(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 103621038 A
(43)申请公布日 2014.03.05

(21)申请号 201280030334.2
(22)申请日 2012.07.11
(30)优先权数据
61/506,557 2011.07.11 US
61/645,517 2012.05.10 US
13/545,803 2012.07.10 US
13/545,796 2012.07.10 US
(85)PCT国际申请进入国家阶段日
2013.12.20
(86)PCT国际申请的申请数据
PCT/US2012/046219 2012.07.11
(87)PCT国际申请的公布数据
WO2013/009846 EN 2013.01.17
(71)申请人 甲骨文国际公司
地址 美国加利福尼亚
(72)发明人 B-D·约翰逊 R·安特森
L·P·胡瑟 D·布莱安
O·托卢德巴肯
(74)专利代理机构 中国国际贸易促进委员会专利商标事务所 11038
代理人 冯玉清
(51)Int.Cl.
H04L 29/06(2006.01)
H04L 63/02(2006.01)

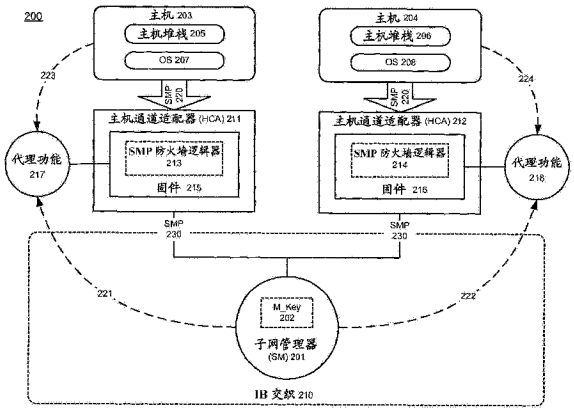
权利要求书4页 说明书10页 附图5页

(54)发明名称

中间件机器环境中支持子网管理数据包防火墙限制和业务保护中的至少一项的系统和方法

(57)摘要

系统和方法可在中间件机器环境中提供子网管理数据包(SMP)防火墙限制。可在主机通道适配器(HCA)上提供安全固件实现,其中HCA与中间件机器环境中的主机相关联。安全固件实现操作来接收来自或发往主机的至少一个SMP,并阻止主机发送或接收至少一个SMP。此外,安全固件实现可包括能代表主机与外部管理组件通信的代理功能。系统和方法可在中间件机器环境中提供基于交换机的SMP业务保护。中间件机器环境包括操作来接收发往子网管理代理(SMA)组件的至少一个SMP的网络交换机。网络交换机可检查至少一个SMP是否包括正确的管理密钥,并当其不包括正确的管理密钥时,阻止其转发到目的地SMA。此外,网络交换机还能为每个外部端口指定不同的管理密钥,并能对特定外部端口处的进入和外出SMP业务强制单独的限制。



CN 103621038 A

1. 一种在运行于一个或多个微处理器上的中间件机器环境中提供子网管理数据包(SMP)防火墙限制的方法,包括 :

在连接到 infiniband (IB)交织的主机通道适配器(HCA)上提供安全固件实现,其中所述 HCA 与主机相关联 ;

通过所述安全固件实现,接收至少一个 SMP,其中所述至少一个 SMP 是从所述主机接收的或者发往所述主机的 ;以及

通过所述安全固件实现,防止所述主机向所述 IB 交织发送所述至少一个 SMP 或接收发往所述主机的所述至少一个 SMP。

2. 根据权利要求 1 所述的方法,还包括 :

在所述安全固件实现中包括 SMP 防火墙组件。

3. 根据权利要求 2 所述的方法,还包括 :

允许所述 SMP 防火墙组件阻止一个或多个基于 SMP 的操作。

4. 根据权利要求 2 或 3 所述的方法,还包括 :

允许所述 SMP 防火墙组件阻止所述主机上的软件和子网管理器之间的基于 SMP 的通信。

5. 根据权利要求 2 到 4 中的任一项所述的方法,还包括 :

实现特殊规则作为所述 SMP 防火墙组件的一部分。

6. 根据权利要求 5 所述的方法,还包括 :

允许所述特殊规则定义特定的基于 SMP 的请求和响应类型以严格控制的速率发送和接收,和 / 或为直接路由 SMP 和本地标识符路由 SMP 二者定义源和目的地限制。

7. 根据任一项前述权利要求所述的方法,还包括 :

允许所述安全固件实现包括代理功能,其中所述代理功能能通过本地带外接口与所述主机上的软件进行通信。

8. 根据权利要求 7 所述的方法,还包括 :

允许子网管理器通过所述代理功能来向所述主机软件发送 SMP。

9. 根据任一项前述权利要求所述的方法,还包括 :

阻止从远程 IB 节点对配置信息的未经授权的检索。

10. 根据权利要求 7 所述的方法,还包括 :

允许所述代理功能负责代表主机堆栈软件来实施特定合法操作。

11. 一种在运行于一个或多个微处理器上的中间件机器环境中提供子网管理数据包(SMP)防火墙限制的系统,包括 :

主机通道适配器(HCA)与之相关联的一个或多个主机 ;以及

所述 HCA 上的安全固件实现,

其中,所述安全固件实现操作来

接收来自所述主机或发往所述主机的至少一个 SMP ;以及

阻止所述主机发送或接收所述至少一个 SMP。

12. 根据权利要求 11 所述的系统,其中 :

所述安全固件实现包括 SMP 防火墙组件。

13. 根据权利要求 12 所述的系统,其中 :

