卡的一种示例，例如可以包括用户识别模块 (SIM)、集成电路

卡 (ICC)、通用集成电路卡 (UICC)、通用用户识别模块 (USIM) 或者可移除用户识别模块 (R-UIM)。当 UIM 38 是 R-UIM 时，UIM 38 可以从设备 50 可移除。在一个示例实施例中，在 GSM 和 UMTS 应用的上下文中，例如，当 UIM 38 是 UICC 时，UICC 可以包括用户识别模块 (SIM) 应用、通用 SIM(USIM) 应用、因特网协议多媒体服务识别模块 (ISIM) 应用等，用于访问对应的公共陆地移动网络 (PLMN)，但是应该理解的是，一个或多个这些应用也可被用来访问一个或多个其他网络。

[0044] UIM 38 的存储器 52 可以存储与移动订户和任何其他适当数据相关的信息单元。例如，UIM 38 的存储器可以存储与移动订户相关的信息单元（例如，PIN 码）和 / 或用于向网络运营商和 / 或设备 50 验证移动订户。就此方面而言，UIM 38 的内容可以是不可访问的直到移动订户被验证为止。

[0045] 附加地，UIM 38 可以存储应用（例如，算法）以及在一些情况中 UIM38 的处理器 54 可以执行应用并且发出命令或者对命令进行响应。在一个示例实施例中，UIM 38 的处理器 54 可以执行类似于本文描述的算法移除模块 78 的功能，以移除或禁用可能存储在 UIM 存储器 52 或另一存储器（例如，存储器装置 76）中的一个或多个弱算法。

[0046] 例如，在示例实施例中，UIM 38 的处理器 54 可以与网络装置（例如，图 3 的网络装置 90）通信并且可以向网络装置提供 UIM 38 所支持以及所使用的算法的指示（例如，列表）。响应于指示的接收，网络装置可以确定由网络装置支持的由 UIM 38 所使用的算法中的任何算法是否是弱算法。网络装置可以向 UIM 38 的处理器 54 发送消息以指示处理器 54 移除或禁用该弱算法。响应于从网络装置接收到该消息，处理器 54 可以移除或禁用 UIM 38 的弱算法。就此方面而言，UIM 38 的处理器 54 可以利用被网络装置指定的强算法以便于与网络装置的通信。

[0047] 现在参见图 3，提供了根据示例实施例的网络装置的框图。如图 3 所示，网络装置 90（例如，服务器，基站，接入点 (AP)（例如，WLAN AP 或 WiFi AP)) 可以包括处理器 94、存储器 96、用户输入接口 95、通信接口 98 和算法移除管理器 97。存储器 96 可包括易失性和 / 或非易失性存储器，并且可以存储内容、数据和 / 或类似物。存储器 96 可以存储客户端应用（例如，算法）、指令、和 / 或类似物以供处理器 94 来执行网络装置 90 的各种操作。存储器 96 可以是有形非临时装置。

[0048] 处理器 94 可以以许多不同的方式来实施。例如，处理器 94 可以实施为各种处理装置中的一个或多个，例如协处理器、微处理器、控制器、DSP，具有或不具有随附 DSP 的处理电路，或者包括集成电路的各种其他处理装置，其中集成电路例如 ASIC、FPGA、MCU、硬件加速器、专用计算机芯片等。在示例实施例中，处理器 94 可以被配置来执行存储于存储器 96 中的或者处理器 94 以其他方式可访问的指令。这样，无论是通过硬件或是软件方法或者通过它们的组合来配置，处理器 94 均可以代表当被相应配置时能够根据本发明实施例执行操作的实体（例如，被物理地实施于电路中）。因此，例如，当处理器 94 被实施为 ASIC、FPGA 等时，处理器 94 可以是用于实施本文所描述的操作的专门配置的硬件。

[0049] 可替换地，作为另一示例，当处理器 94 被实施为软件指令的执行器时，指令可以专门配置处理器 94 以在指令被执行时执行本文描述的算法和操作。然而，在某些情况下，处理器 94 可以是特定装置（例如，移动终端或网络装置）的处理器，适于通过处理器 94 的进一步配置通过用于执行本文所描述的算法和操作的指令而使用本发明的实施例。除了其

他方面之外，处理器 94 还可以包括被配置来支持处理器 94 的操作的时钟、算术逻辑单元 (ALU) 和逻辑门。

[0050] 处理器 94 还可以被连接到通信接口 98 或其它装置以用于显示、发送和 / 或接收数据、内容、和 / 或类似物。所述用户输入接口 95 可以包括允许网络实体从用户接收数据的许多装置中的任何装置，诸如小键盘、触摸显示器、游戏杆或其他输入设备。就此方面而言，处理器 94 可以包括被配置来控制用户输入接口的一个或多个元件中的至少一些功能的用户接口电路。处理器和 / 或处理器的用户接口电路可以被配置成通过存储在处理器可访问的存储器（例如，易失性存储器、非易失性存储器和 / 或类似物）中的计算机程序指令（例如，软件和 / 或固件）来控制用户接口的一个或多个元件的一个或多个功能。

[0051] 在示例实施例中，处理器 94 可以被实施为、包括或者以其他方式控制算法移除模块 97。算法移除模块 97 可以是任何装置，例如按照软件操作或者以硬件或者硬件和软件的结合来实施的装置或电路（例如，在软件控制下操作的处理器 94，实施为专门被配置成执行本文描述操作的 ASIC 或 FPGA 的处理器 94，或者它们的组合），从而配置该装置或电路来执行冲突管理器 97 的对应功能，如下所述。因此，在使用软件的示例中，执行该软件的装置或电路（例如，在一个示例中为处理器 94）形成与此类装置相关联的结构。

