



(12) 发明专利

(10) 授权公告号 CN 107683596 B

(45) 授权公告日 2021.05.11

(21) 申请号 201580080901.9

(22) 申请日 2015.12.18

(65) 同一申请的已公布的文献号  
申请公布号 CN 107683596 A

(43) 申请公布日 2018.02.09

(30) 优先权数据  
62/146613 2015.04.13 US

(85) PCT国际申请进入国家阶段日  
2017.12.13

(86) PCT国际申请的申请数据  
PCT/EP2015/080499 2015.12.18

(87) PCT国际申请的公布数据  
W02016/165792 EN 2016.10.20

(73) 专利权人 瑞典爱立信有限公司

地址 瑞典斯德哥尔摩

(72) 发明人 M.维夫韦松 V.莱托维尔塔  
K.普费弗 V.托维南

(74) 专利代理机构 中国专利代理(香港)有限公司 72001

代理人 姜冰 杨美灵

(51) Int.Cl.  
H04L 29/06 (2006.01)  
H04W 12/069 (2021.01)  
H04W 8/00 (2009.01)  
H04W 48/16 (2009.01)

审查员 周天豪

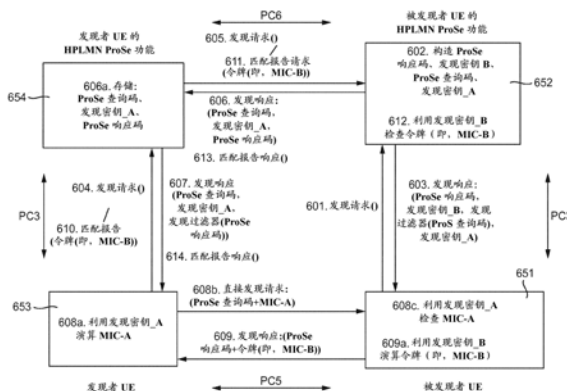
权利要求书3页 说明书17页 附图20页

(54) 发明名称

用于末端装置发现另一个末端装置的方法和设备

(57) 摘要

公开一种由邻近服务服务器执行的方法。该方法包括：生成ProSe查询码和ProSe响应码，至少将ProSe响应码与第一和第二发现密钥一起发送给第一末端装置，以及至少将第一发现密钥和ProSe查询码发送给第二末端装置，使得第二末端装置能够通过空中接口安全地发现第一末端装置。



1. 一种由邻近服务服务器执行的方法,包括:  
生成ProSe查询码和ProSe响应码,  
至少将所述ProSe响应码与第一和第二发现密钥一起发送给第一末端装置,以及  
至少将所述第一发现密钥和所述ProSe查询码发送给第二末端装置,  
使得所述第二末端装置能够通过空中接口安全地发现所述第一末端装置。
2. 根据权利要求1所述的方法,还包括:作为预备步骤,生成所述第一发现密钥和所述第二发现密钥。
3. 根据权利要求1所述的方法,还包括:作为预备步骤,从密钥管理服务器接收所述第一和第二发现密钥。
4. 根据任一前述权利要求所述的方法,还包括:基于所述ProSe查询码生成发现过滤器,并将它发送给所述第一末端装置。
5. 根据权利要求1至3中任一权利要求所述的方法,还包括:从所述第二末端装置接收指示所述第二末端装置想要通过空中接口发现所述第一末端装置的发现请求,所述邻近服务服务器在此之后向所述第二末端装置发送所述第一发现密钥和ProSe查询码。
6. 根据权利要求5所述的方法,还包括:向所述第二末端装置与其进行通信的第二邻近服务服务器发送所述ProSe响应码。
7. 根据权利要求1至3中任一权利要求所述的方法,还包括:从所述第二末端装置接收包括所述ProSe响应码和基于所述第二发现密钥的令牌的匹配报告请求。
8. 根据权利要求7所述的方法,还包括利用所述第二发现密钥验证所述令牌。
9. 根据权利要求7所述的方法,如果所述令牌已验证,那么所述方法还包括向所述第二末端装置发送指示所述第一末端装置是真的匹配报告响应。
10. 根据权利要求1至3中任一权利要求所述的方法,还包括:向所述第二末端装置发送所述第二发现密钥,使得所述第二末端装置能够验证所述第一末端装置是真的。
11. 根据权利要求1至3中任一权利要求所述的方法,其中所述第二末端装置包括多个第二末端装置,使得所述方法还包括向每个第二末端装置发送所述ProSe查询码和所述第一发现密钥。
12. 一种服务器,包括:  
生成单元,用于生成ProSe查询码和ProSe响应码,  
传送单元,用于至少将所述ProSe响应码与第一和第二发现密钥一起发送给第一末端装置,以及至少将所述第一发现密钥和所述ProSe查询码发送给第二末端装置,使得所述第二末端装置能够通过空中接口安全地发现所述第一末端装置。
13. 一种包括处理器和存储器的服务器,所述存储器包含由所述处理器可执行的指令,使得网络节点可进行操作以实行根据权利要求1至11中任一权利要求所述的方法。
14. 一种由末端装置执行的方法,所述方法包括:  
从邻近服务服务器接收第一发现密钥、第二发现密钥和ProSe响应码,  
从想要发现所述末端装置的第二末端装置接收包括ProSe查询码和令牌的直接发现请求,  
利用所述第一发现密钥验证所述令牌。
15. 根据权利要求14所述的方法,还包括:所述末端装置从所述邻近服务服务器接收基

于ProSe查询码的发现过滤器。

16. 根据权利要求14或15所述的方法,其中所述末端装置通过空中接口接收所述ProSe查询码和所述令牌,并且所述令牌基于所述第一发现密钥。

17. 根据权利要求14或15所述的方法,如果所述末端装置验证了从所述第二末端装置接收的所述令牌,那么所述方法还包括向所述第二末端装置发送包括基于所述第二发现密钥的第二令牌的发现响应。

18. 根据权利要求14或15所述的方法,还包括:作为预备步骤,所述末端装置向它的邻近服务服务器发送发现请求,以便请求允许所述第二末端装置发现所述末端装置。

19. 一种末端装置,包括:

传送单元,用于从邻近服务服务器接收第一发现密钥、第二发现密钥和ProSe响应码,以及用于从想要发现所述末端装置的第二末端装置接收包括ProSe查询码和令牌的直接发现请求,

验证单元,用于利用所述第一发现密钥验证所述令牌。

20. 一种包括处理器和存储器的末端装置,所述存储器包含由所述处理器可执行的指令,使得网络节点可进行操作以便实行根据权利要求14至18中任一权利要求所述的方法。

21. 一种由邻近服务服务器执行的方法,所述方法包括:

从第二邻近服务服务器至少接收第一发现密钥、ProSe查询码和ProSe响应码,

基于所述ProSe响应码生成发现过滤器,并向第一末端装置发送所述发现过滤器、第一发现密钥和ProSe查询码,使得所述第一末端装置能够通过空中接口安全地发现第二末端装置。

22. 根据权利要求21所述的方法,还包括:从所述第一末端装置接收包括基于第二发现密钥的令牌的匹配报告请求,并将所述令牌转发给所述第二邻近服务服务器以便进行验证。

23. 根据权利要求22所述的方法,如果所述第二邻近服务服务器验证了所述令牌,那么所述方法还包括从所述第二邻近服务服务器接收指示所述第二末端装置是真的的响应。

24. 根据权利要求21所述的方法,还包括:所述邻近服务服务器从所述第二邻近服务服务器接收第二发现密钥,并将所述第二发现密钥发送给所述第一末端装置。

25. 根据权利要求21至24中任一权利要求所述的方法,还包括:作为预备步骤,所述邻近服务服务器从所述第一末端装置接收指示所述第一末端装置想要发现所述第二邻近服务服务器的所述第二末端装置地发现请求。

26. 根据权利要求25所述的方法,还包括向所述第二邻近服务服务器发送指示所述第一末端装置想要发现所述第二邻近服务服务器的所述第二末端装置地发现请求。

27. 一种服务器,包括:

传送单元,用于从第二邻近服务服务器至少接收第一发现密钥、ProSe查询码和ProSe响应码,

生成单元,用于基于所述ProSe响应码生成发现过滤器,并将所述发现过滤器、第一发现密钥和ProSe查询码发送给第一末端装置,使得所述第一末端装置能够通过空中接口安全地发现第二末端装置。

28. 一种包括处理器和存储器的服务器,所述存储器包含由所述处理器可执行的指令,

使得网络节点可进行操作以便实行根据权利要求21至26中任一权利要求所述的方法。

29. 一种由末端装置执行的方法,所述方法包括:

从邻近服务服务器接收ProSe查询码和第一发现密钥,  
向第二末端装置发送包括基于所述第一发现密钥的令牌是直接发现请求,以及  
从所述第二末端装置接收包括ProSe响应码和第二令牌的发现响应。

30. 根据权利要求29所述的方法,还包括从所述邻近服务服务器接收基于所述ProSe响应码的发现过滤器。

31. 根据权利要求30所述的方法,还包括:所述末端装置利用所述发现过滤器来标识从所述第二末端装置接收的所述ProSe响应码。

32. 根据权利要求29至31中任一权利要求所述的方法,还包括:所述末端装置将所述第二令牌转发给所述邻近服务服务器以便进行验证。

33. 根据权利要求32所述的方法,如果所述第二令牌已验证,那么所述方法还包括从所述邻近服务服务器接收指示所述第二末端装置是真的的消息。

34. 根据权利要求29至31中任一权利要求所述的方法,还包括:所述末端装置从所述邻近服务服务器接收第二发现密钥,并且所述末端装置利用所述第二发现密钥验证所述第二令牌,从而认证所述第二末端装置。

35. 根据权利要求29至31中任一权利要求所述的方法,还包括:作为预备步骤,向所述邻近服务服务器发送指示所述末端装置想要发现所述第二末端装置的发现请求。

36. 根据权利要求29至31中任一权利要求所述的方法,其中所述末端装置包括多个末端装置,使得所述方法还包括:每个末端装置接收相同的ProSe查询码和第一发现密钥,并向相同的第二末端装置发送直接发现请求,且从所述相同的第二末端装置接收直接发现响应。

37. 一种末端装置,包括:

传送单元,用于从邻近服务服务器接收ProSe查询码和第一发现密钥,以及用于向第二末端装置发送包括基于所述第一发现密钥的令牌是直接发现请求,并用于从所述第二末端装置接收包括ProSe响应码和第二令牌的发现响应。

38. 一种包括处理器和存储器的末端装置,所述存储器包含由所述处理器可执行的指令,使得网络节点可进行操作以便实行根据权利要求29至36中任一权利要求所述的方法。

39. 一种计算机可读介质,所述计算机可读介质上存储有计算机程序,所述计算机程序当在计算机上运行时配置成实行根据权利要求1至11、14至18、21至26或29至35中任一权利要求所述的方法。

## 用于末端装置发现另一个末端装置的方法和设备

### 技术领域

[0001] 本发明涉及用于使得末端装置能够安全地发现另一个末端装置的方法。它还涉及用于使得末端装置能够安全地发现另一个末端装置的服务器和末端装置。

### 背景技术

[0002] 邻近服务(ProSe)是能够由3GPP系统基于彼此邻近的UE提供的服务。这些服务之一是ProSe发现。3GPP TS 22.278和3GPP TS 23.303中描述了ProSe服务,并且它允许装置到装置(D2D)通信的可能性,而无需通过无线电接入网络传递消息。

[0003] 当满足许可、授权和邻近准则时,ProSe发现利用演进型UMTS地面无线电接入(E-UTRA)来标识ProSe使能的UE彼此邻近,而不管它们是否正在利用演进型UMTS地面无线电接入网络(E-UTRAN)或扩展型分组核心(EPC)网络。邻近准则能够由运营商配置。

[0004] ProSe发现过程涉及通过空中接口由一个装置发送和由另一个装置接收的发现消息。然后,这另一个装置以发现消息做出应答。两个发现消息均包括用于标识每个装置的ProSe码。但是,一个装置可重播从另一个装置接收的ProSe码,并且因此假装是所述另一个装置。因此,存在对于装置在它们彼此邻近时安全地发现彼此的需要。

### 发明内容

[0005] 根据本发明的一方面,提供有一种由邻近服务服务器执行的方法,该方法包括:生成ProSe查询码和ProSe响应码,至少将所述ProSe响应码与第一和第二发现密钥一起发送给第一末端装置,以及至少将所述第一发现密钥和所述ProSe查询码发送给第二末端装置,使得所述第二末端装置能够通过空中接口安全地发现所述第一末端装置。

[0006] 在一个实施例中,所述方法还包括:作为预备步骤,生成所述第一发现密钥和所述第二发现密钥。所述方法还可包括:作为预备步骤,从密钥管理服务器接收所述第一和第二发现密钥。

[0007] 在一个实施例中,所述方法包括:基于所述ProSe查询码生成发现过滤器,并将它发送给所述第一末端装置。

[0008] 在另一个实施例中,所述方法包括:从所述第二末端装置接收指示所述第二末端装置想要通过空中接口发现所述第一末端装置地发现请求,所述邻近服务服务器在此之后向所述第二末端装置发送所述第一发现密钥和ProSe查询码。

[0009] 所述方法还可包括:向所述第二末端装置与其进行通信的第二邻近服务服务器发送所述ProSe响应码。

[0010] 在一个实施例中,所述方法包括:从所述第二末端装置接收包括所述ProSe响应码和基于所述第二发现密钥的令牌的匹配报告请求。

[0011] 在一备选实施例中,所述方法包括利用所述第二发现密钥验证所述令牌。

[0012] 如果所述令牌已验证,那么所述方法还可包括向所述第二末端装置发送指示所述第一末端装置是真的匹配报告响应。

[0013] 在一个实施例中,所述方法包括:向所述第二末端装置发送所述第二发现密钥,使得所述第二末端装置能够验证所述第一末端装置是真的。

[0014] 在一个实施例中,所述第二末端装置包括多个第二末端装置,使得所述方法可包括向每个第二末端装置发送所述ProSe查询码和所述第一发现密钥。

[0015] 根据本发明的另一个方面,提供有一种服务器,其包括:生成单元,用于生成ProSe查询码和ProSe响应码;传送单元,用于至少将所述ProSe响应码与第一和第二发现密钥一起发送给第一末端装置,以及至少将所述第一发现密钥和所述ProSe查询码发送给第二末端装置,使得所述第二末端装置能够通过空中接口安全地发现所述第一末端装置。

[0016] 根据本发明的第四方面,提供有一种包括处理器和存储器的服务器,所述存储器包含由所述处理器可执行的指令,使得网络节点可进行操作以实行根据所附权利要求1至11中任一权利要求的方法。

[0017] 根据本发明还有的另一方面,提供有一种由末端装置执行的方法,所述方法包括:从邻近服务服务器接收第一发现密钥、第二发现密钥和ProSe响应码;从想要发现所述末端装置的第二末端装置接收包括ProSe查询码和令牌是直接发现请求;利用所述第一发现密钥验证所述令牌。

[0018] 所述方法还可包括:第一末端装置从所述邻近服务服务器接收基于ProSe查询码的发现过滤器。

[0019] 在一个实施例中,所述第一末端装置通过空中接口接收所述ProSe查询码和所述令牌,并且所述令牌基于所述第一发现密钥。

[0020] 如果所述第一末端装置验证了从所述第二末端装置接收的所述令牌,那么所述方法还可包括向所述第二末端装置发送包括基于所述第二发现密钥的第二令牌的发现响应。

[0021] 在一个实施例中,所述方法包括:作为预备步骤,所述末端装置向它的邻近服务服务器发送发现请求,以便请求允许所述第二末端装置发现所述末端装置。

[0022] 根据本发明的另一方面,提供有一种末端装置,其包括:传送单元,用于从邻近服务服务器接收第一发现密钥、第二发现密钥和ProSe响应码,以及用于从想要发现所述末端装置的第二末端装置接收包括ProSe查询码和令牌是直接发现请求;验证单元,用于利用所述第一发现密钥验证所述令牌。

[0023] 根据本发明还有的另一方面,提供有一种包括处理器和存储器的末端装置,所述存储器包含由所述处理器可执行的指令,使得网络节点可进行操作以便实行根据所附权利要求14至18中任一权利要求的方法。

[0024] 根据本发明的另外方面,提供有一种由邻近服务服务器执行的方法,所述方法包括:从第二邻近服务服务器至少接收第一发现密钥、ProSe查询码和ProSe响应码;基于所述ProSe响应码生成发现过滤器,并向第一末端装置发送所述发现过滤器、第一发现密钥和ProSe查询码,使得所述第一末端装置能够通过空中接口安全地发现第二末端装置。