[0052] 算法移除模块 97 可以接收设备 50 使用的一个或多个算法的指示（例如，列表）。在示例实施例中，算法移除模块 97 可以周期性地（例如，在设备 50 注册到网络 30 的情形中，每天、每周、每月）接收设备 50 使用的算法的指示。响应于指示的接收，算法移除模块 97 可以分析该算法并且可以确定算法中的任何算法是否为弱算法（例如，较不安全的算法（例如，过时或陈旧的算法））。算法移除模块 97 还可以确定算法中的任何算法是否为网络装置 90 支持的强算法。算法移除模块 97 可以向设备 50 发送消息，指示 UIM 38 的模块 78 或处理器 54 禁用或移除弱算法，并且可以指示 UIM38 的算法移除模块 78 或 UIM 38 的处理器 54 执行网络装置支持的、算法移除模块 97 确定为强算法的算法。可替换地，算法移除模块 97 可以指示 UIM 38 的算法移除模块 78 或 UIM 38 的处理器 54 执行强算法，并且代替移除弱算法，算法移除模块 97 可以指示 UIM 38 的算法移除模块 78 或处理器 54 更新弱算法以便基于算法移除模块 97 发送给设备 50 的数据产生较强算法。

[0053] 现在参见图 4，提供了网络实体的示例实施例的框图。如图 4 所示，网络实体 100（本文也称为管理网络装置 100）（例如，管理服务器）可以包括处理器 104、和存储器 106。存储器 106 可以包括易失性和 / 或非易失性存储器，并且可以存储内容、数据和 / 或类似物。存储器 106 可以存储客户端应用（例如，算法）、指令、和 / 或类似物，以供处理器 94 来执行网络实体的各种操作。存储器 106 可以是有形非临时装置。

[0054] 处理器 104 还可以被连接到通信接口 107 或其它装置以用于显示、发射和 / 或接收数据、内容、和 / 或类似物。所述用户输入接口 105 可以包括允许网络实体 100 从用户接收数据的许多装置中的任何装置，诸如小键盘、触摸显示器、游戏杆或其他输入设备。就此方面而言，处理器 104 可以包括被配置来控制用户输入接口的一个或多个元件中的至少一些功能的用户接口电路。处理器和 / 或处理器的用户接口电路可以被配置成通过存储在处理器可访问的存储器（例如，易失性存储器、非易失性存储器和 / 或类似物）中的计算机程序指令（例如，软件和 / 或固件）控制用户接口的一个或多个元件的一个或多个功能。

[0055] 网络实体 100 可以从网络装置 90 接收指定由一个或多个设备 50 使用的一个或多

个算法的数据。响应于指示的接收，网络实体的处理器 104 可以确定算法中的任何一个是否是弱的。在处理器 104 确定一个或多个算法为弱算法的情形中，处理器 104 可以向设备 50 发送消息，该消息包括指示设备 50 移除或禁用弱算法的数据。该消息还可以包括指示设备执行网络实体和该设备 50 支持的强算法的数据。

[0056] 现在参考图 5，根据示例实施例的系统图被提供。系统 7 可以包括通信装置 163，165 和 167（例如，设备 50），网络装置 108（例如，网络装置 90），接入点 110（例如，网络装置 90），和管理网络装置 112（例如，网络实体 100）。尽管图 5 示出系统 7 包括三个通信装置 163，165，167，一个网络装置 108，一个接入点 110 和一个管理网络装置 112，但是应当指出，系统 7 可以包括任何合适数目的通信设备 163，165，167，网络装置 108，接入点 110 和网络管理装置 112，而不脱离本发明的精神和范围。

[0057] 在一个示例实施例中，网络装置 108 可以从通信装置（例如通信装置 163）接收指示由该通信装置利用的算法的指示。网络装置 108 可以分析该算法并且可以确定算法中的任何算法是否为弱算法（例如，该安全性算法易受攻击）。响应于识别一个或多个弱算法，网络装置 108 可以向通信装置发送消息，指示通信装置禁用或移除该弱算法并且执行网络装置和通信装置支持的强算法，如下面更充分描述的那样。在示例实施例中，在弱算法被通信装置禁用但未被移除的情形中，在通信装置执行强算法（例如，以便与网络装置交换数据）的同时网络装置 108 可以将弱算法更新为更安全的。

[0058] 在一个示例实施例中，网络装置 108 可以远程禁用被盗通信装置（例如通信装置 165）上的算法。就此方面而言，网络装置 108 可以禁用或移除被盗通信装置上的所有算法。

[0059] 网络装置 108 可以基于通信装置的用户 / 订户报告通信装置被盗来确定通信装置被盗。可替换地，网络装置 108 可以基于检测到通信装置的异常行为（例如检测到在国外针对服务的过度金融收费）确定通信装置被盗。

[0060] 在另一示例实施例中，响应于从通信装置（例如通信装置 163）接收到指示由通信装置利用的算法的指示，网络装置 108 可以向管理网络装置 112 发送请求，从而识别算法。该请求可以包括请求管理网络装置 112 确定算法中的任何一个是否为弱的数据。响应于确定算法中的一个或多个为弱，管理网络装置 112 可以指示通信装置禁用或移除弱算法。就此方面而言，通信装置（例如通信装置 163）可以不必需要在通信装置处用于禁用或移除算法的用户交互。管理网络装置 112 还可以指示通信装置（例如通信装置 163）执行管理网络装置 112 支持的强算法——通信装置在向网络装置 108 提供指示（例如列表）时指示它也支持该算法。

[0061] 在备选示例实施例中，接入点 110（例如，WLAN AP）可以执行安全性扫描，并且响应于该安全性扫描，接入点 110 可以从通信装置（例如通信装置 163）接收通信装置利用和支持的算法的指示。响应于指示的接收，接入点 110 可以，但是不是必需，向管理网络装置 112 发送请求从而识别算法，并且该请求可以包括请求管理网络装置 112 确定算法中的任何一个是否为弱的信息。在管理网络装置 112 确定算法中的一个或多个为弱的情形中，管理网络装置 112 可以指示通信装置禁用或移除弱算法。管理网络装置 112 还可以指示通信装置执行管理网络装置 112 和通信装置支持的强算法。强算法可以是通信装置在响应于安全性扫描与接入点 110 通信时指示它也支持的算法之一。