[0025] 在一个实施例中,所述方法包括:从所述第一末端装置接收包括基于第二发现密钥的令牌的匹配报告请求,并将所述令牌转发给所述第二邻近服务器以便进行验证。

[0026] 如果所述第二邻近服务器验证了所述令牌,那么所述方法还可包括从所述第二邻近接收指示所述第二末端装置是真的的响应。

[0027] 在一个实施例中,所述方法还包括:所述邻近服务服务器从所述第二邻近服务服

务器接收第二发现密钥,并将所述第二发现密钥发送给所述第一末端装置。

[0028] 在另一个实施例中,所述方法还可包括:作为预备步骤,所述邻近服务服务器从所述第一末端装置接收指示所述第一末端装置想要发现所述第二邻近服务服务器的所述第二末端装置的发现请求。

[0029] 在一个实施例中,所述方法可包括向所述第二邻近服务服务器发送指示所述第一末端装置想要发现所述第二邻近服务服务器的所述第二末端装置的发现请求。

[0030] 根据本发明的另一个方面,提供有一种服务器,其包括:传送单元,用于从第二邻近服务服务器至少接收第一发现密钥、ProSe查询码和ProSe响应码;生成单元,用于基于所述ProSe响应码生成发现过滤器,并将所述发现过滤器、第一发现密钥和ProSe查询码发送给第一末端装置,使得所述第一末端装置能够通过空中接口安全地发现第二末端装置。

[0031] 根据本发明还有的另一个方面,提供有一种包括处理器和存储器的服务器,所述存储器包含由所述处理器可执行的指令,使得网络节点可进行操作以便实行根据所附权利要求21至26中任一权利要求的方法。

[0032] 根据本发明另外的方面,提供有一种由末端装置执行的方法,所述方法包括:从邻近服务服务器接收ProSe查询码和第一发现密钥;向第二末端装置发送包括基于所述第一发现密钥的令牌直接发现请求;以及从所述第二末端装置接收包括ProSe响应码和第二令牌的发现响应。

[0033] 在一个实施例中,所述方法包括从所述邻近服务服务器接收基于所述ProSe响应码的发现过滤器。

[0034] 在另一个实施例中,所述方法包括:所述末端装置利用所述发现过滤器来标识从所述第二末端装置接收的所述ProSe响应码。

[0035] 在一个实施例中,所述末端装置可将所述第二令牌转发给所述邻近服务服务器以便进行验证。

[0036] 如果所述第二令牌已验证,那么所述方法还可包括从所述邻近服务服务器接收指示所述第二末端装置是真的的消息。

[0037] 在备选实施例中,所述方法可包括:所述末端装置从所述邻近服务服务器接收第二发现密钥,并且所述末端装置利用所述第二发现密钥验证所述第二令牌,从而认证所述第二末端装置。

[0038] 在一个实施例中,所述方法可包括:作为预备步骤,向所述邻近服务服务器发送指示所述末端装置想要发现所述第二装置的发现请求。

[0039] 在另一个实施例中,所述末端装置可包括多个末端装置,使得所述方法还包括:每个末端装置接收相同的ProSe查询码和第一发现密钥,并向相同的第二末端装置发送直接发现请求,且从所述相同的第二末端装置接收直接发现响应。

[0040] 根据本发明的另一个方面,提供有一种末端装置,其包括:传送单元,用于从邻近服务服务器接收ProSe查询码和第一发现密钥,以及用于向第二末端装置发送包括基于所述第一发现密钥的令牌直接发现请求,并用于从所述第二末端装置接收包括ProSe响应码和第二令牌的发现响应。

[0041] 根据本发明的还有的另一方面,提供有一种包括处理器和存储器的末端装置,所述存储器包含由所述处理器可执行的指令,使得网络节点可进行操作以便实行根据所附权

利要求29至36中任一权利要求的方法。

[0042] 根据另外的方面,提供有一种计算机程序,当其在计算机上运行时配置成实行根据所附权利要求1至11、14至18、21至26或29至35中任一权利要求的方法。

[0043] 根据本发明的还有的另一方面,提供有一种计算机程序产品,其包括计算机可读介质和存储在所述计算机可读介质上的上面所描述的计算机程序。

## 附图说明

[0044] 图1示出根据本发明的实施例操作的第一网络;

[0045] 图2示出根据本发明的实施例操作的第二网络;

[0046] 图3示出网络的形式;

[0047] 图4示出ProSe功能和它们与UE的接口;

[0048] 图5示出ProSe功能和它们的接口;

[0049] 图6示出本发明的一实施例;

[0050] 图7示出根据本发明的另一个实施例;

[0051] 图8是示出根据本发明的一实施例由服务器执行的方法步骤的流程图;

[0052] 图9是示出根据本发明的另一个实施例由服务器执行的方法步骤的流程图;

[0053] 图10是示出根据本发明的还有的另一个实施例由服务器执行的方法步骤的流程图;

[0054] 图11是示出根据本发明的一实施例由末端装置执行的方法步骤的流程图;

[0055] 图12是示出根据本发明的另一个实施例由末端装置执行的方法步骤的流程图;

[0056] 图13是示出根据本发明的一实施例由服务器执行的方法步骤的流程图;

[0057] 图14是示出根据本发明的另一个实施例由服务器执行的方法步骤的流程图;

[0058] 图15是示出根据本发明的一实施例由末端装置执行的方法步骤的流程图;

[0059] 图16是示出根据本发明的另一个实施例由末端装置执行的方法步骤的流程图;

[0060] 图17是示出服务器的框图;

[0061] 图18是示出末端装置的框图;

[0062] 图19是示出服务器的框图;

[0063] 图20是示出服务器的另一个示例的框图;

[0064] 图21是示出末端装置的一示例的框图;

[0065] 图22是示出末端装置的另一个示例的框图;

[0066] 图23是示出服务器的一示例的框图;

[0067] 图24是示出服务器的另一个示例的框图;

[0068] 图25是示出末端装置的一示例的框图;以及

[0069] 图26是示出末端装置的另一个示例的框图。

## 具体实施方式

[0070] 图1示出包括服务于小区12的第一基站10的蜂窝通信网络的一部分,其中在小区12内具有第一无线通信装置(UE1)14和第二无线通信装置(UE2)16。

[0071] 图2示出另一个蜂窝通信网络的一部分,它包括服务于第一小区22的第一基站20



和服务于第二小区28的第二基站26,其中在小区22内有第一无线通信装置(UE1)24,并且在小区28内有第二无线通信装置(UE2)30。

[0072] 在本文中所描述的示例中,将参与这些方法的装置作为用户设备装置(UE)加以描述。将了解,该术语用于指:用户操作的便携式通信装置,诸如智能电话、膝上型计算机等;其它便携式装置,诸如跟踪装置等;以及主要打算用来在使用时保持静止的装置,诸如传感器、智能仪表等。术语“用户设备装置”还应理解为包括无线通信装置、末端装置和终端装置,并且它不限于是用户操作的装置。

[0073] 在如图1和图2中所示的示例中,网络形成如第三代合作伙伴计划(3GPP)定义的演进型UMTS地面无线电接入网络(E-UTRAN)的部分。3GPP系统提供能够供彼此邻近的用户设备(UE)装置使用的邻近服务(ProSe)的可能性。3GPP TS 22.278和3GPP TS 23.303中描述了ProSe系统。例如,ProSe系统允许装置到装置(D2D)通信的可能性,而无需通过无线电接入网络传递消息。

[0074] ProSe系统的一个方面是ProSe发现的过程。当满足允许、授权和邻近准则时,ProSe发现过程利用演进型UMTS地面无线电接入(使用或不使用E-UTRAN的情况下)或扩展型分组核心(EPC)网络来标识ProSe使能的UE彼此邻近。邻近准则能够由运营商配置。

[0075] ProSe发现的一个特定形式是ProSe直接发现,它是由ProSe使能的UE所采用的通过只利用具有E-UTRA技术的两个UE的能力来发现它附近的其它ProSe使能的UE的规程。

[0076] 术语“ProSe使能的UE”是指支持ProSe要求和相关联的规程的UE。ProSe使能的UE可以是非公共安全UE和/或公共安全UE。

[0077] 图1和图2示出D2D ProSe的场景,其中UE1和UE2各自位于小区的覆盖中,小区可以是如图1中所示的相同小区12,或者可以是如图2中所示的不同小区22、28。当UE1扮演作为传送器的角色时,UE1发送发现消息,并且UE2接收它。这两个装置UE1和UE2能够改变它们作为传送器和接收器的角色。除了UE2之外,还能够通过至少一个其它UE接收来自UE1的传送。

[0078] ProSe发现过程能够作为孤立过程使用(即,在它之后不一定跟随ProSe通信),或作为其它服务的启用者使用。

[0079] 图3是ProSe网络架构的图示。在图3中,假设两个用户设备装置UE A和UE B订阅到相同的公共陆地移动网络(PLMN)。

[0080] 这两个用户设备装置UE A和UE B各自具有通过LET-Uu接口到演进型UMTS地面无线电接入网络(E-UTRAN)的相应连接。S1接口将E-UTRAN连接到演进型分组核心(EPC)网络,除了其它网络节点外,EPC网络还包括移动性管理实体(MME)、服务网关(SGW)、分组网关(PGW)、归属订户服务器(HSS)和安全用户平面位置(SUPL)定位平台(SLP)。

[0081] 该网络还包括至少一个应用服务器,其利用ProSe能力来构建应用功能性。

[0082] 核心网络还包括ProSe功能,它提供诸如下列的功能性:授权和配置UE以便进行发现和直接通信(在非漫游情形中由用户的归属PLMN中的ProSe功能控制,并且在漫游情形中由归属PLMN或受访PLMN ProSe功能控制);启用EPC级ProSe发现的功能性;处置和存储ProSe相关的新订户数据和ProSe身份;以及与安全性相关的功能性。

[0083] ProSe功能具有朝向每个UE的PC3参考点,并且具有朝向EPC的PC4参考点。

[0084] ProSe功能还具有朝向至少一个ProSe应用服务器的PC2参考点,所述至少一个ProSe应用服务器利用ProSe能力来构建应用功能性。

[0085] 每个UE包括ProSe应用,它具有朝向ProSe应用服务器的PC1参考点。

[0086] 这些UE、即UE A和UE B利用PC5参考点来用于控制和用户平面来用于发现和通信,以便进行中继以及一对一通信(直接在UE之间以及通过LTE-Uu接口在UE之间)。参考点PC5在本文中又称为两个UE(UE A和UE B)之间的空中接口。

[0087] 图4更详细地示出ProSe功能。归属公共陆地移动网络(HPLMN)的ProSe功能410包括三个子功能:DPF 411、直接发现名称管理功能412和EPC级发现功能413。直接发现名称管理功能用于供开放式ProSe直接发现来分配和处理在ProSe直接发现中使用的ProSe应用ID和ProSe应用码的映射。它利用存储在归属订户服务器(HSS)中的ProSe相关的订户数据来授权每个发现请求。它还向UE 414提供必需的安全资料以便保护通过空中接口PC5传送的发现消息。

[0088] 图5示出不同公共陆地移动网络(PLMN)的若干个ProSe功能和它们的接口。归属PLMN(HPLMN)510具有朝向本地PLMN 511的PC6或PC7参考点。HPLMN 510还可具有朝向受访PLMN(VPLMN)512的PC7参考点。

[0089] 在ProSe直接发现规程中,存在两种模型:模型A(“我在这里”)和模型B(“谁在那里”/“你在那里吗”)。模型A定义参与ProSe直接发现的ProSe使能的UE的两个角色。一个角色由宣告UE担任,宣告UE宣告能够供它邻近的具有发现宣告UE的许可的其它UE使用的某些信息。另一个角色由监测UE担任,监测UE监测宣告UE邻近的某些感兴趣的信息。

[0090] 模型B定义参与ProSe直接发现的ProSe使能的UE的两个角色。第一个角色由发现者(discoverer)UE担任,发现者UE传送包含关于什么是有兴趣去发现的某些信息的请求。另一个角色由被发现者(discoveree)UE担任,被发现者UE接收请求消息并且能够用与发现者UE的请求有关的信息做出应答。应了解,这两个UE可转变角色。

[0091] ProSe直接发现规程能够是“开放式”或“限制性”发现规程。ProSe开放式直接发现能够是孤立服务启用者,它能够例如对于发现者/监测UE中的被许可使用来自被发现者/宣告UE的信息的某些应用使用该信息。例如,被发现者/宣告UE可以是附近的出租车,并且发现者/监测UE想要寻找附近的出租车。换句话说,对于谁能够发现谁没有或只有很少的限制。

[0092] 在ProSe限制性直接发现规程中,对谁能够发现谁有一定限制。ProSe使能的UE应当能够只可被彼此邻近且被可发现的ProSe使能的UE(被发现者/宣告UE)明确许可的其它ProSe使能的UE(发现者/监测UE)发现。ProSe限制性直接发现允许由被发现者/宣告UE在应用层定义许可以便确定发现者/监测UE发现被发现者/宣告UE的能力。

[0093] 应了解,开放式和限制性ProSe直接发现规程均能够使用模型A或模型B。

[0094] 现在再次更加详细地参考模型B,当发现者UE想要发现它附近或邻近的被发现者UE时,发现者UE通过空中接口(PC5)广播包括ProSe查询码的直接发现请求消息。(ProSe查询码是由归属公共陆地移动网络(HPLMN)中的ProSe功能生成或分配的码,并且它使得被发现者能够标识发现者。)被发现者UE监听发现消息,并利用基于ProSe查询码的发现过滤器,以便标识从发现者UE发送的直接发现请求消息。当发现过滤器标识从发现者UE发送的ProSe查询码时,被发现者UE通过空中(PC5接口)广播包括ProSe响应码的直接发现响应消息。ProSe响应码由ProSe功能分配给被发现者UE。

[0095] 现在将参考图6描述本发明的实施例。在该实施例中,被发现者UE 651、被发现者

UE的归属公共陆地移动网络(HPLMN) ProSe功能652、发现者UE 653和发现者UE的HPLMN ProSe功能654交换消息。

[0096] 首先,被发现者UE 651采用它的HPLMN ProSe功能652发起发现请求规程(步骤601),其通过发送请求允许应用服务器(见图3)中的预定发现者UE发现所述被发现者UE 651的发现请求来进行。被发现者UE通过PC3接口发送请求。

[0097] 接着,被发现者UE的HPLMN ProSe功能652生成或构造ProSe查询码、ProSe响应码、发现密钥A(第一发现密钥)和发现密钥B(第二发现密钥)(步骤602)。但是,在另一个没有示出的实施例中,HPLMN ProSe功能652不生成发现密钥A和发现密钥B,而是它转而从密钥管理服务接收这些密钥。

[0098] ProSe功能652还基于ProSe查询码生成或准备发现过滤器。发现过滤器是ProSe查询码、0个或多个ProSe应用掩码和存活时间值的容器,并且下文将更详细地解释它的使用。

[0099] 然后,ProSe功能652通过PC3接口将包括ProSe响应码、发现密钥A、发现密钥B和发现过滤器的发现响应发送给被发现者UE 651(步骤603)。

[0100] 与此同时,发现者UE 653采用其HPLMN ProSe功能654发起发现请求规程(步骤604),这通过在PC3接口上向它的HPLMN ProSe功能654发送用来发现被发现者UE 651的发现请求来进行。然后,发现者UE的HPLMN ProSe功能654通过PC6接口向被发现者UE的HPLMN ProSe功能652发送发现请求(步骤605)。作为响应,被发现者UE的HPLMN ProSe功能652通过PC6接口向发现者UE的HPLMN ProSe功能654发送发现响应,发现响应包括ProSe查询码、发现密钥A和ProSe响应码(步骤606)。然后,发现者UE的HPLMN ProSe功能654可存储ProSe查询码、发现密钥A和ProSe响应码(步骤606a)。

[0101] 然后,发现者UE的HPLMN ProSe功能654基于ProSe响应码配置或生成发现过滤器,并接着向发现者UE 653发送发现响应,发现响应包括ProSe查询码、发现密钥A和基于ProSe响应码的发现过滤器(步骤607)。

[0102] 此后,发现者UE 653利用发现密钥A演算令牌。令牌可以是消息完整性码(MIC)。利用在3GPP TS 33.220中描述的密钥导出函数(KDF)以及发现密钥A和时间值一起作为输入参数以演算MIC(步骤608a)。该令牌在本文中称为MIC-A。也能够利用ProSe查询码作为额外输入参数。应了解,令牌不限于MIC,在备选实施例中,能够改为使用消息认证码。

[0103] 当发现者UE 653想要发现它附近的被发现者UE 651时,发现者UE 653通过PC5接口广播直接发现请求消息(608b)。直接发现请求包括ProSe查询码和MIC-A。

[0104] 然后,被发现者UE 651听到直接发现请求,并且通过利用它的基于ProSe查询码的发现过滤器,被发现者UE 651标识或匹配从发现者UE 653接收的ProSe查询码。当被发现者UE 651已经进行了匹配时,它通过利用相同的发现密钥A和时间值演算MIC-A来验证令牌(步骤608c)。如果MIC-A与从发现者UE 653接收的令牌匹配,那么被发现者UE 651知道发现者UE是真的,并且因此能够安全地允许发现者UE 653发现所述被发现者UE 651。在下一步骤中,被发现者UE 651基于发现密钥B和时间值演算包括MIC的另一个令牌(步骤609a)。该令牌在本文中称为MIC-B。但是,应了解,如上文结合发现密钥A所论述的,能够使用备选令牌。

[0105] 接着,被发现者UE 651通过PC5接口向发现者UE 653发送发现响应(步骤609b)。发现响应包括ProSe响应码和MIC-B(基于发现密钥B的另一个令牌)。

[0106] 然后,发现者UE 653听到发现响应,并且通过利用它的基于ProSe响应码的发现过滤器,标识或匹配从被发现者UE 651发送的ProSe响应码。为了使发现者UE 653查明被发现者UE 651是否是真的,发现者UE 653发起匹配报告规程。它通过在PC3接口上向它的HPLMN ProSe功能654发送匹配报告请求而这么做(步骤610)。匹配报告消息包括令牌MIC-B。它还可包括ProSe响应码。然后,发现者UE的HPLMN ProSe功能654通过PC6接口将匹配报告请求转发给被发现者UE的HPLMN ProSe功能652(步骤611)。

[0107] 接着,被发现者UE的HPLMN ProSe功能652通过利用发现密钥B和时间值演算MIC-B来验证令牌。如果MIC-B与经由发现者UE 653和它的HPLMN ProSe功能654从被发现者UE 651接收的令牌匹配,那么被发现者UE的ProSe功能652通过PC6接口向发现者UE的HPLMN ProSe功能654发送匹配报告响应(步骤613),并且发现者UE的HPLMN ProSe功能654将匹配报告响应转发给发现者UE 653(步骤614)。一旦接收到匹配报告响应,发现者UE 653便知道被发现者UE 651是真的。

[0108] 该方法的优点之一是,因为被发现者UE 651和发现者UE 653共享发现密钥(A),所以被发现者UE 651能够验证发现者UE 653,以使得被发现者UE 651知道发现者UE 653是真的,而不是重播ProSe查询码的另一个冒充或假冒的发现者UE。

[0109] 此外,被发现者UE 651在听到满足它的发现过滤器的发现请求消息时不需要采用它的HPLMN ProSe功能来发起匹配报告规程,转而是被发现者UE 651自己能够验证在发现请求消息中接收的令牌。

[0110] 还有利的是,发现密钥B从未离开被发现者UE的ProSe功能652。这意味着,发现者UE 653不能通过向另一个发现者UE重播ProSe响应码而假装是被发现者UE。

[0111] 有利地,该方法能够适用于开放式直接发现规程和限制性直接发现二者。

[0112] 还有的另一个优点是,被发现者UE 651和发现者UE 653能够直接交换ProSe查询码和ProSe响应码,而无需在中间发信号通知网络。

[0113] 现在将参考图7描述另一个实施例。该实施例与参考图6描述的实施例的差别在于,被发现者UE的HPLMN ProSe功能将发现密钥B转发给发现者UE,使得发现者UE不需要发起匹配报告过程,而是能够自己验证从被发现者UE接收的MIC-B。

[0114] 在该实施例中,被发现者UE 751、被发现者UE的归属公共陆地移动网络(HPLMN) ProSe功能752、发现者UE 753和发现者UE的HPLMN ProSe功能754交换消息。

[0115] 首先,被发现者UE 751采用它的HPLMN ProSe功能752来发起发现请求规程(步骤701),这通过发送请求允许应用服务器(见图3)中的预定发现者UE发现所述被发现者UE 751的发现请求来进行。被发现者UE 751通过PC3接口发送请求。

[0116] 接着,被发现者UE的HPLMN ProSe功能752生成ProSe查询码、ProSe响应码、发现密钥A(第一发现密钥)和发现密钥B(第二发现密钥)(步骤702)。但是,在另一个实施例中,HPLMN ProSe功能752不生成发现密钥A和B,而是它转而从密钥管理服务器接收这些密钥。

[0117] HPLMN ProSe功能752还基于ProSe查询码生成发现过滤器。如之前所描述,发现过滤器是ProSe查询码、0个或多个ProSe应用掩码和存活时间值的容器,并且下文将更加详细地解释它的使用。

[0118] 然后,ProSe功能752通过PC3接口向被发现者UE 751发送包含ProSe响应码、发现密钥A、发现密钥B和发现过滤器的发现响应(步骤703)。

[0119] 与此同时,发现者UE 753采用它的HPLMN ProSe功能754来发起发现请求规程(步骤704),这通过在PC3接口上向它的HPLMN ProSe功能754发送用来发现被发现者UE 751的发现请求来进行。然后,发现者UE的HPLMN ProSe功能754通过PC6接口向被发现者UE的HPLMN ProSe功能752发送发现请求(步骤705)。作为响应,被发现者UE的HPLMN ProSe功能752通过PC6接口向发现者UE的HPLMN ProSe功能754发送发现响应,发现响应包括ProSe查询码、发现密钥A、发现密钥B和ProSe响应码(步骤706)。接着,发现者UE的HPLMN ProSe功能754可存储ProSe查询码、发现密钥A、发现密钥B和ProSe响应码(步骤706a)。

[0120] 然后,发现者UE的HPLMN ProSe功能754基于ProSe响应码配置发现过滤器,并接着向发现者UE 753发送发现响应,发现响应包括ProSe查询码、发现密钥A、发现密钥B和基于ProSe响应码的发现过滤器(步骤707)。

[0121] 此后,发现者UE 753利用发现密钥A演算令牌。令牌可以是消息完整性码(MIC)。利用在3GPP TS 33.220中描述的密钥导出函数(KDF)以及发现密钥A和时间值一起作为输入参数以演算MIC(步骤708a)。该令牌在本文中称为MIC-A。(也能够利用ProSe查询码作为额外输入参数。应了解,令牌不限于MIC,在备选实施例中,能够改为使用消息认证码。)

[0122] 当发现者UE 753想要发现它附近的被发现者UE 751时,发现者UE 753通过PC5接口广播直接发现请求消息(708b)。直接发现请求包括ProSe查询码和MIC-A。

[0123] 然后,被发现者UE 751听到直接发现请求,并且通过利用它的基于ProSe查询码的发现过滤器,被发现者UE 751标识或匹配从发现者UE 753接收的ProSe查询码。当被发现者UE 751已进行了匹配时,它通过利用相同的发现密钥A和时间值演算MIC-A来验证令牌(步骤708c)。如果MIC-A与从发现者UE 753接收的令牌匹配,那么被发现者UE 751知道发现者UE 753是真的,并且因此能够安全地允许发现者UE 753发现所述被发现者UE 751。它通过基于发现密钥B和时间值进一步演算包括MIC的另一个令牌而这么做(步骤709a)。该令牌在本文中称为MIC-B。但是,应了解,如上文结合发现密钥A所论述的,能够使用备选令牌。

[0124] 然后,被发现者UE 751通过PC5接口向发现者UE 753发送发现响应(步骤709b)。发现响应包括ProSe响应码和MIC-B(基于发现密钥B的另一个令牌)。

[0125] 然后,发现者UE 753听到发现响应,并且通过利用它的基于ProSe响应码的发现过滤器,标识或匹配从被发现者UE 751发送的ProSe响应码。为了使发现者UE 753查明被发现者UE 651是否是真的,发现者UE 753通过利用发现密钥B和时间值演算MIC-B来验证令牌。如果MIC-B与从被发现者UE 751接收的令牌匹配,那么发现者UE 653知道被发现者UE 651是真的,即,被发现者UE没有重播属于另一个被发现者UE的ProSe响应码。

[0126] 该实施例共享与参考图6描述的实施例类似的优点。例如,该方法的优点之一是,因为被发现者UE 751和发现者UE 753共享发现密钥(A),所以被发现者UE 751能够验证发现者UE 753,使得被发现者UE 751知道发现者UE 753是真的,而不是在重播ProSe查询码的另一个冒充或假冒的发现者UE。

[0127] 此外,被发现者UE 751在听到满足它的发现过滤器的发现请求消息时不需要采用它的HPLMN ProSe功能来发起匹配报告规程,而是转而被发现者UE 751自己能够验证在发现请求消息中接收的令牌。类似地,发现者UE 753在听到满足它的发现过滤器的发现响应消息时不需要发起匹配报告规程。而是,发现者UE 753自己能够验证从被发现者UE 752接收的令牌。

[0128] 有利地,该方法能够适用于开放式直接发现规程和限制性直接发现二者。

[0129] 与参考图6描述的实施例类似,另一个优点是,被发现者UE 751和发现者UE 753能够直接交换ProSe查询码和ProSe响应码,而无需在中间发信号通知网络。

[0130] 在参考图6和图7描述的两个实施例中,应了解,发现者UE 653、753可以是全都接收相同ProSe查询码、基于特定ProSe响应码的发现过滤器、以及第一发现密钥的发现者UE的群组。这使得群组中的任何发现者UE能够发现被发现者UE。因此,第一发现密钥和ProSe查询码并非是针对特定发现者UE是指定的。

[0131] 备选地,群组的每个发现者UE可另外接收相同的第二发现密钥,因此每个UE在从被发现者UE 651、751接收发现响应607、707时,能够验证或认证所述被发现者UE 651、751。

[0132] 现在将描述实现参考图6和图7描述的方法的实施例。

[0133] 现在将参考图8描述服务器的方法的实施例。服务器可以是邻近服务服务器,诸如ProSe功能。邻近服务服务器如第一末端装置(被发现者UE)一样是相同的公共陆地移动网络(PLMN)的部分,并且因此能够视为是第一末端装置的归属PLMN ProSe功能。第一末端装置和邻近服务服务器通过PC3接口传送信息。邻近服务服务器还经由与第二末端装置(发现者UE)相同的PLMN的另一个或第二邻近服务服务器或ProSe功能向以及从第二末端装置发送和接收信息。因此,第二邻近服务服务器能够视为是第二末端装置(发现者UE)的归属PLMN ProSe功能。

[0134] 如所提及的,通过诸如邻近服务服务器的服务器执行该方法。该方法包括:生成ProSe查询码和ProSe响应码(801);或将ProSe查询码和ProSe响应码分配给第一末端装置。在下一步骤中,邻近服务服务器至少将ProSe响应码与第一和第二发现密钥一起发送给第一末端装置802。此后,邻近服务服务器至少将第一发现密钥和ProSe查询码发送给第二末端装置803,以便使得第二末端装置能够通过空中接口安全地发现第一末端装置。

[0135] 现在将参考图9描述该方法的另一个实施例。在该实施例中,邻近服务服务器能够生成第一发现密钥和第二发现密钥901,或者备选地,它能够从密钥管理服务器接收这两个密钥902。接着,邻近服务服务器生成ProSe查询码和ProSe响应码903,或者将这些码分配给第一末端装置。此后,它至少将ProSe响应码与第一和第二发现密钥一起发送给第一末端装置904。然后,邻近服务服务器从第二末端装置接收指示第二末端装置想要通过空中接口发现第一末端装置的发现请求905。在下一步骤中,邻近服务服务器至少将第一发现密钥和ProSe查询码发送给第二末端装置906,并接着基于ProSe查询码生成发现过滤器,且将它发送给第一末端装置907。备选地,能够将基于ProSe查询码的发现过滤器与在步骤904中所陈述的ProSe响应码、第一和第二发现密钥一起发送给第一末端装置。然后,邻近服务服务器还将ProSe响应码发送给第二末端装置与其进行通信的第二邻近服务服务器908。(这使得第二邻近服务服务器而不是邻近服务服务器能够基于ProSe响应码生成发现过滤器。)在下一步骤中,邻近服务服务器经由第二末端装置从第一末端装置接收包括基于第二发现密钥的令牌以及ProSe响应码的匹配报告请求909。然后,它利用第二发现密钥验证令牌910,并接着通过向第二末端装置发送指示第一末端装置是真的匹配报告响应来做出应答911。在一个实施例中,在步骤912,第二末端装置包括多个第二末端装置,使得该方法还包括向每个第二末端装置发送ProSe查询码和第一发现密钥,如步骤906中所陈述的那样。

[0136] 现在将参考图10描述另一个实施例。该实施例1000与参考图9描述的实施例的差

别在于,邻近服务服务器还向第二末端装置发送第二发现密钥,使得第二末端装置能够在不发送匹配报告请求的情况下验证或认证第一末端装置。

[0137] 前几个步骤1001、1002、1003、1004、1005、1006对应于图9中的步骤901、902、903、904、905和906,并且因此将不再详细描述。在步骤1007中,邻近服务服务器向第二末端装置发送第二发现密钥。邻近服务服务器还基于ProSe查询码生成发现过滤器,并将它发送给第一末端装置(1008),这与图9中的步骤907类似。它还将ProSe响应码发送给第二末端装置与其进行通信的第二邻近服务服务器1009。(这使得第二邻近服务服务器而不是邻近服务服务器能够基于ProSe响应码生成发现过滤器。)在还有的另一个实施例中,在步骤1010,第二末端装置包括多个第二末端装置,使得该方法还包括向每个末端装置发送ProSe查询码、第一发现密钥和第二发现密钥,如步骤1006和1007中所陈述的那样。

[0138] 现在将参考图11描述本发明的另一个方面。图11示出由末端装置(被发现者UE)执行的方法1100。末端装置通过PC3接口与它的邻近服务服务器或HPLMN ProSe功能通信。末端装置还通过空中接口PC5与第二末端装置(发现者UE)通信。

[0139] 在该方法中,末端装置从邻近服务服务器接收第一发现密钥、第二发现密钥和ProSe响应码1102。末端装置还从想要发现末端装置的第二末端装置接收包括ProSe查询码和令牌的直接发现请求1103。然后,末端装置利用第一发现密钥验证令牌1104。

[0140] 图12示出另一个实施例,其中通过末端装置实行或执行方法1200。在该方法中,末端装置向邻近服务服务器发送发现请求以便请求允许第二末端装置发现该末端装置1201。然后,末端装置从它的邻近服务服务器接收第一发现密钥、第二发现密钥和ProSe响应码1202。它还从邻近服务服务器接收基于ProSe查询码的发现过滤器1203。此后,末端装置从想要发现末端装置的第二末端装置接收包括ProSe查询码和令牌的直接发现请求1204。末端装置可通过空中接口接收ProSe查询码和令牌,并且令牌基于第一发现密钥1205。此后,末端装置利用第一发现密钥验证令牌1206。如果验证成功,那么末端装置向第二末端装置发送包括基于第二发现密钥的第二令牌的发现响应1207。

[0141] 现在将参考图13描述本发明的另一个实施例。图13示出诸如邻近服务服务器(它可以是ProSe功能)的服务器的方法。邻近服务服务器如第一末端装置(发现者UE)一样是相同的公共陆地移动网络(PLMN)的部分,并且因此能够视为是第一末端装置的归属PLMN ProSe功能。第一末端装置和邻近服务服务器通过PC3接口传送信息。邻近服务服务器还向以及从第二末端装置(被发现者UE)的相同PLMN的第二邻近服务服务器或ProSe功能发送和接收信息。因此,第二邻近服务服务器能够视为是第二末端装置的归属PLMN ProSe功能。

[0142] 在该方法1300中,邻近服务服务器从第二邻近服务服务器至少接收第一发现密钥、ProSe查询码和ProSe响应码1301。接着,它基于ProSe响应码生成发现过滤器1302,并且此后将发现过滤器、第一发现密钥和ProSe查询码发送给第一末端装置1303。

[0143] 现在将参考图14描述另一个实施例。该方法1400也由诸如与执行方法1300的邻近服务服务器类似的邻近服务服务器的服务器来执行。邻近服务服务器从第一末端装置(发现者UE)接收指示第一末端装置想要发现第二邻近服务服务器的第二末端装置(被发现者UE)的发现请求1401。接着,邻近服务服务器将指示第一末端装置想要发现第二邻近服务服务器的第二末端装置(被发现者UE)的发现请求发送或转发给第二邻近服务服务器1402。然后,邻近服务服务器从第二邻近服务服务器至少接收第一发现密钥、ProSe查询码和ProSe响应码1403。