[0062] 现在参见图 6，提供了从通信装置禁用或移除算法的示例方法的流程图。在操作

600 处，通信装置（例如，通信装置 163）可以向网络装置（例如网络装置 108）发送由通信装置利用的支持算法（例如，安全性算法（例如，加密算法））的指示（例如，列表）。网络装置可以确定算法中的一个或多个是否为弱，如下面更充分说明的那样。网络装置还可以确定算法中的一个或多个为强。

[0063] 在操作 605 处，网络装置可以经由通信信道向通信装置提供消息，指示通信装置使用检测到的强算法用于促进与网络装置的通信。强算法（例如更安全的算法）可以是被指示为通信装置支持的算法之一。就此方面而言，网络装置可以指示通信装置执行该强算法。在操作 610 处，网络装置可以触发或请求通信装置针对安全检查而联络网络装置。响应于请求的接收，通信装置可以向网络装置提供用于通信装置支持的算法的安全性协议（例如，算法列表）。网络装置可以分析算法的安全性协议并且可以确定对应的算法是强还是弱。

[0064] 可替换地，网络装置可以基于分析接收到的通信装置所支持的算法的指示（例如，算法的列表）来确定弱算法，并且可以向通信装置发出远程命令以禁用检测到的弱算法。命令可以例如用长的共享秘密密钥（例如，长密码）或基于公钥基础设施 (PKI) 而被强认证，并且该命令的完整性可被保护。由网络装置提供给通信装置的远程命令可以指示一个或多个弱算法。

[0065] 在一个示例实施例中，网络装置的算法移除管理器（例如，算法移除管理器 97）可以（例如远程地）更新通信装置使用的弱算法。在备选示例实施例中，网络装置可以请求管理网络装置（例如管理网络装置 112）从通信装置移除或禁用弱算法或者更新通信装置的弱算法。

[0066] 响应于接收到命令，通信装置的 UIM 的处理器（例如处理器 54）或算法移除模块（例如，算法移除模块 78）可以验证命令的安全性和正确性。通信装置的 UIM 的处理器或算法移除模块可以部分地基于被用于与网络装置的安全性认证的共享秘密密钥或公共密钥来确定命令的安全性。通信装置可以分析昭示被允许向通信装置发送远程命令的操作者的文件。在通信装置确定命令不是从文件中识别的获准操作者接收来的情形中，通信装置可以确定命令是不安全的或者未被认证的。文件可以被存储在通信装置的存储器（例如，存储器装置 76）中或者通信装置的 UIM（例如，存储在 UIM 存储器 52 中）中。

[0067] 在操作 615 处，通信装置可以检查通信装置为了不同目的所支持的算法。例如，装置支持的一些算法可以被用于无线电安全性，并且另一些算法可以被用于其他目的，例如浏览器安全性。举例来说，在启动浏览器的情形中，浏览器安全性算法可以被通信装置执行。无线电安全性和浏览器安全性算法是示例，并且据此通信装置可以针对其他目的（例如，认证）检查并利用任何其他适当的算法。

[0068] 在操作 620 处，被网络装置识别的（例如，在命令中指出的）弱算法可以从通信装置所支持的算法（例如，从所支持的算法列表）中移除或禁用。在示例实施例中，在存在至少一个强算法可被通信装置使用的情形中，网络装置可以指示通信装置禁用 / 移除弱算法。在一个示例实施例中，在通信装置当前仅支持弱算法的情形中，弱算法可以不被禁用或移除，以允许通信装置使用该弱算法用于与网络装置通信。

[0069] 在备选示例实施例中，弱算法可以不必被移除或禁用。替换地，网络装置可以给弱算法放置一些条件（例如，一个条件为仅针对 WLAN 通信使用弱算法）。

[0070] 在一些示例实施例中，被确定为弱的算法可能是以硬件来实现的。如此，以硬件实现的算法可能（例如通过软件）不是容易移除或者不是容易更新的。就此方面而言，网络装置可以向通信装置发送标志以指定以硬件实现的算法应该被启用还是被禁用。该标志可以包括用于标注该算法应被启用还是禁用的位。响应于接收到该标志，通信装置可以将标志位存储在存储器（例如，存储器装置 76，UIM 存储器 52）中。

[0071] 可选地，在操作 625 处，通信装置可以向网络装置发送确认消息，从而确认弱算法被从通信装置中移除或禁用了。附加地或者替换地，在后续时刻，网络装置可以向通信装置发送消息以检查弱算法是否被禁用或移除。就此方面而言，通信装置可以告知网络装置通信装置可以使用的强算法并且由于没有弱算法被识别，所以网络装置可以确定弱算法被禁用或移除。

[0072] 在备选示例实施例中，一个或多个算法可以通过执行自去激活，而禁用或移除它们本身。就此方面而言，算法（例如，认证算法）可以具有基于输入和密钥（例如，共享密钥）的确定的输出。代替网络装置发送具有固定序列的命令以从通信装置中移除整个算法，网络装置可以发送由要与相应密钥（例如，共享密钥）一起在通信装置中使用的输入挑战（例如，输入数据（例如，认证输入数据））组成的消息，其可以触发算法产生一个或多个序列输出值。响应于算法移除模块或 UIM 处理器执行算法（例如，弱算法），算法可以检测输出值并且可以确定输出值表示禁用或移除算法。在此方面，响应于检测到该输出值，算法可以移除或禁用它本身。