在下一步骤1404中,邻近服务服务器基于ProSe响应码生成发现过滤器。此后,邻近服务服务器将发现过滤器、第一发现密钥和ProSe查询码发送给第一末端装置。

[0144] 在一个备选方案中,邻近服务服务器接着从第一末端装置接收包括基于第二发现密钥的令牌的匹配报告请求,并接着将令牌转发给第二邻近服务器以进行验证1406。如果第二邻近服务服务器验证了该令牌,那么该方法还包括从第二邻近服务器接收认证第二末端装置的响应,即,邻近服务服务器告知第一末端装置第二末端装置是真的1407。

[0145] 在另一个备选方案中,邻近服务服务器不接收和转发令牌。转而,它从第二邻近服务服务器接收第二发现密钥,并将该第二发现密钥发送或转发给第一末端装置1408。通过这样做,第一末端装置能够自己验证或认证第二末端装置。

[0146] 在图15中,示出由末端装置(发现者)执行的方法1500。末端装置通过PC3接口与它的邻近服务服务器或HPLMN ProSe功能通信。末端装置还通过空中接口PC5与第二末端装置(被发现者)通信。

[0147] 在方法1500中,末端装置从邻近服务服务器接收ProSe查询码和第一发现密钥1501。然后,它向第二末端装置发送包括基于第一发现密钥的令牌的直接发现请求1502。在下一步骤1503中,末端装置从第二末端装置接收包括ProSe响应码和第二令牌的发现响应1503。

[0148] 现在将参考图16描述方法1600的另一个实施例。该方法由与执行方法1500的末端装置类似的末端装置(发现者)来执行。

[0149] 在该方法1600中,末端装置从邻近服务服务器接收ProSe查询码和第一发现密钥1601。它还接收基于ProSe响应码的发现过滤器1602。然后,末端装置向第二末端装置(被发现者UE)发送包括基于第一发现密钥的令牌的直接发现请求1603。作为响应,它从第二末端装置接收包括ProSe响应码和第二令牌的发现响应1604。然后,末端装置利用发现过滤器标识从第二末端装置接收的ProSe响应码1605。

[0150] 接着,该实施例有两个备选方案。在第一个备选方案中,末端装置将第二令牌转发给它的邻近服务服务器以进行验证1606。如果验证成功,那么末端装置从它的邻近服务服务器接收指示第二末端装置是真的消息1607。尽管图中没有示出,但是在另一个邻近服务服务器、即第二末端装置(被发现者)的邻近服务服务器中进行令牌的验证。

[0151] 在第二个备选方案中,末端装置不发送或接收匹配报告,而是它转而从邻近服务服务器接收第二发现密钥,并且末端装置利用第二发现密钥验证第二令牌,从而认证或验证第二末端装置是真的1608。

[0152] 对于方法1600的各种实施例,应意识到,执行方法1600的末端装置可以是多个末端装置,使得该方法还包括每个末端装置接收相同的ProSe查询码和第一发现密钥并向相同的第二末端装置发送直接发现请求以及从所述第二末端装置接收直接发现响应1609。

[0153] 方法800、900、1000、1100、1200、1300、1400、1500和1600的实施例全都享有参考图6和图7描述的相应实施例的优点。

[0154] 上文描述的方法可在诸如末端装置(它可以是UE)的邻近服务服务器的服务器中或在末端装置本身中进行。可在接收到合适的计算机可读指令时进行这些方法,指令可在邻近服务服务器或末端装置上运行的计算机程序内实施。图17和图18示出可在例如从计算机程序接收到合适指令时执行本发明的方法的邻近服务服务器1701和末端装置1801的示



例。参考图17和图18,邻近服务服务器和末端装置中的每一个都包括处理器和存储器。存储器包含可由处理器执行的指令,使得邻近服务服务器可进行操作以便实行方法800、900、1000、1300和1400的任何实施例和/或末端装置可进行操作以便实行方法1100、1200、1500和1600的任何实施例。

[0155] 在图19中,示出服务器1901的实施例。服务器1901可以是充当被发现者的末端装置的邻近服务服务器或ProSe功能。该服务器包括PC6接口1904,它在PC6接口1904上与充当发现者的末端装置的其它邻近服务服务器或ProSe功能通信。该服务器还包括PC3接口1905,它在PC3接口1905上与它的属于相同PLMN的末端装置(被发现者)通信。服务器1901包括处理器1902和存储器1903。存储器包含可由处理器执行的指令,使得邻近服务服务器配置成生成ProSe查询码和ProSe响应码,至少将ProSe响应码与第一和第二发现密钥一起发送给第一末端装置,并至少将第一发现密钥和ProSe查询码发送给第二末端装置,使得第二末端装置能够通过空中接口安全地发现第一末端装置。

[0156] 服务器1901还可配置成生成第一发现密钥和第二发现密钥或从密钥管理服务器接收第一和第二发现密钥。

[0157] 在一个实施例中,该服务器配置成基于ProSe查询码生成发现过滤器并将它发送给第一末端装置。

[0158] 在一个实施例中,服务器1901配置成从第二末端装置接收指示第二末端装置想要通过空中接口发现第一末端装置的发现请求,在此之后邻近服务服务器将第一发现密钥和ProSe查询码发送给第二末端装置。

[0159] 服务器1901还可配置成将ProSe响应码发送给第二末端装置与其进行通信的第二邻近服务服务器。

[0160] 在一个实施例中,服务器1901配置成从第二末端装置接收包括ProSe响应码和基于第二发现密钥的令牌的匹配报告请求。该服务器还可配置成利用第二发现密钥验证令牌。如果令牌已验证,那么服务器可配置成将指示第一末端装置是真的匹配报告响应发送给第二末端装置。

[0161] 在一备选实施例中,服务器1901可配置成将第二发现密钥发送给第二末端装置,使得第二末端装置能够验证第一末端装置是真的。

[0162] 应了解,服务器能够配置成使得它将相同的ProSe查询码和相同的第一发现密钥发送给属于一群组的若干个第二末端装置。此后,每个第二末端装置能够向相同的第一末端装置(被发现者)发送直接发现请求。因此,ProSe查询码和第一发现密钥并非是针对特定第二末端装置是指定的。

[0163] 图20示出可根据例如从计算机程序接收的计算机可读指令执行本文中描述的方法800、900、1000中的任何方法的第一末端装置(被发现者)的邻近服务服务器2001或ProSe功能的另一个实施例中的功能单元。将了解,图20中示出的单元是软件实现的功能单元,并且它们可在软件模块的任何合适的组合中实现。

[0164] 参考图20,邻近服务服务器2001包括:生成单元2002,用于生成ProSe查询码和ProSe响应码;传送单元2003,用于至少将ProSe响应码与第一和第二发现密钥一起发送给第一末端装置,并至少将第一发现密钥和ProSe查询码发送给第二末端装置,使得第二末端装置能够通过空中接口安全地发现第一末端装置。

[0165] 邻近服务服务器2001还包括用于执行软件或单元的处理单元以及用于存储这些不同单元的存储器。

[0166] 生成单元2002还可包括用于生成第一发现密钥和第二发现密钥的部件。备选地，传送单元2003从密钥管理服务器接收第一和第二发现密钥。

[0167] 生成单元2002还可包括用于基于ProSe查询码生成发现过滤器并将它发送给第一末端装置的部件。

[0168] 传送单元2003可包括用于从第二末端装置接收指示第二末端装置想要通过空中接口发现第一末端装置的发现请求的部件。它还用于将ProSe响应码发送给第二末端装置与其进行通信的第二邻近服务服务器。传送单元2003还可包括用于从第二末端装置接收包括ProSe响应码和基于第二发现密钥的令牌的匹配报告请求的部件。

[0169] 该邻近服务服务器还可包括用于利用第二发现密钥验证令牌的验证单元2004。这在图20中用虚线示出，以便指示该单元是可选的。

[0170] 在一备选实施例中，邻近服务服务器2001不包括验证单元2004。在该实施例中，传送单元2003包括用于向第二末端装置发送第二发现密钥以使得第二发现密钥能够自己验证第一末端装置的部件。在该实施例中，传送单元不接收匹配报告请求或不发送匹配报告响应。

[0171] 上文描述的传送单元2003能够用于对于一组第二末端装置发送和接收如上所述的信息，使得传送单元将相同的ProSe查询码和第一发现密钥发送给群组中的若干个成员。它还可将第二发现密钥发送给群组的若干个成员。

[0172] 在一些示例中，传送单元2003、验证单元2004和生成单元2002可借助于来自计算机程序的帮助而实现，计算机程序在处理器上运行时使得传送单元、验证单元和生成单元进行协作以便实行上文描述的方法800、900、1000的示例。

[0173] 图21示出可充当被发现者的末端装置2101。该末端装置包括用来与它的邻近服务服务器或ProSe功能通信的PC3接口2102。该末端装置还包括PC5接口2103，采用PC5接口2103，该末端装置与第二末端装置（发现者）通信。末端装置2101还包括处理器2104和存储器2105。存储器包含可由处理器执行的指令，使得末端装置配置成从邻近服务服务器接收第一发现密钥、第二发现密钥和ProSe响应码，从想要发现末端装置的第二末端装置接收包括ProSe查询码和令牌的直接发现请求，并利用第一发现密钥验证令牌。

[0174] 该末端装置还可配置成从邻近服务服务器接收基于ProSe查询码的发现过滤器，发现过滤器用于标识从第二末端装置接收的ProSe查询码。第一末端装置还可配置成使得它通过空中接口接收ProSe查询码和令牌，并且令牌基于第一发现密钥。

[0175] 在一个实施例中，该末端装置配置成验证从第二末端装置接收的令牌，该方法还包括向第二末端装置发送包括基于第二发现密钥的第二令牌的发现响应。该末端装置还可按照如下作为预备步骤进行配置，它向它的邻近服务服务器发送发现请求，以便请求允许第二末端装置发现所述末端装置。

[0176] 图22示出在可根据例如从计算机程序接收的计算机可读指令执行本文中描述的方法1100和1200中的任何方法的末端装置2201（被发现者）的另一个实施例中的功能单元。将了解，图22中示出的单元是软件实现的功能单元，并且它们可在软件模块的任何合适的组合中实现。

[0177] 参考图22, 末端装置2201包括用于从邻近服务服务器接收第一发现密钥、第二发现密钥和ProSe响应码以及从想要发现末端装置的第二末端装置(发现者UE)接收包括ProSe查询码和令牌的直接发现请求的传送单元2202。末端装置2201还包括用于利用第一发现密钥验证令牌的验证单元2203。

[0178] 传送单元2202还可包括用于从邻近服务服务器接收基于ProSe查询码的发现过滤器的部件, 发现过滤器用于标识从第二末端装置接收的ProSe查询码。该末端装置可包括用于利用发现过滤器来标识ProSe查询码的标识模块(未示出)。

[0179] 传送单元还可包括用于通过空中接口接收ProSe查询码和令牌的部件, 并且令牌基于第一发现密钥。

[0180] 如果验证单元2203验证了从第二末端装置接收的令牌, 那么传送单元2204还可包括用于向第二末端装置发送包括基于第二发现密钥的第二令牌的发现响应的部件。

[0181] 还应意识到, 传送单元2202还可包括用于向它的邻近服务服务器发送发现请求以便请求允许第二末端装置发现所述末端装置的部件。

[0182] 在一些示例中, 传送单元2202和验证单元2203可借助于来自计算机程序的帮助而实现, 计算机程序在处理器上运行时使得传送单元和验证单元进行协作以便实行上文描述的方法1100和1200的示例。

[0183] 在图23中, 公开另一个服务器2301的实施例。服务器2301可以是充当发现者的末端装置的邻近服务服务器或ProSe功能。服务器2301包括PC6接口2302, 它在PC6接口2302上与充当被发现者的末端装置的其他邻近服务服务器或ProSe功能通信。该服务器还包括PC3接口2303, 它在PC3接口2303上与它的属于相同PLMN的末端装置(发现者)通信。服务器2301包括处理器2304和存储器2305。存储器2305包含可由处理器执行的指令, 使得邻近服务装置配置成从第二邻近服务服务器至少接收第一发现密钥、ProSe查询码和ProSe响应码, 基于ProSe响应码生成发现过滤器, 并将发现过滤器、第一发现密钥和ProSe查询码发送给第一末端装置, 使得第一末端装置(发现者UE)能够通过空中接口安全地发现第二末端装置(被发现者UE)。

[0184] 服务器2301还可配置成从第一末端装置接收包括基于第二发现密钥的令牌的匹配报告请求并将令牌转发给第二邻近服务器以进行验证。如果第二邻近服务器验证了令牌, 那么服务器2301还配置成从第二邻近接收指示第二末端装置是真的响应。

[0185] 在一备选实施例中, 服务器2301可配置成从第二邻近服务服务器接收第二发现密钥并将第二发现密钥发送给第一末端装置。

[0186] 服务器2301可配置成从第一末端装置接收指示第一末端装置想要发现第二邻近服务服务器的第二末端装置地发现请求。

[0187] 在还有的另一个实施例中, 服务器2301可配置成向第二邻近服务服务器发送指示第一末端装置想要发现第二邻近服务服务器的第二末端装置地发现请求。

[0188] 图24示出在充当发现者的末端装置的邻近服务服务器2401或ProSe功能的另一个实施例中的功能单元。邻近服务服务器2401可根据例如从计算机程序接收的计算机可读指令执行本文中描述的方法1300和1400中的任何方法。将了解, 图24中示出的单元是软件实现的功能单元, 并且可在软件模块的任何合适的组合中实现。

[0189] 参考图24, 邻近服务服务器2401包括用于从第二邻近服务服务器至少接收第一发

现密钥、ProSe查询码和ProSe响应码的传送单元2402以及用于基于ProSe响应码生成发现过滤器的生成单元2403。传送单元2402还包括用于将发现过滤器、第一发现密钥和ProSe查询码发送给第一末端装置以使得第一末端装置能够通过空中接口安全地发现第二末端装置的部件。

[0190] 传送单元2403还可包括用于接收包括基于第二发现密钥的令牌的匹配报告请求并将令牌转发给第二邻近服务器以进行验证的部件。

[0191] 如果令牌已验证,那么传送单元2402还包括用于从第二邻近接收指示第二末端装置是真的响应的部件。

[0192] 在另一个实施例中,传送单元包括用于从第二邻近服务服务器接收第二发现密钥并将第二发现密钥发送给第一末端装置的部件。

[0193] 传送单元2402还可包括用于从第一末端装置接收指示第一末端装置想要发现第二邻近服务服务器的第二末端装置的发现请求的部件。传送单元2402还可包括用于向第二邻近服务服务器发送指示第一末端装置想要发现第二邻近服务服务器的第二末端装置的发现请求的部件。

[0194] 在一些示例中,生成单元2403和传送单元2402可借助于来自计算机程序的帮助而实现,计算机程序在处理器上运行时使得传送单元、验证单元和生成单元进行协作以便实行上文描述的方法1300和1400的示例。

[0195] 图25示出可充当发现者的末端装置2501。该末端装置包括用来与它的邻近服务服务器或ProSe功能通信的PC3接口2502。末端装置2501还包括PC5接口2503,它采用PC5接口2503来与第二末端装置(被发现者)通信。末端装置2501还包括处理器2504和存储器2505。存储器包含可由处理器执行的指令,使得末端装置配置成从邻近服务服务器接收ProSe查询码和第一发现密钥,向第二末端装置发送包括基于第一发现密钥的令牌的直接发现请求,并从第二末端装置接收包括ProSe响应码和第二令牌的发现响应。

[0196] 末端装置2501还可配置成从邻近服务服务器接收基于ProSe响应码的发现过滤器。

[0197] 在一个实施例中,末端装置2501配置成利用发现过滤器标识从第二末端装置接收的ProSe响应码。

[0198] 末端装置2501还可配置成将第二令牌转发给邻近服务服务器以进行验证。如果第二令牌已验证,那么末端装置可配置成从邻近服务服务器接收指示第二末端装置是真的消息。

[0199] 在一个实施例中,末端装置2501配置成从邻近服务服务器接收第二发现密钥,并且末端装置利用第二发现密钥验证第二令牌,从而认证第二末端装置。

[0200] 在一个实施例中,末端装置2501可配置成向邻近服务服务器发送指示末端装置想要发现第二装置的发现请求。

[0201] 在另一个实施例中,多个末端装置2501可配置成接收相同的ProSe查询码和第一发现密钥,并向相同的第二末端装置发送直接发现请求,以及从所述相同的第二末端装置接收直接发现响应。

[0202] 图26示出在可根据例如从计算机程序接收的计算机可读指令执行本文中描述的方法1500和1600中的任何方法的末端装置2601(发现者)的另一个实施例中的功能单元。将

了解,图26中示出的单元是软件实现的功能单元,并且它们可在软件模块的任何合适的组合中实现。

[0203] 参考图26,末端装置2601包括用于从邻近服务服务器接收ProSe查询码和第一发现密钥、向第二末端装置发送包括基于第一发现密钥的令牌是直接发现请求并从第二末端装置接收包括ProSe响应码和第二令牌的发现响应的传送单元2602。

[0204] 传送单元2602还可包括用于从邻近服务服务器接收基于ProSe响应码的发现过滤器的部件。

[0205] 末端装置还可包括用于利用发现过滤器标识从第二末端装置接收的ProSe响应码的标识单元2603。图26中用虚线指示该可选特征。

[0206] 传送单元2602还可包括用于将第二令牌转发给邻近服务服务器以进行验证的部件。如果第二令牌已验证,那么传送单元还可包括用于从邻近服务服务器接收指示第二末端装置是真的消息的部件。

[0207] 在一个实施例中,传送单元2602还包括用于从邻近服务服务器接收第二发现密钥的部件,并且末端装置还包括用于利用第二发现密钥验证第二令牌从而认证第二末端装置的验证单元2604。正如在图26中由虚线所指示的那样,验证单元2604是可选的。

[0208] 传送单元2602还可包括用于向邻近服务服务器发送指示末端装置想要发现第二装置的发现请求的部件。

[0209] 在一个实施例中,存在多个末端装置2601,并且每个末端装置包括用于接收相同的ProSe查询码和第一发现密钥、以及向相同的第二末端装置发送直接发现请求和从所述第二末端装置接收直接发现响应的传送单元。

[0210] 在一些示例中,传送单元2602、标识单元2603和验证单元2604可借助于来自计算机程序的帮助而实现,计算机程序在处理器上运行时使得传送单元、验证单元和标识单元进行协作以便实行上文描述的方法1500和1600的示例。

[0211] 应注意,上面提到的实施例说明而不是限制本发明,并且在不偏离随附权利要求的范围的情况下,本领域技术人员将能够设计许多备选实施例。词语“包括”不排除存在权利要求中所列的元件或步骤以外的元件或步骤,“一(a)”或“一(an)”不排除多个,并且单个特征或其它单元可满足权利要求中记载的若干个单元的功能。权利要求中的任何参考符号不应理解为是为了限制它们的范围。