[0073] 标注或表示算法应被移除或禁用的输出值可以在算法的执行环境中被（例如由通信装置）预配置。在示例实施例中，在已经出现预定义数目的连续输出值的情形中，算法可以自动地禁用它本身。预确定数目的连续输出值可能响应于使用与用于计算输出的算法相关的密钥执行从网络装置接收到的输入而出现。网络装置可以确保输出值在正常操作期间以连续序列出现的概率保持很低，以避免在正常操作中触发此操作发生。换言之，序列不得不具有在正常操作期间统计学上出现的较低概率。被 UIM 的 UIM 处理器或算法移除模块执行且算法可以确定算法是否将要被禁用 / 移除的模式可以变化。

[0074] 为了说明的目的而非限制，代替若干连续输出值以检测算法是否应被禁用 / 移除，作为示例，可以使用两个连续值之后随有一个（或另一特定数量的）随机值之后再随有预定义值，来确定算法是否应被禁用。在此示例中，被执行的算法可以分析以特定顺序出现的三个定义值。在备选示例实施例中，被 UIM 的 UIM 处理器或算法移除模块执行的算法可以分析任何适当顺序的输出值（例如，连续输出值）而不分析定义顺序。例如，在有两个连续预定义输出值的情形中，若干随机值可以跟随预定义值之一，该预定义值之后可以随有一个或多个随机值，该随机值之后可以随有预定义值中的另一个。就此方面而言，输出值可以包括交织的预确定值和随机值的序列。如此，示例实施例可以允许要被使用的输出值的任何适当的变形或组合。

[0075] 该方法的一个益处是输出值可以作为正常验证值被返回（例如，认证验证值）给网络装置。就此方面而言，网络装置（例如，网络装置 108）可以能够基于通过相应的通信装置（例如，通信装置 163）而被提供给网络装置的返回值和返回值序列，来确定算法已经被禁用或移除的情形。基于外部地观察算法，该方法可以允许禁用算法看起来像正常操作（例如，正常认证处理）。据此，窃听者无法区分正常认证处理或禁用算法处理。

[0076] 在一个示例实施例中，禁用算法的自去激活方法还可以针对证书而被使用。就此方面而言，通信装置的UIM的算法UIM处理器或移除模块可以检查已被验证的证书序列。例如，通信装置可以具有多个预先存储的证书或者共享的秘密密钥，其可以担当装置证书或操作者证书（例如，为了认证或认证的目的），并且每个证书可以签署／绑定用于某个算法的密钥。在其中相应算法被确定为弱的情形中，证书可以被禁用或移除，而不是算法被禁用或移除。替换地，作为被禁用的算法的一部分，被确定为弱算法的证书可以被禁用或移除。

[0077] 系统7可以允许利用不同方法来禁用或移除一个或多个算法。例如，如上所述，一种方法可以针对一个或多个算法定义“固定的输入”，在其中，可以有针对系统7的相应通信装置（例如，通信装置163、165、167）预先配置的特定输出。算法的输出可以取决于与来自网络装置（例如，网络装置108）的输入挑战（例如，认证输入数据）一起使用的密钥。另一方法可以针对算法利用“固定的输出”来确定算法是否应被禁用或移除。就此方面而言，每个通信装置可以要求特定的输入挑战集合（例如，认证输入）以禁用或移除算法。备选示例实施例可以允许在一个方案中结合“固定的输入”和“固定的输出”方法。

[0078] 就此方面而言，一个或多个禁用序列值（在本文中也被称为响应值）可以由通信装置的算法（例如，弱算法）提供给网络装置。网络装置可以分析禁用序列值以确定该算法被禁用或移除。禁用序列值可以不必到达网络装置（例如，验证实体）并且因此即使未从通信装置的相应算法收到任何响应，算法（例如，弱算法）也可以被禁用。禁用序列值可以在可能失败的下一认证运行处被网络装置检测到。在一个示例实施例中，通过利用固定的已知密钥或者通过产生未被认为有效输出的固定输出，被禁用的算法仍然可以向网络装置提供响应。在认证输入可以不到达网络装置的情形中，下一认证值的接收可以重置检测方案以使得禁用序列能够被启动。认证值是当算法仍然充分起作用时网络装置可以期待的值。如此，网络装置可以知晓算法让人处于操作中，因此此返回值代表使用相应密钥和应该已被移除的算法的对输入挑战的有效响应。

[0079] 现在参见图7，提供了用于禁用或移除一个或多个弱算法的流程图的示例实施例。在操作700处，网络装置（例如，网络装置108（例如，网络装置90））可以包括用于接收由通信装置（例如，通信装置163（例如设备50））利用的一个或多个算法的指示的装置，诸如算法移除管理器97、处理器94和／或类似物。在操作705处，网络装置可以包括用于确定一个或多个算法是否被识别为弱算法的装置，诸如算法移除管理器97、处理器94和／或类似物。在一个示例实施例中，弱算法可以是相对于强算法而言较不安全的算法。在操作715处，网络装置可以包括用于使能向通信装置提供消息以指示通信装置移除、禁用算法中的至少一个检测到的弱算法或指派至少一个条件给该检测到的弱算法的装置，诸如算法移除管理器97、处理器94和／或类似物。

[0080] 应当指出，图6和图7是根据本发明的示例实施例的系统、方法和计算机程序产品的流程图。应当理解：流程图的每个块以及流程图中的块组合可以通过各种手段来实现，例如硬件、固件和／或包括一个或多个计算机程序指令的计算机程序产品。例如，上述程序中的一个或多个可以由计算机程序指令来实施。就此方面而言，在示例实施例中，实施上述程序的计算机程序指令由存储器装置（例如，存储器装置76、存储器96、存储器106）来存储并由处理器（例如，处理器70、处理器94、处理器104、算法移除模块78、算法移除管理器97）来执行。正如应该理解的那样，任何此类计算机程序指令可以被加载至计算机或其他可

编程设备（例如硬件）上以制造机器，以使在计算机或其他可编程设备上执行的指令使得在流程图块中规定的功能得以实现。在一个实施例中，计算机程序指令被存储在计算机可读存储器中，其可以引导计算机或其他可编程设备按照特定方式工作，以使存储于计算机可读存储器中的指令产生包括指令的制品，该指令实现流程图块中规定的功能。计算机程序指令还可以被加载至计算机或其他可编程设备上以使得一系列操作在计算机或其他可编程设备上被执行以便产生计算机实现的过程，从而使得在计算机或其他可编程设备上执行的指令实现流程图块中规定的功能。

[0081] 据此，流程图的块支持用于执行指定功能的装置的组合。还应理解，流程图的一个或多个块以及流程图中的块的组合可以通过执行特定功能的以专用硬件为基础的计算机系统、或专用硬件与计算机指令的结合来实现。

[0082] 在示例实施例中，用于执行图 6 和图 7 的方法的设备可以包括被配置来执行上述的一些操作或每一个操作 (600-625、700-715) 的处理器（例如处理器 70、处理器 94、处理器 104、算法移除模块 78、算法移除模管理器 97）。通过执行硬件实现的逻辑功能、执行存储的指令、或者执行用于执行每个操作的算法，处理器例如可以被配置来执行操作 (600-625、700-715)。替换地，设备可以包括用于执行上述每个操作的装置。就此方面而言，根据示例实施例，用于执行操作 (600-625、700-715) 的装置示例例如可以包括处理器 70（例如，作为用于执行上述任何操作的装置），处理器 94、处理器 104、算法移除模块 78、算法移除管理器 97 和 / 或用于执行指令或执行用于处理信息的算法的装置或电路，如上所述。

[0083] 本领域技术人员从本发明相关的前文详细说明和附图中呈现的教导获益，将显然易知在此处阐明的本发明的许多修改和其它实施例。因此，应该理解本发明并不局限于所公开的特定实施例，修改和其它实施例意图包括在随附的权利要求的范围内。此外，虽然前文详细说明和相关联的附图描述在元件和 / 或功能的某些示例组合的上下文中的示例实施例，但是应该理解不偏离随附的权利要求范围可以由替代实施例提供元件和 / 或功能的不同组合。例如，就此方面而言，与上面明确描述的不同的元件和 / 或功能的不同组合也被预期可以阐明在随附的权利要求范围的部分中。虽然此处使用特定术语，但是仅以通用和描述性意义使用而非限制性目的。