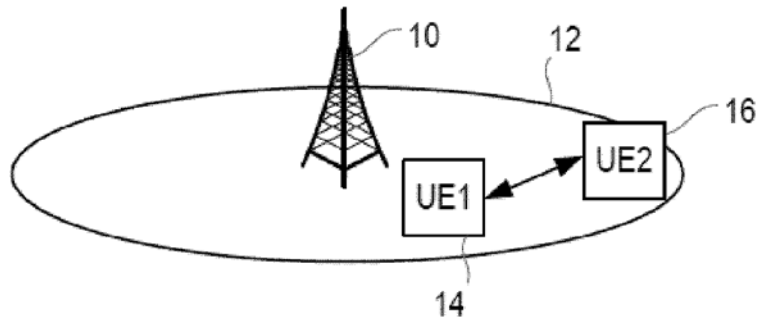


图 1

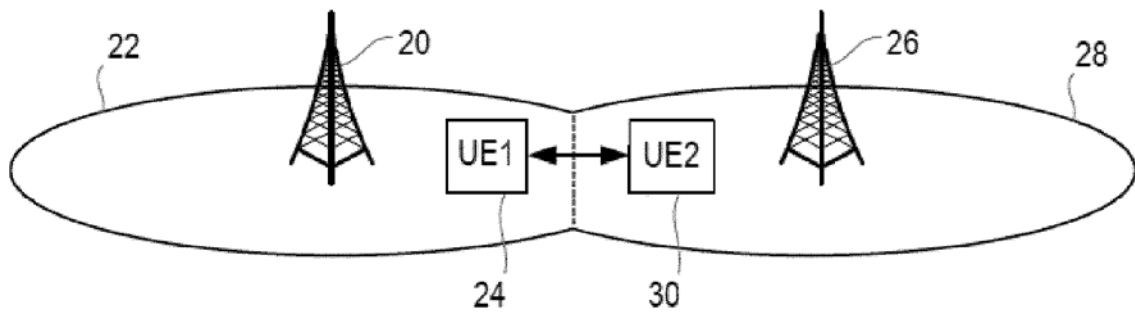


图 2

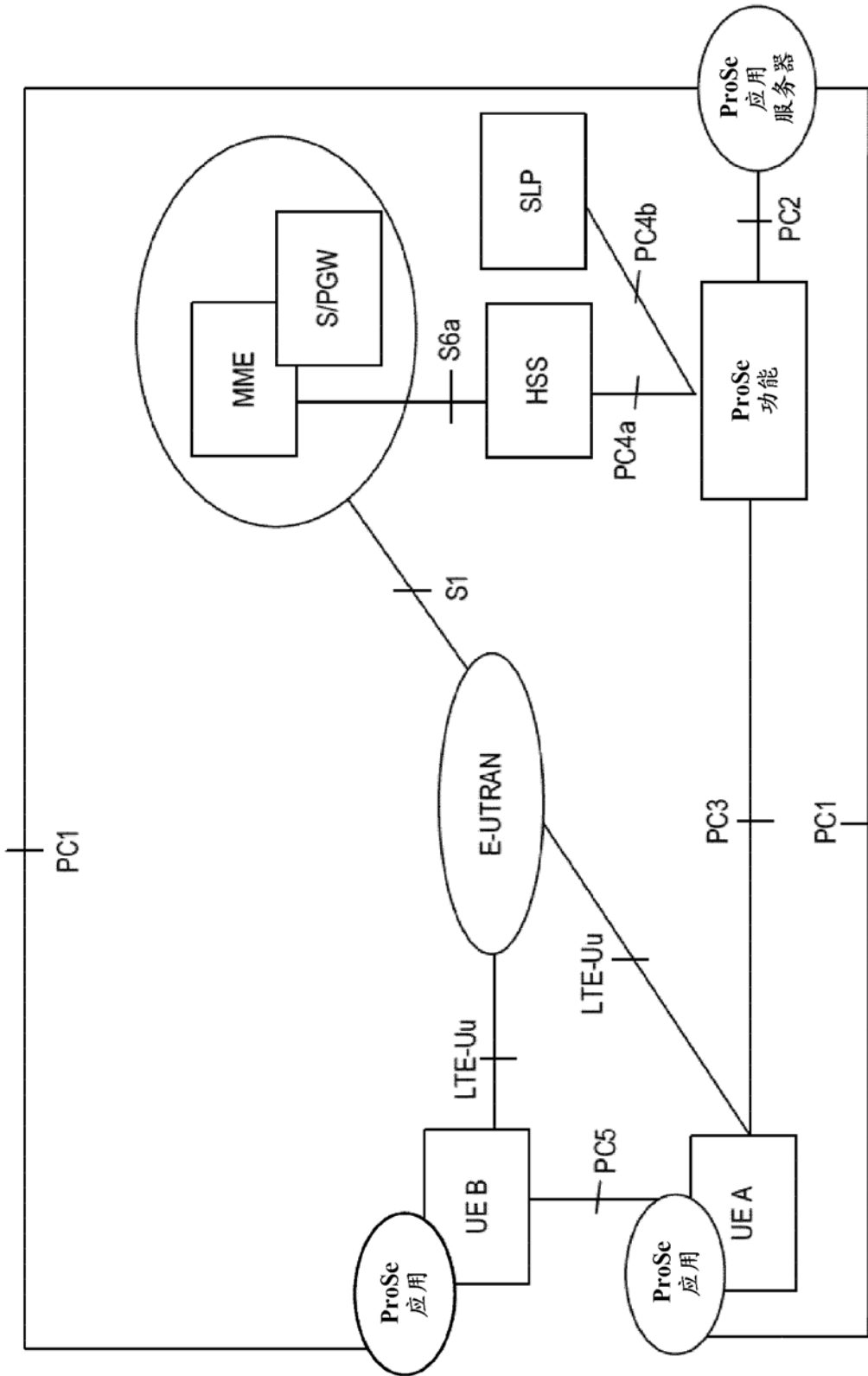


图 3

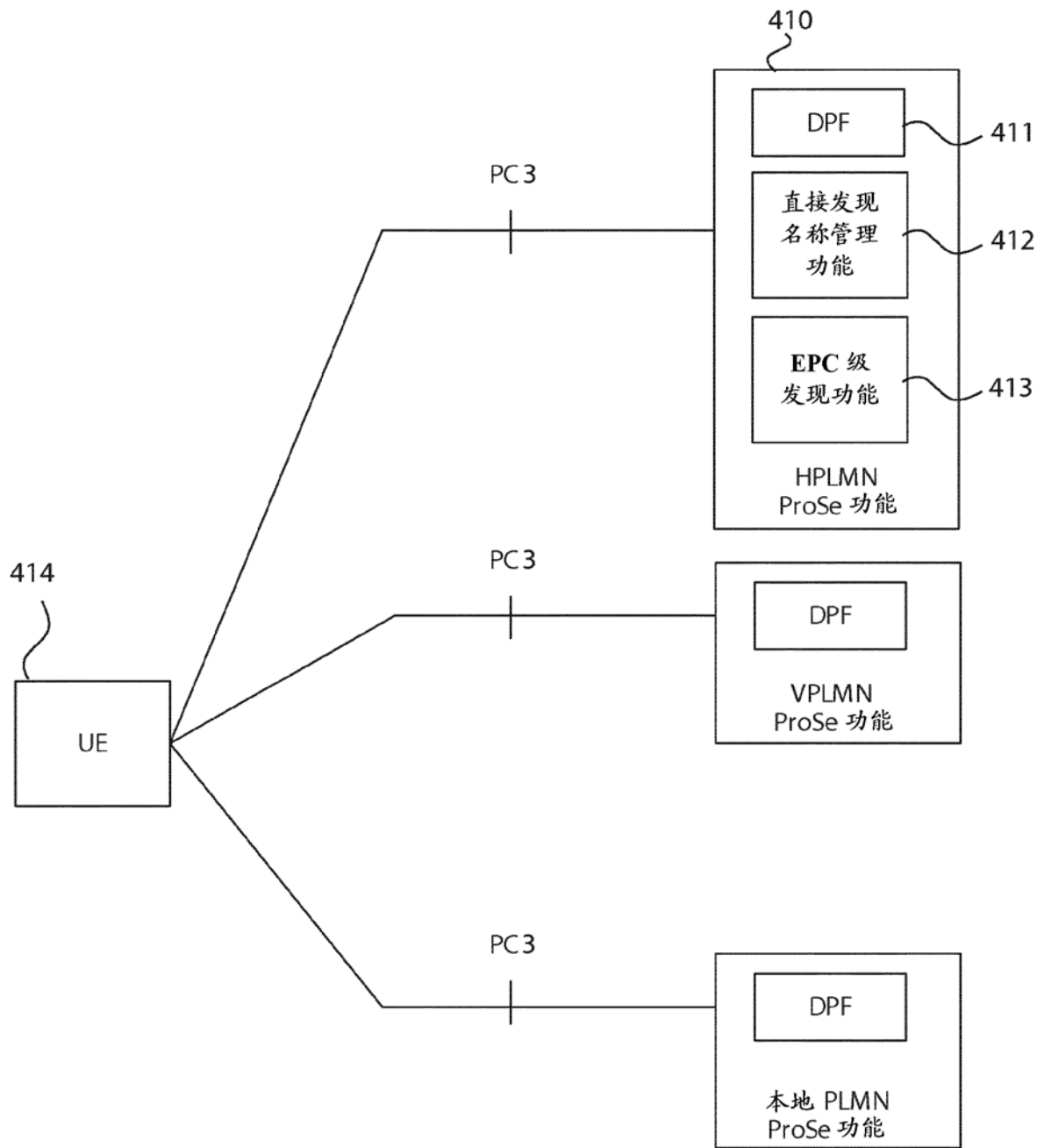


图 4



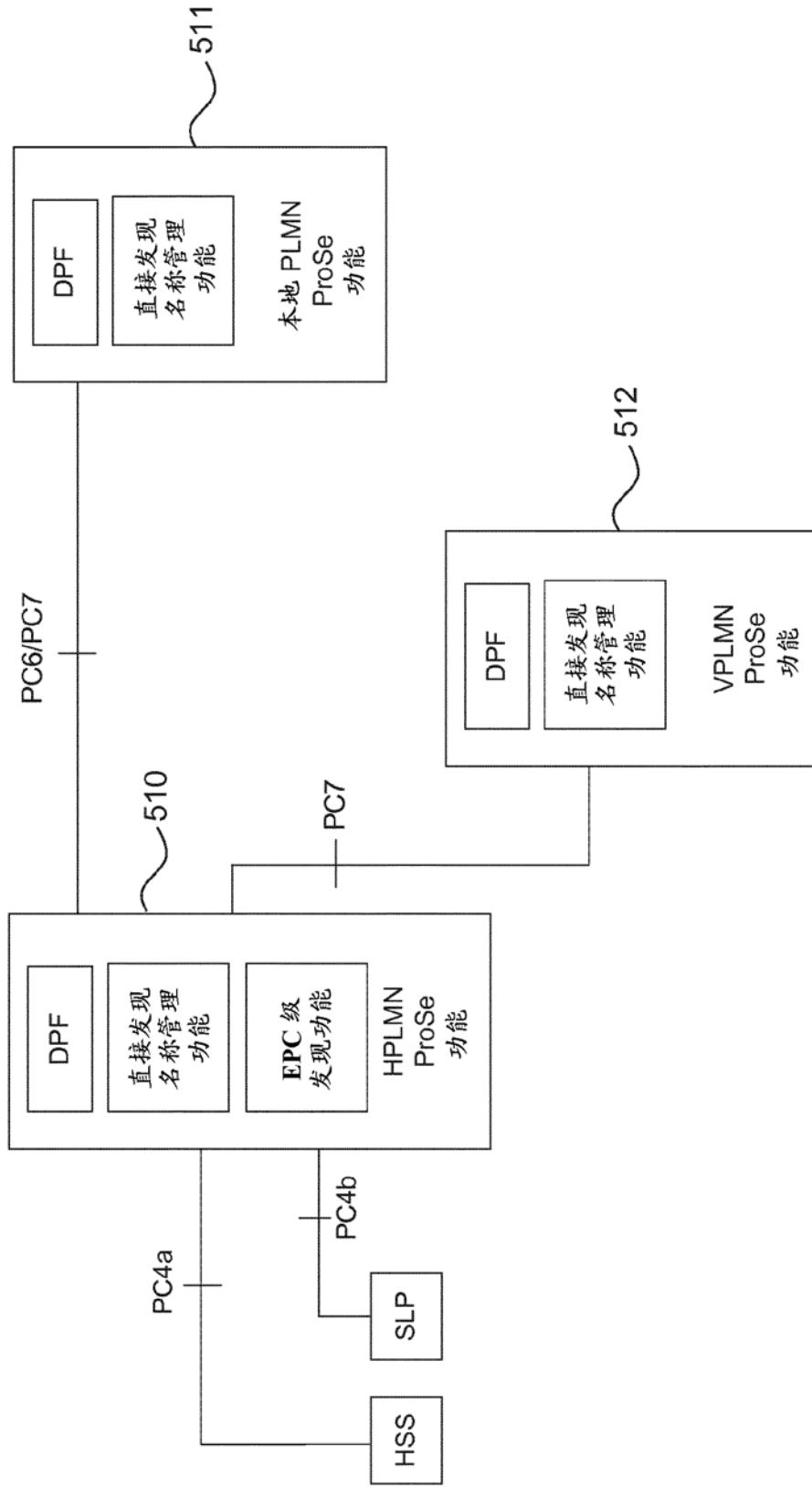


图 5

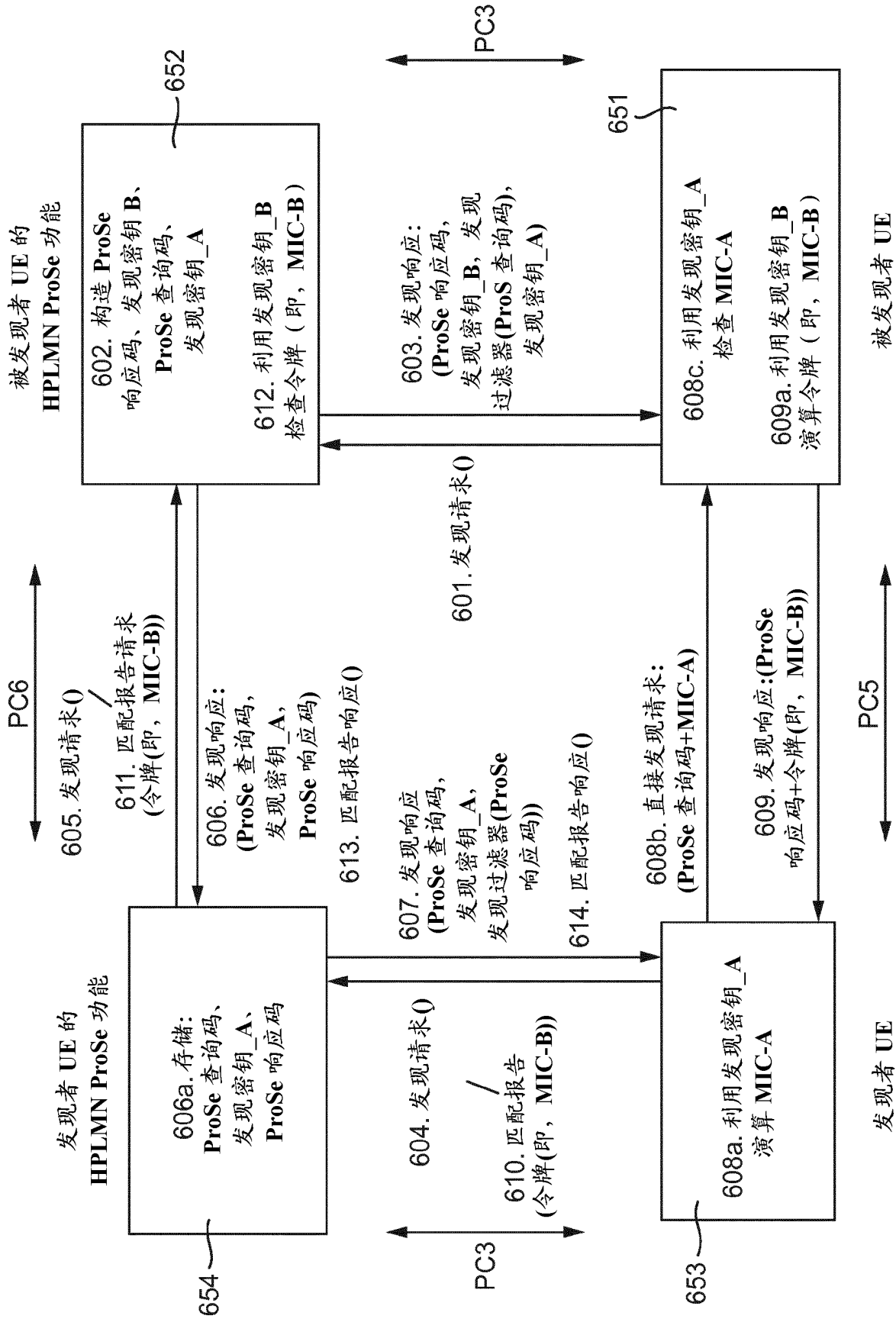


图 6

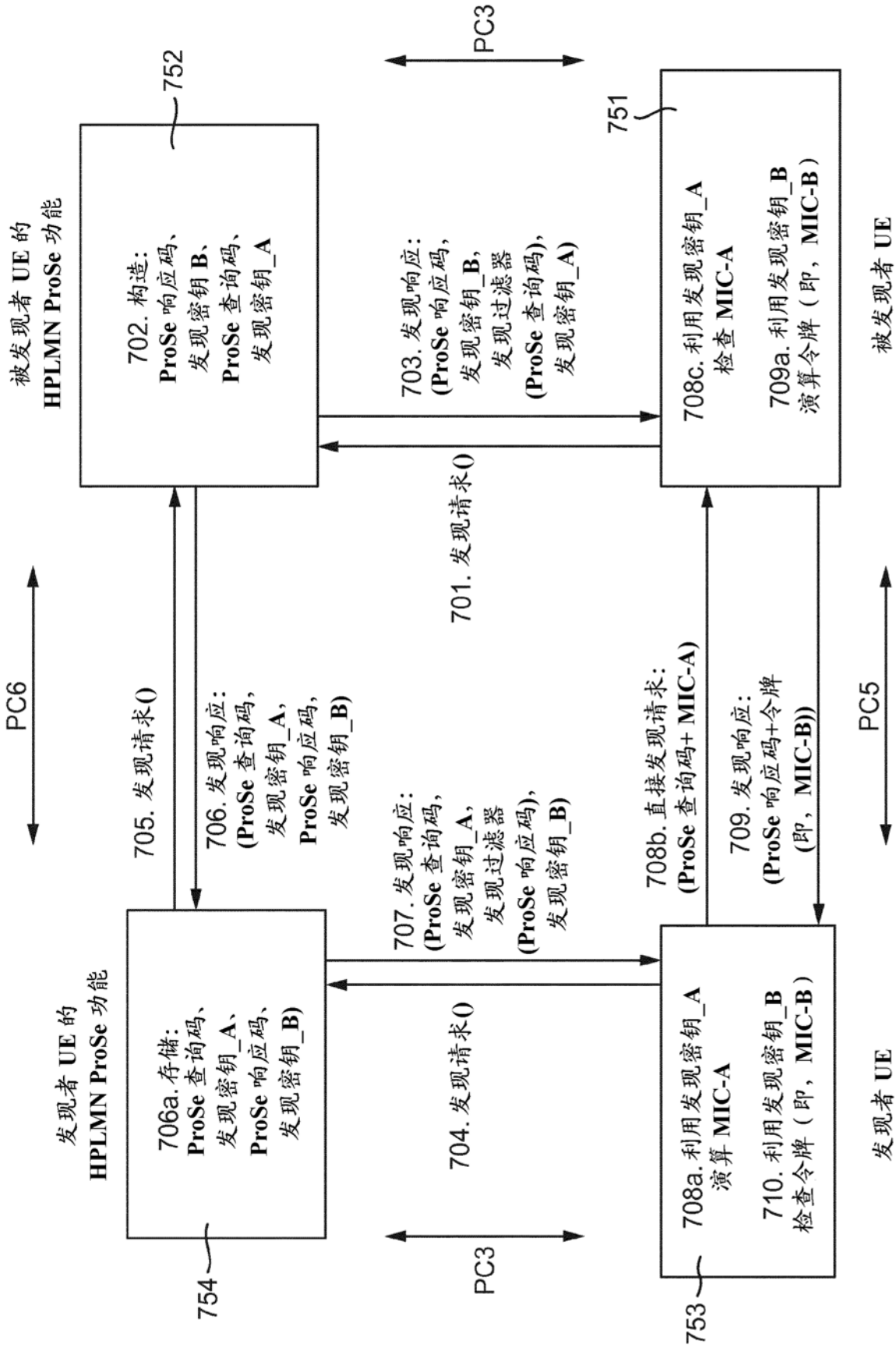


图 7

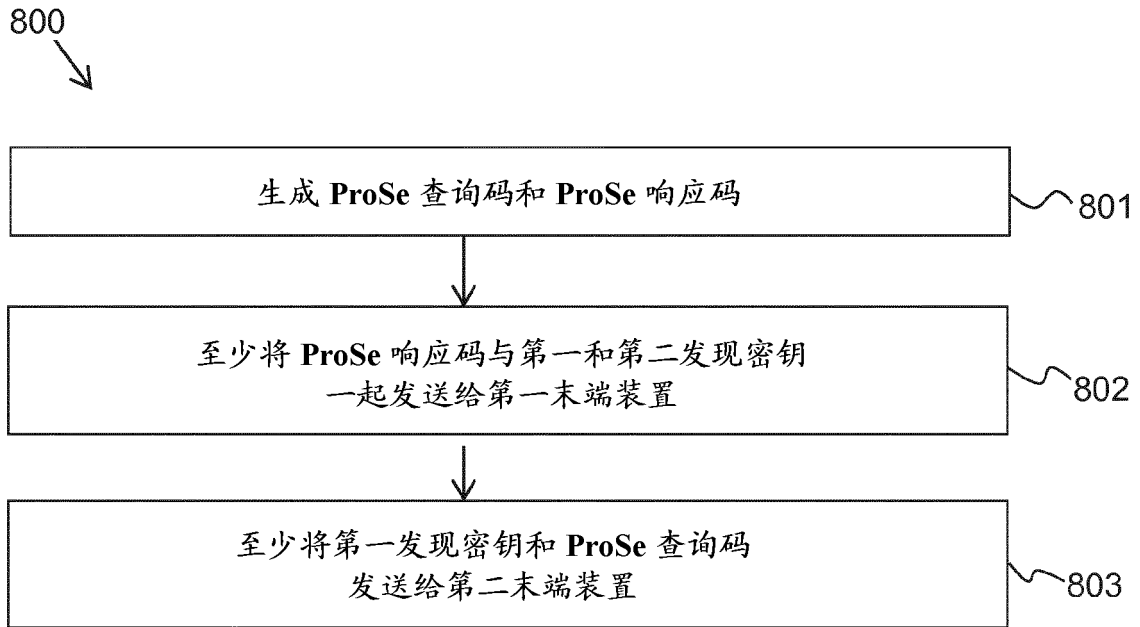


图 8

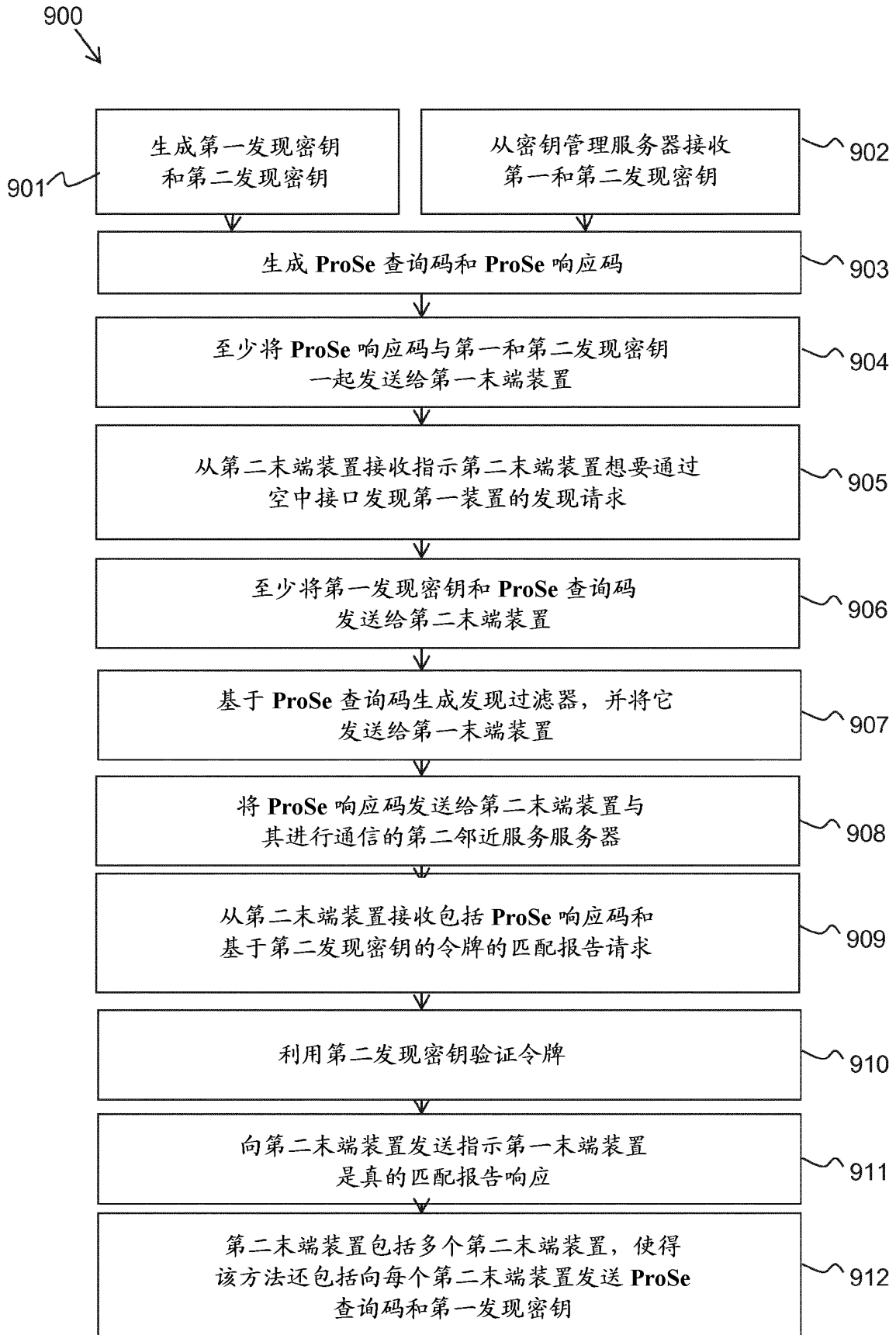