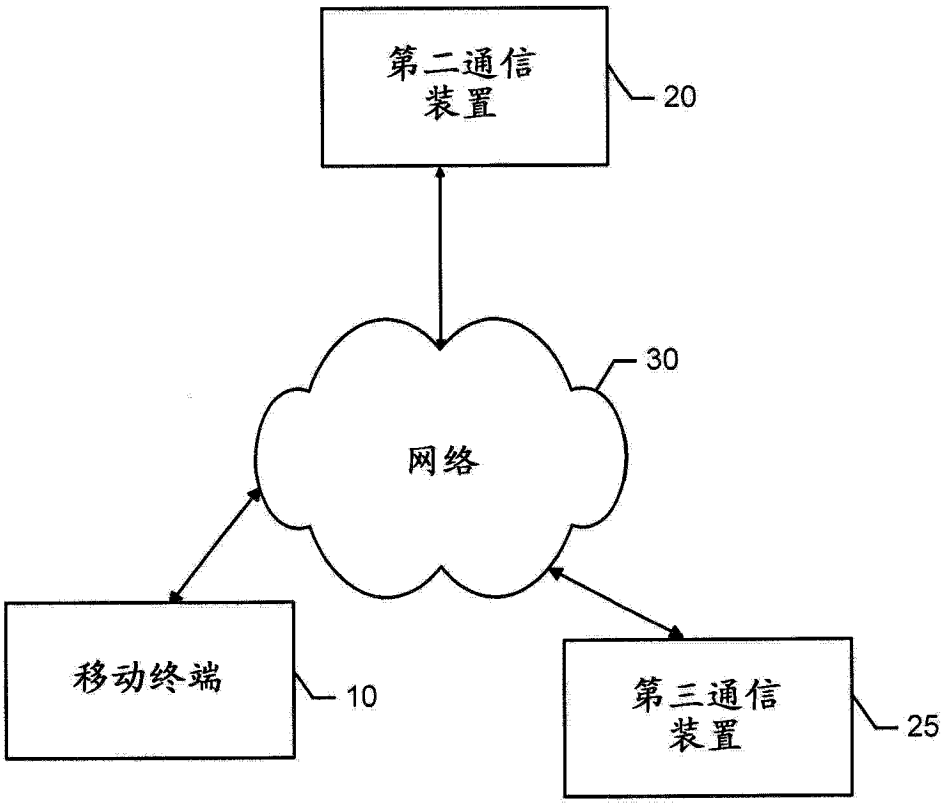



图 1

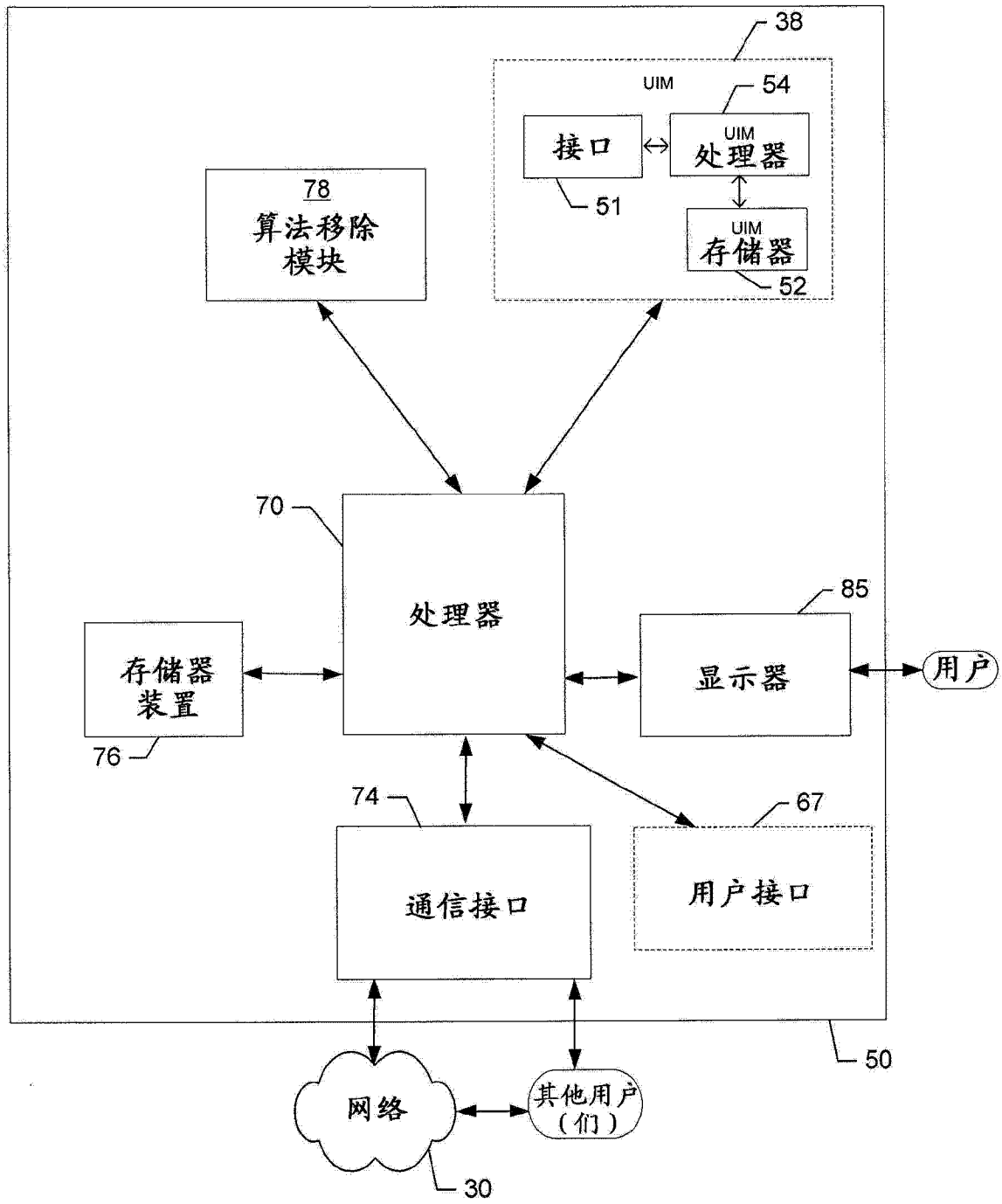

38
UIM
54
接口
UIM
处理器
51
UIM
存储器
52
78
算法移除
模块
70
处理器
85
存储器
装置
显示器
用户
76
74
67
通信接口
用户接口
50
网络
其他用户
(们)
30

图 2

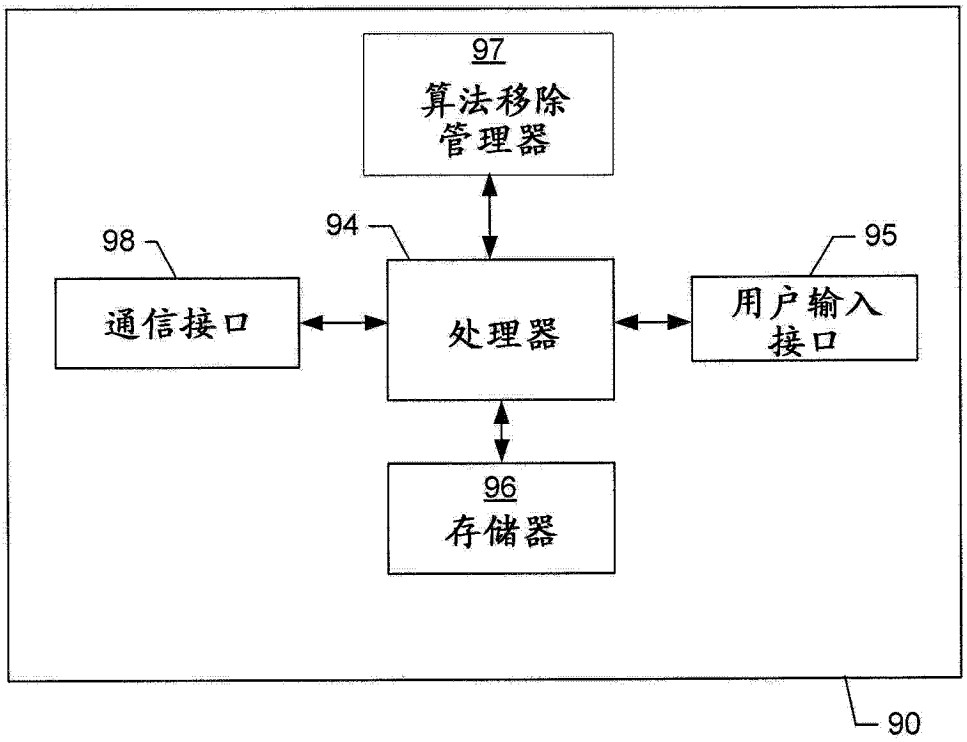

97
算法移除管理器
94
98
95
通信接口
处理器
用户输入接口