图 9

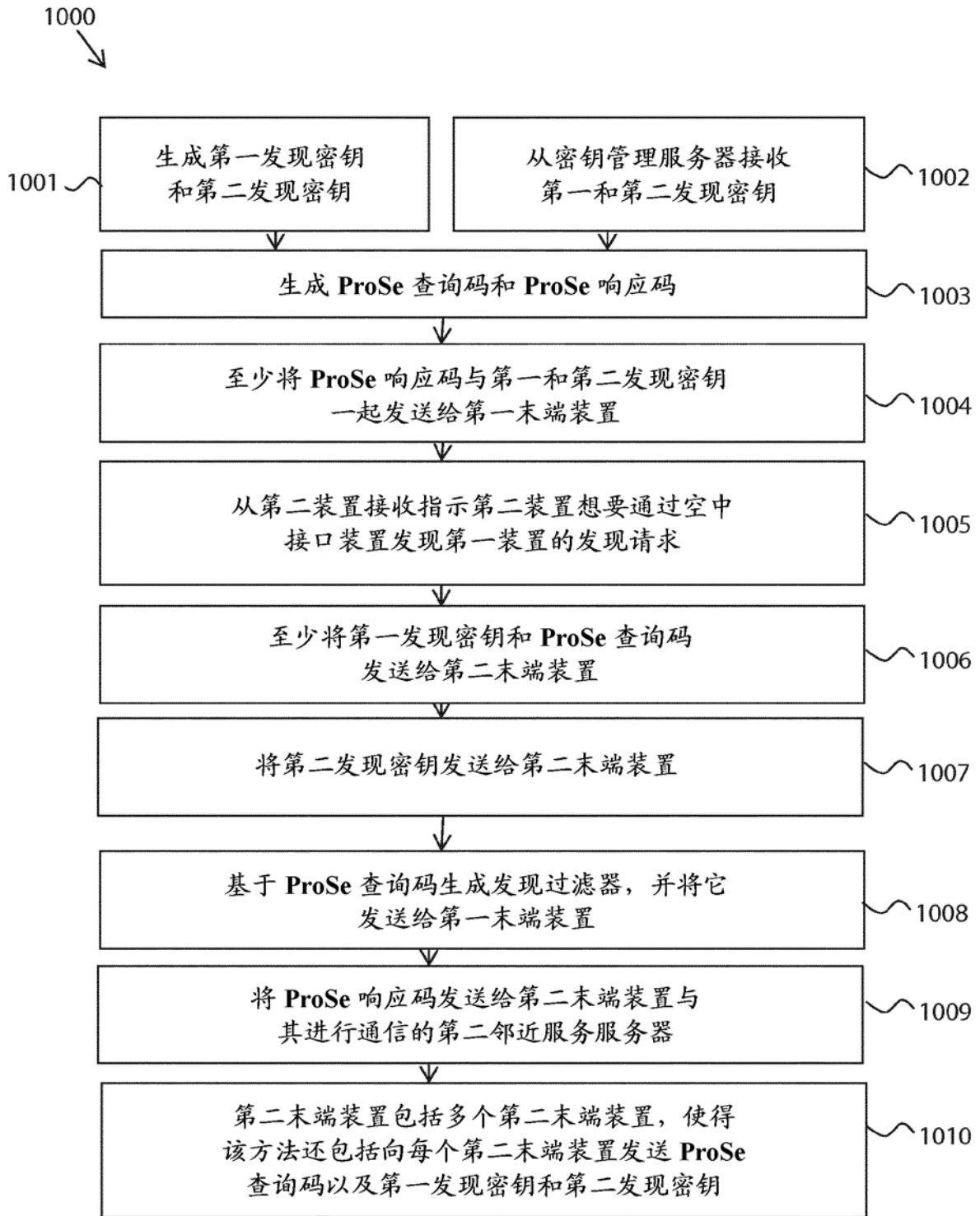


图 10

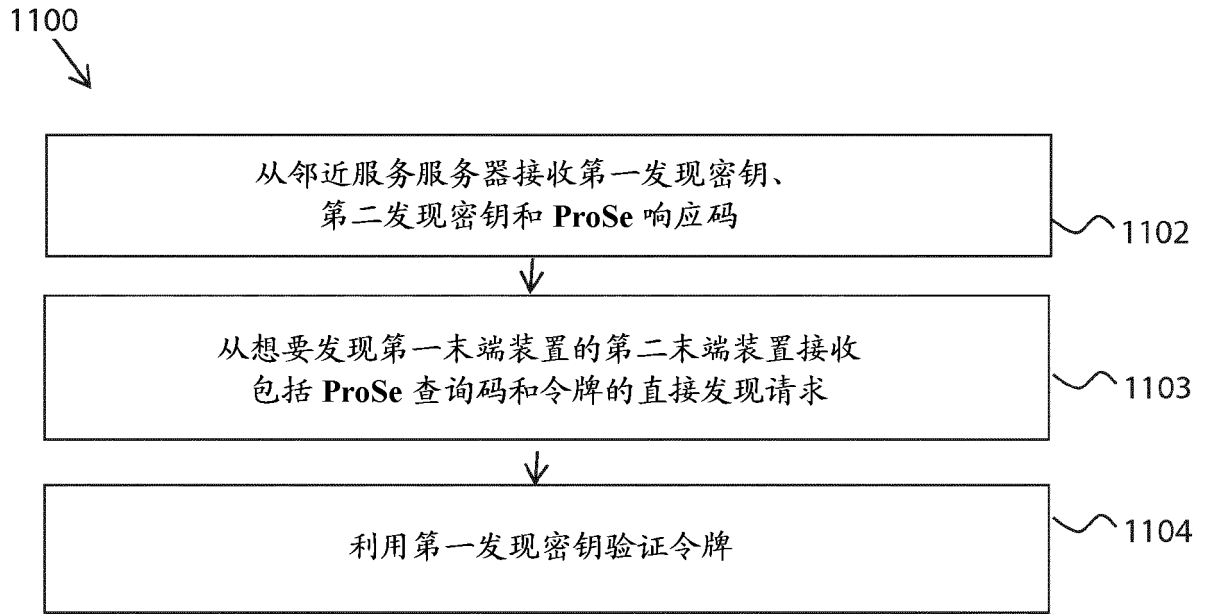


图 11

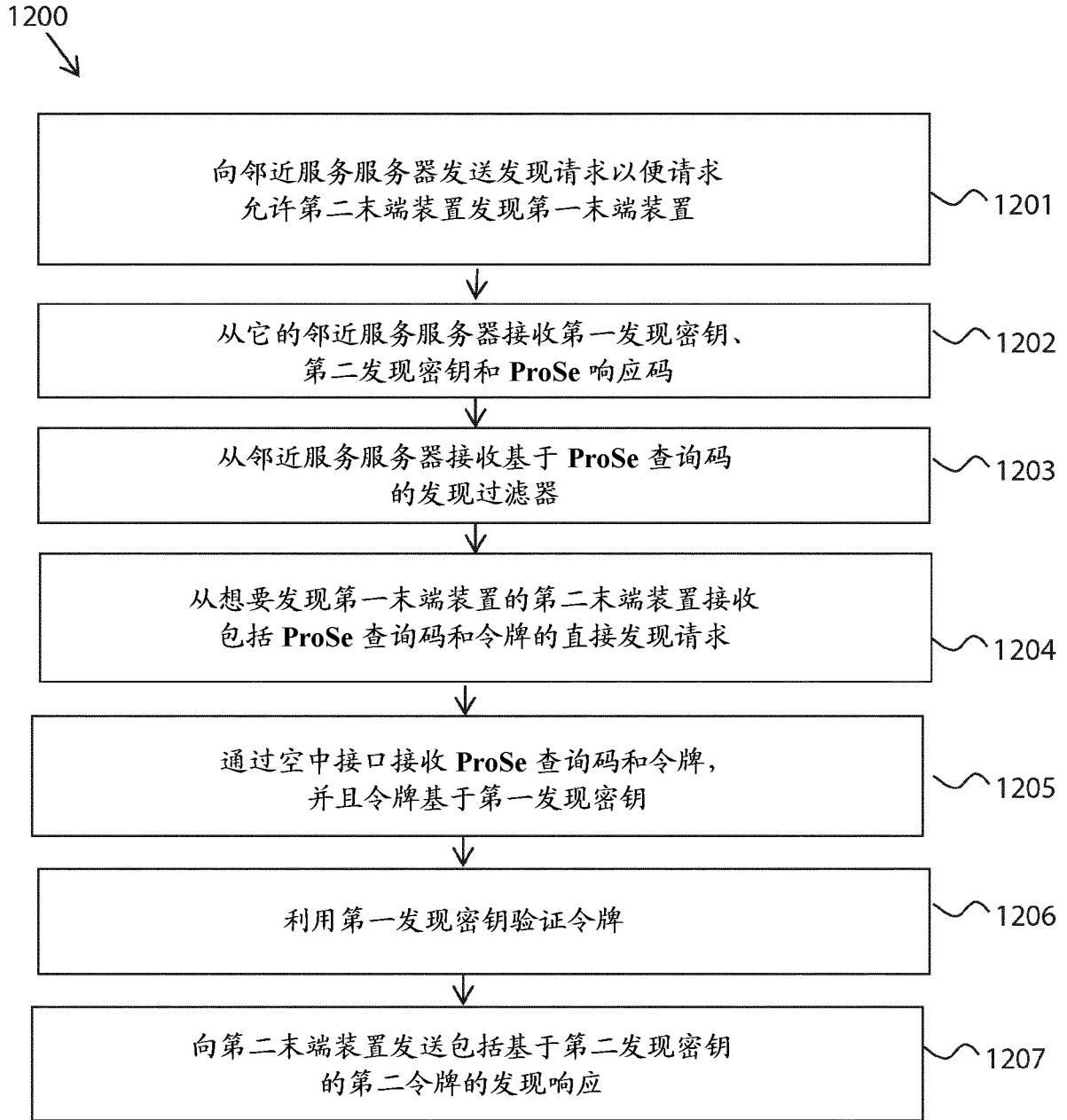


图 12



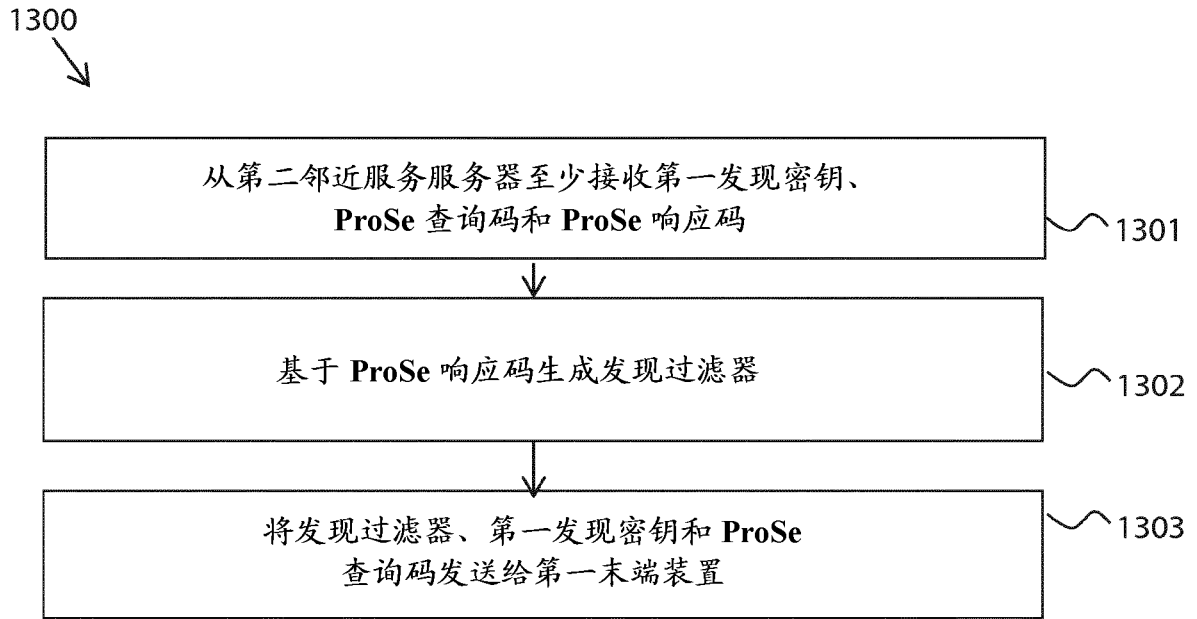


图 13

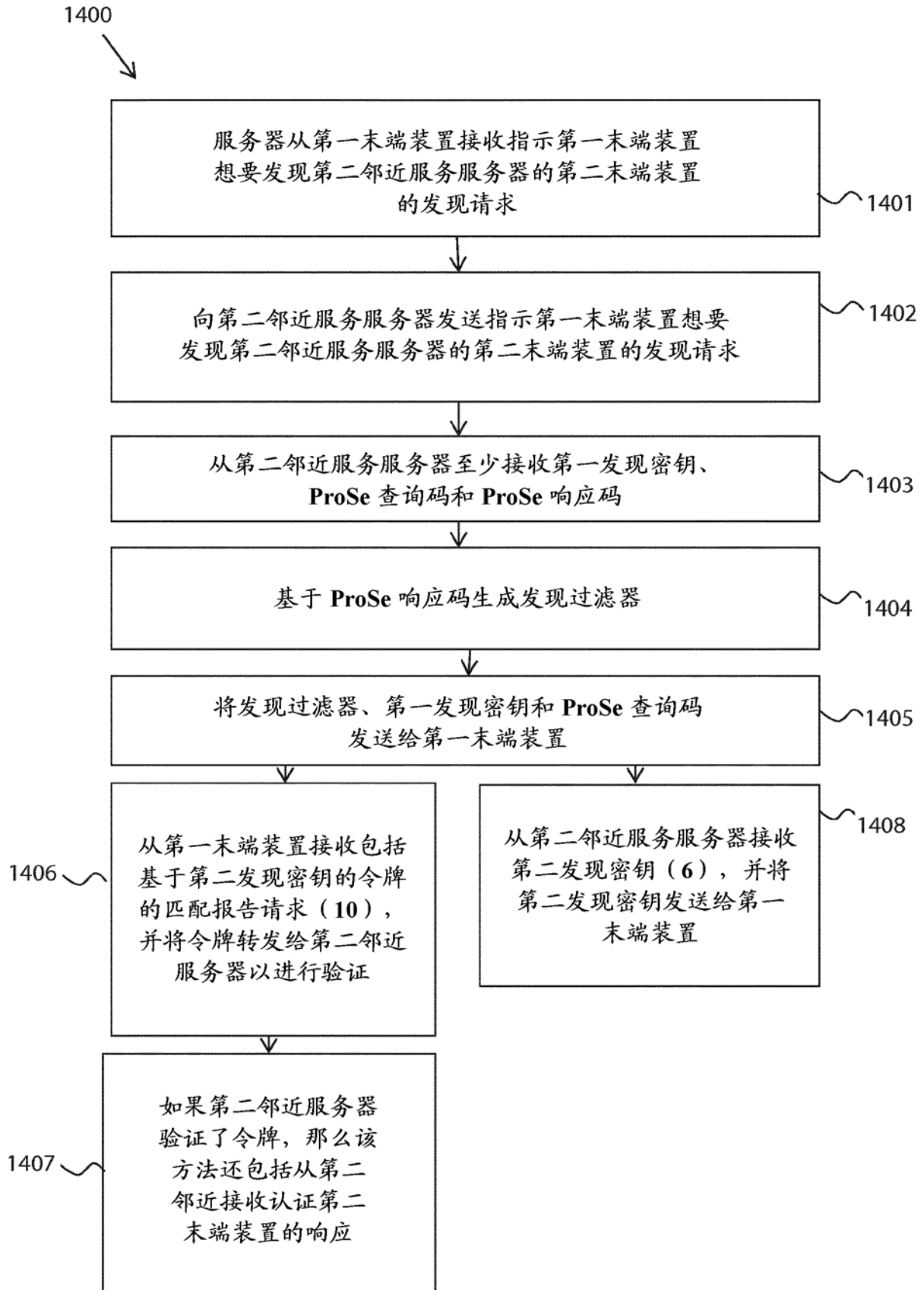


图 14

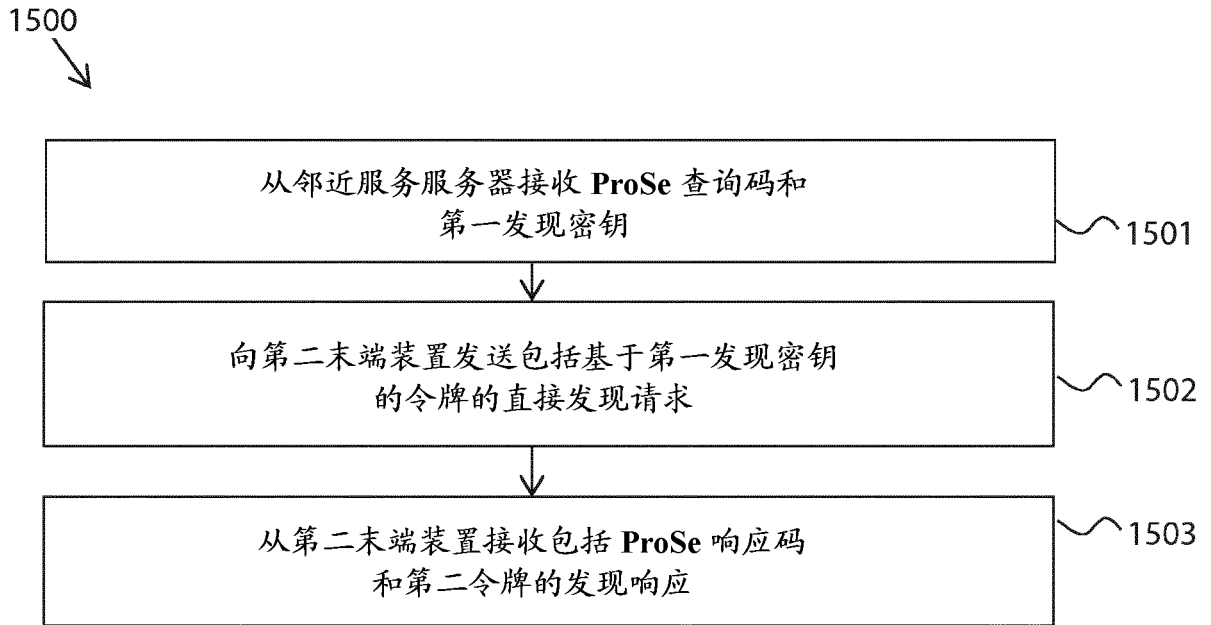


图 15

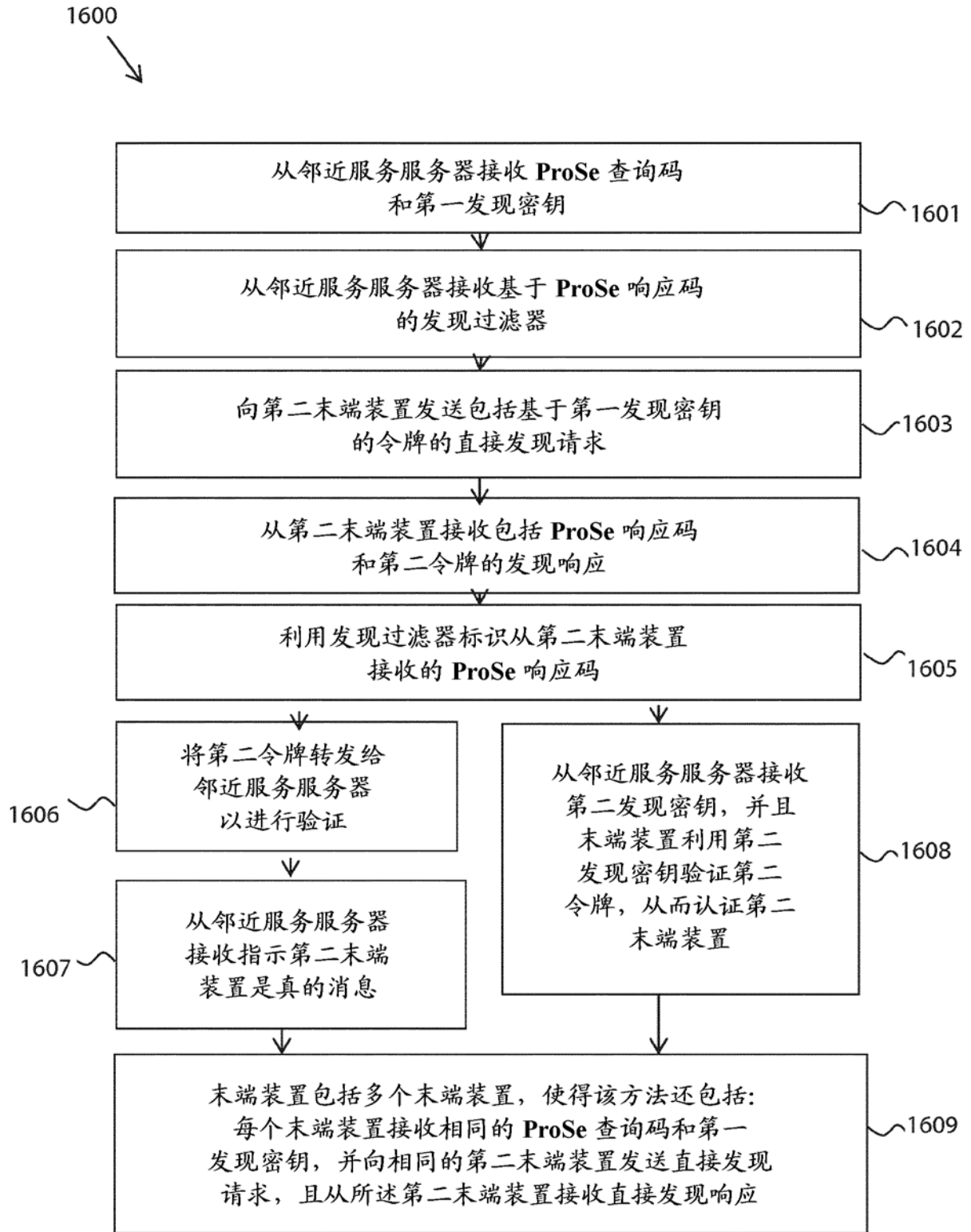


图 16

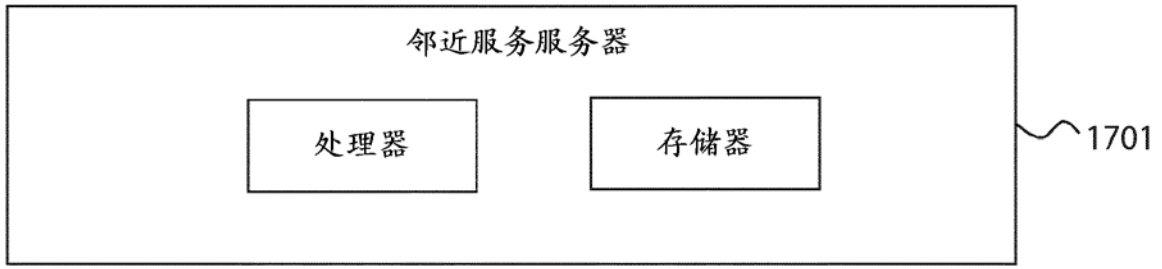


图 17