96
存储器
90

图 3

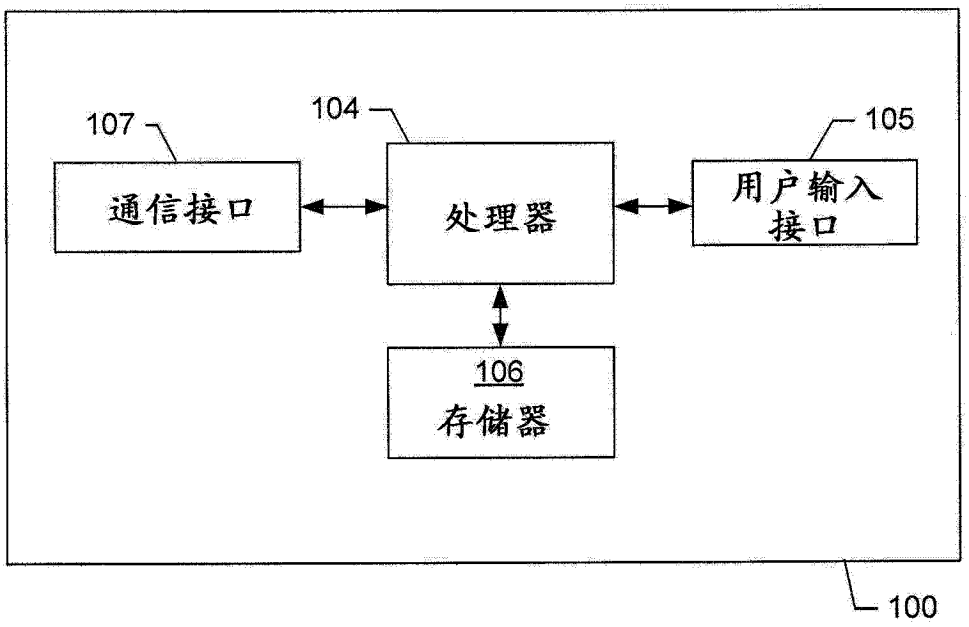

104
107
105
通信接口
处理器
用户输入接口
106
存储器
100

图 4

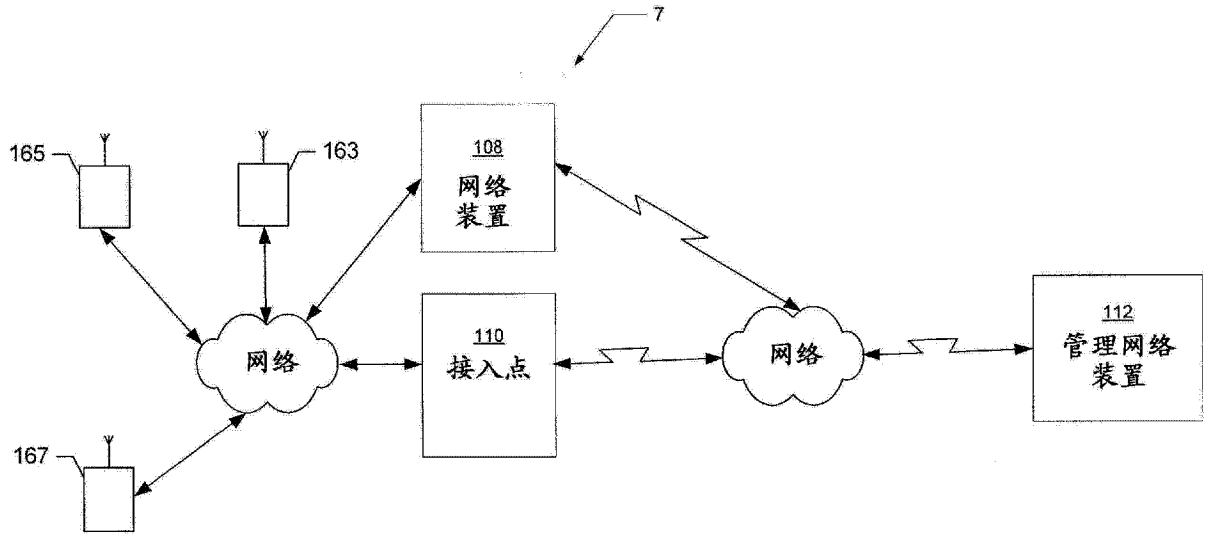



图 5

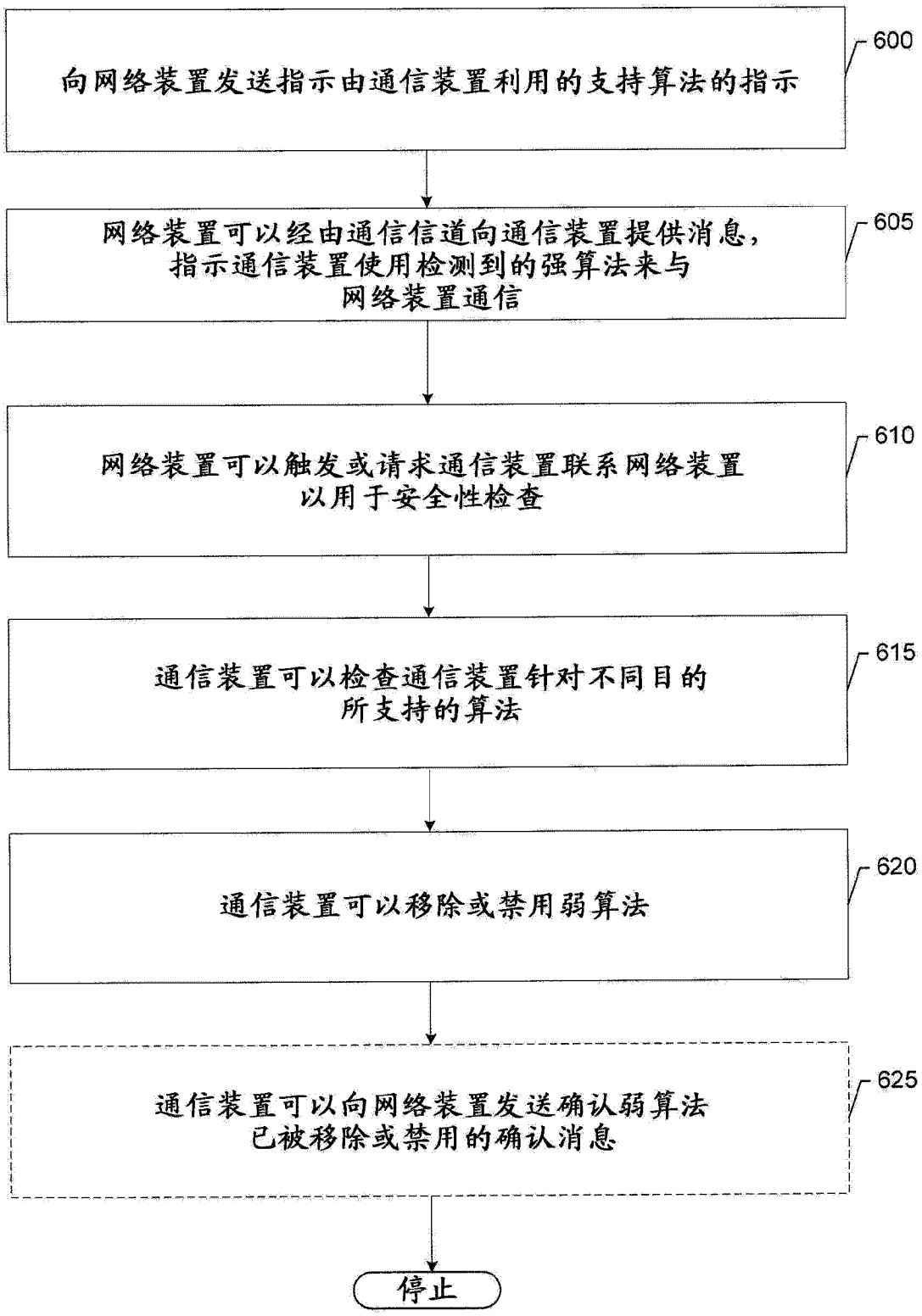

向网络装置发送指示由通信装置利用的支持算法的指示
600
网络装置可以经由通信信道向通信装置提供消息，指示通信装置使用检测到的强算法来与网络装置通信
605
网络装置可以触发或请求通信装置联系网络装置以用于安全性检查
610
通信装置可以检查通信装置针对不同目的所支持的算法
615
通信装置可以移除或禁用弱算法
620
通信装置可以向网络装置发送确认弱算法已被移除或禁用的确认消息
625
停止

图 6

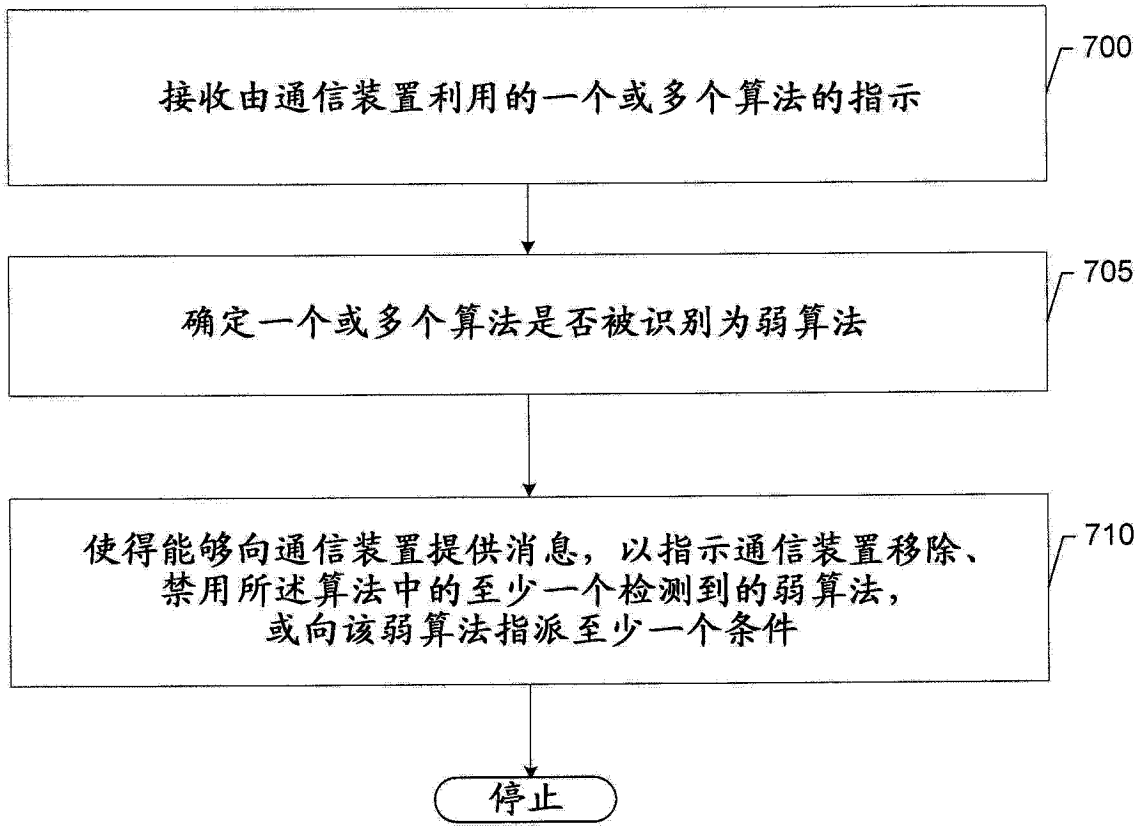

接收由通信装置利用的一个或多个算法的指示
700
确定一个或多个算法是否被识别为弱算法
705
使得能够向通信装置提供消息，以指示通信装置移除、
禁用所述算法中的至少一个检测到的弱算法，
或向该弱算法指派至少一个条件
710
停止

图 7