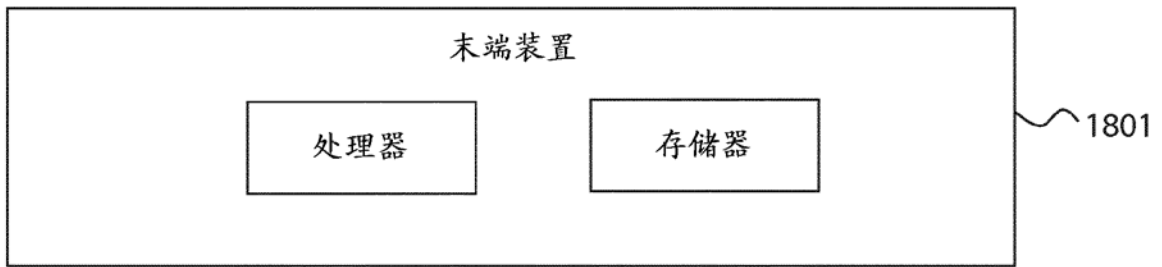


图 18

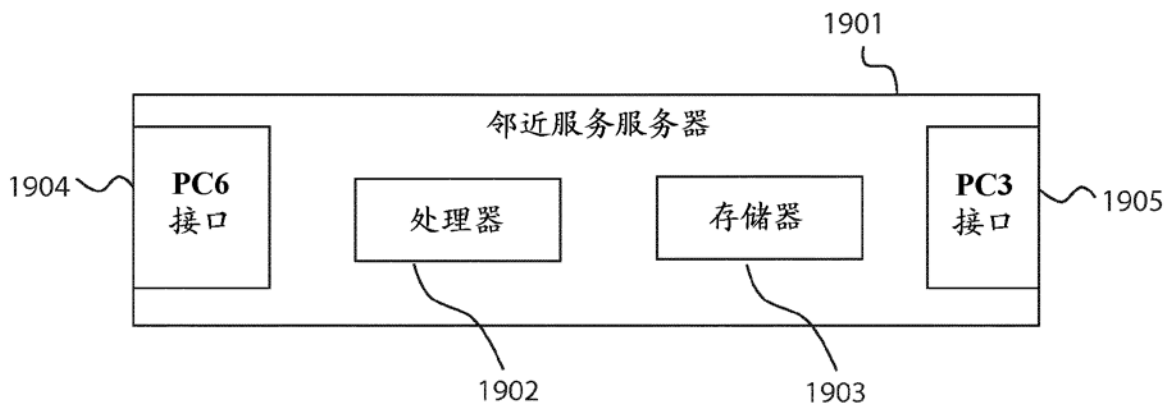


图 19

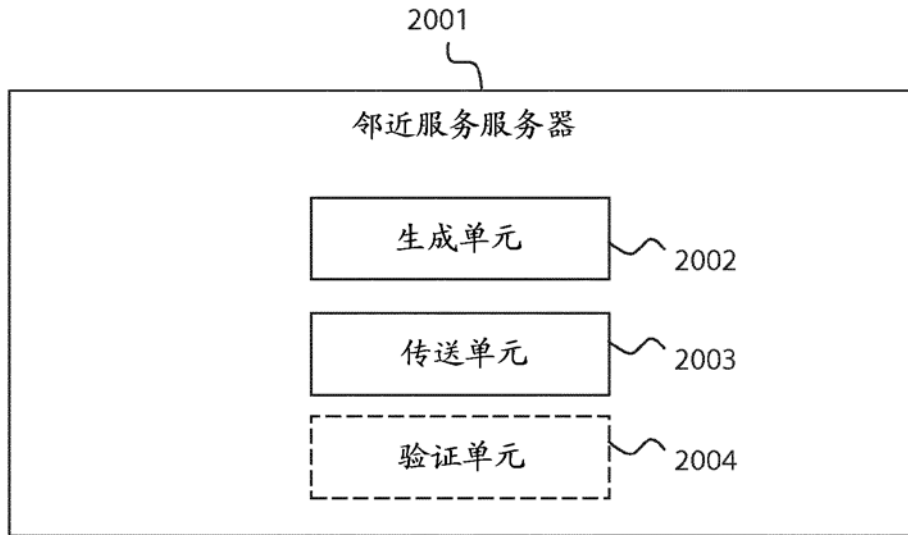


图 20

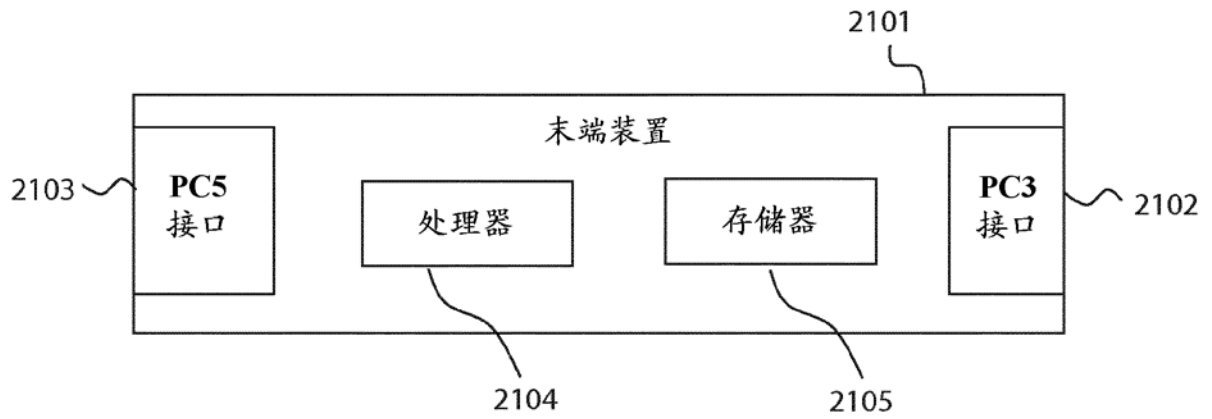


图 21

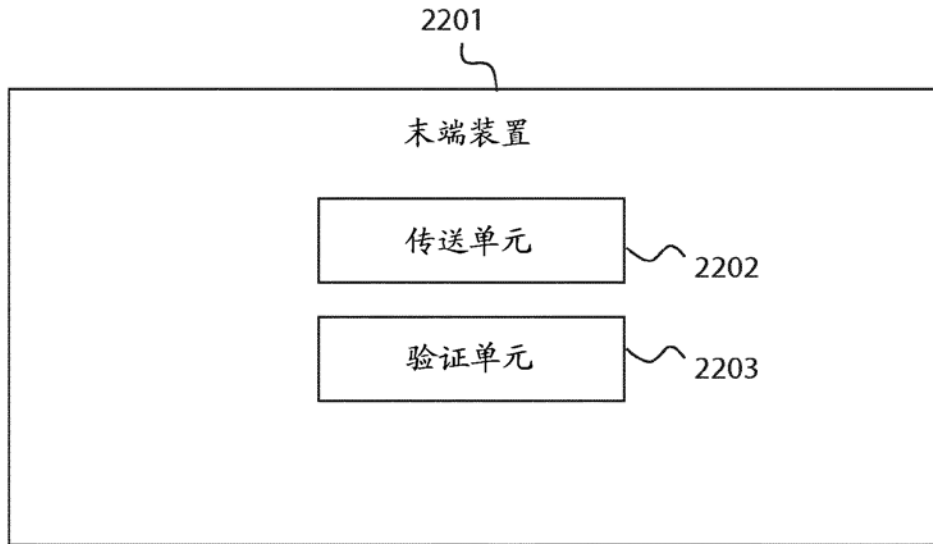


图 22

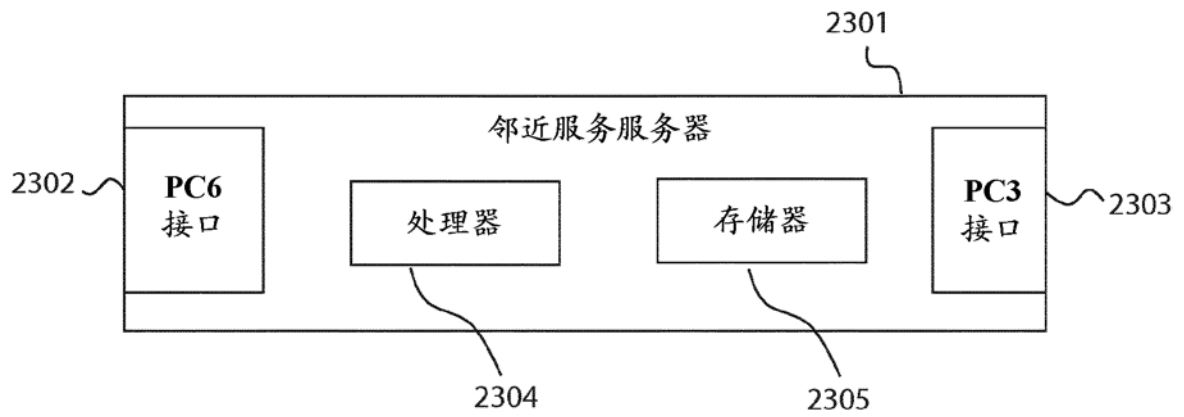


图 23

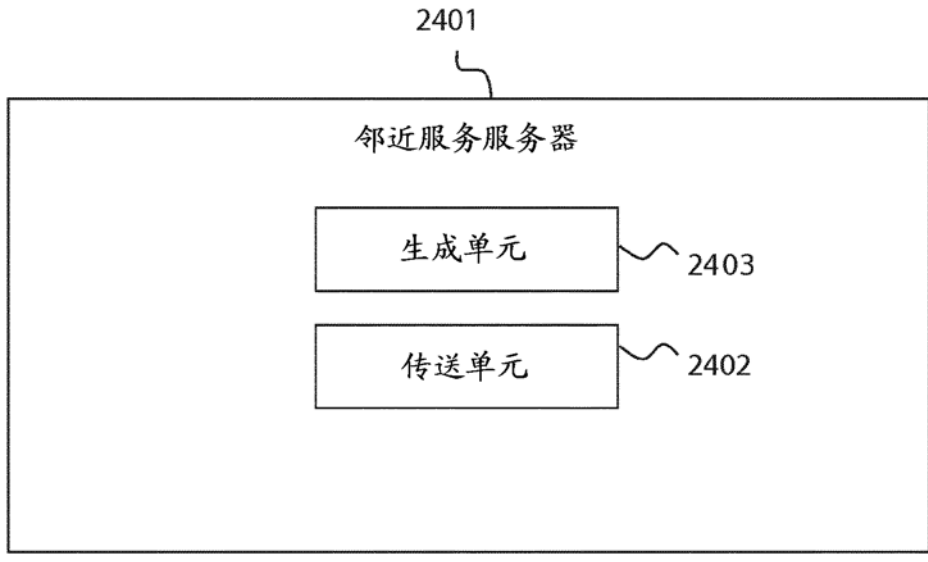


图 24

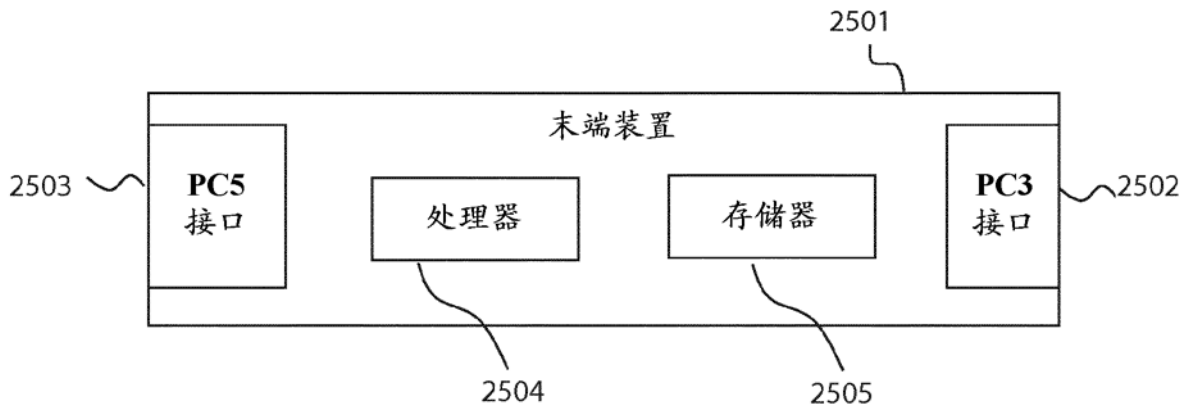


图 25



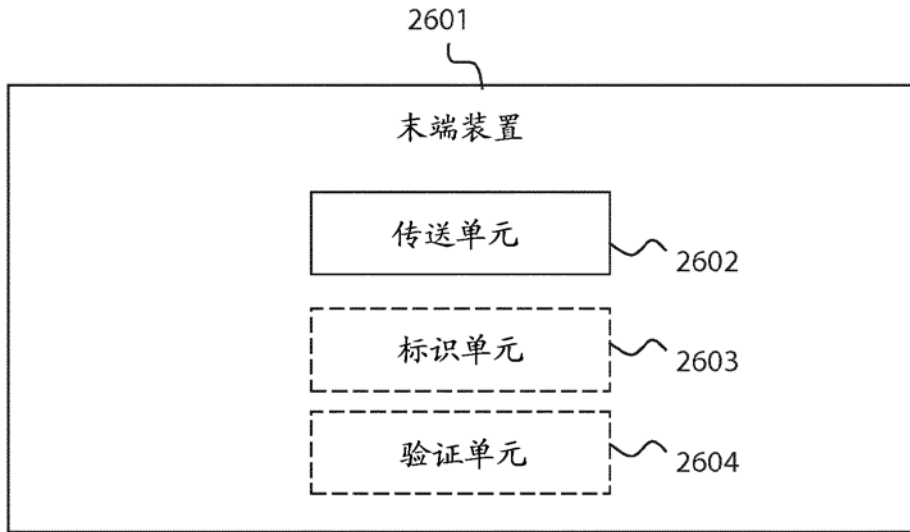


图 26