所述 SMP 防火墙组件能阻止一个或多个基于 SMP 的操作。

14. 根据权利要求 12 或 13 所述的系统，其中：

所述 SMP 防火墙组件能阻止所述主机上的软件和子网管理器之间的基于 SMP 的通信。

15. 根据权利要求 12 到 14 中的任一项所述的系统，还包括：

实施为所述 SMP 防火墙组件的一部分的特殊规则。

16. 根据权利要求 15 所述的系统，其中：

所述特殊规则允许特定的基于 SMP 的请求和响应类型以严格控制的速率发送和接收，和 / 或为直接路由 SMP 和本地 ID 路由 SMP 二者定义源和目的地限制。

17. 根据权利要求 11 到 16 中的任一项所述的系统，其中：

所述安全固件实现包括代理功能，其中所述代理功能能够通过本地带外接口与所述主机上的软件进行通信。

18. 根据权利要求 17 所述的系统，其中：

子网管理器操作为通过所述代理功能向所述主机软件发送 SMP。

19. 根据权利要求 11 到 18 中的任一项所述的系统，其中：

所述安全固件实现操作为阻止从远程 IB 节点对配置信息的未经授权的检索。

20. 一种非暂时性机器可读存储介质，其上存储有用于在中间件机器环境中提供子网管理数据包（SMP）防火墙限制的指令，所述指令在运行时使系统执行下列步骤：

在连接到 infiniband（IB）交织的主机通道适配器（HCA）上提供安全固件实现，其中所述 HCA 与主机相关联；

通过所述安全固件实现，接收至少一个 SMP，其中所述至少一个 SMP 是从所述主机接收的或者发往所述主机的；以及

通过所述安全固件实现，防止所述主机向所述 IB 交织发送所述至少一个 SMP 或接收发往所述主机的所述至少一个 SMP。

21. 一种在运行于一个或多个微处理器上的中间件机器环境中提供基于交换机的子网管理数据包（SMP）业务保护的方法，包括：

通过网络交换机，接收发往子网管理代理（SMA）的一个或多个 SMP；

通过所述网络交换机，检查所述一个或多个 SMP 是否包括正确的管理密钥；以及

当所述一个或多个 SMP 不包括正确的管理密钥时，通过所述网络交换机，阻止所述一个或多个 SMP 被转发到目的地 SMA。

22. 根据权利要求 21 所述的方法，还包括：

根据交织策略，过滤所述一个或多个 SMP。

23. 根据权利要求 22 所述的方法，还包括：

允许所述一个或多个 SMP 中的每一个都是直接路由 SMP。

24. 根据权利要求 22 或 23 所述的方法，还包括：

允许子网管理器使用一个或多个 SMP 来通过所述网络交换机上的特定交换机端口与子网管理代理（SMA）进行通信。

25. 根据权利要求 21 到 24 中的任一项所述的方法，还包括：

为所述网络交换机上的每一个外部端口定义不同的管理密钥。

26. 根据权利要求 25 所述的方法，还包括：

允许所述网络交换机对从外部端口向所述 SMA 发送的 SMP 以及在所述外部端口从所述 SMA 接收到的 SMP 强制单独的限制。

27. 根据权利要求 21 到 26 中的任一项所述的方法，还包括：

通过子网管理器，确保与所述 SMA 相关联的不受信任的远程主机通道适配器（HCA）只在指定了正确的管理密钥时才能发出一个或多个 SMP。

28. 根据权利要求 21 到 27 中的任一项所述的方法，还包括：

指定定义远程 HCA 端口被允许多快地生成 SMP 的 SMP 速率。

29. 根据权利要求 21 到 28 中的任一项所述的方法，还包括：

声明一个或多个交换机端口被信任并允许

SMP 请求被从被信任的端口发送，以及

在被信任的端口处接收 SMP 响应。

30. 如权利要求 29 所述的方法，还包括：

只允许 SMA 请求从被信任的端口发送到不被信任的端口。

31. 一种用于在中间件机器环境中提供基于交换机的子网管理数据包业务保护的系统，包括：

子网管理代理（SMA）组件；

在一个或多个微处理器上运行的网络交换机，其中所述网络交换机操作来

接收发往所述 SMA 组件的一个或多个 SMP；

检查所述一个或多个 SMP 是否包括正确的管理密钥；以及

当至少一个 SMP 不包括正确的管理密钥时，阻止所述一个或多个 SMP 被转发到目的地 SMA。

32. 根据权利要求 31 所述的系统，其中：

所述一个或多个 SMP 根据交织策略被过滤。

33. 根据权利要求 32 所述的系统，其中：

所述一个或多个 SMP 中的每一个都是直接路由 SMP。

34. 根据权利要求 32 或 33 所述的系统，其中：

子网管理器能使用一个或多个 SMP 来通过所述网络交换机上的特定交换机端口与子网管理代理（SMA）进行通信。

35. 根据权利要求 31 到 34 中的任一项所述的系统，其中：

为所述网络交换机上的每一个外部端口定义不同的管理密钥。

36. 根据权利要求 35 所述的系统，其中：

所述网络交换机能对从外部端口向 SMA 发送的 SMP 以及在外部端口从 SMA 接收到的 SMP 强制单独的限制。

37. 根据权利要求 31 到 36 中的任一项所述的系统，还包括：

子网管理器，其确保与所述 SMA 相关联的不受信任的远程主机通道适配器（HCA）只在指定了正确的管理密钥时才能发出 SMP。

38. 根据权利要求 31 到 37 中的任一项所述的系统，其中：

所述网络交换机使用 SMP 速率来定义远程 HCA 端口被允许多快地生成 SMP。

39. 根据权利要求 31 到 38 中的任一项所述的系统，其中：

所述网络交换机上的一个或多个受信任的交换机端口允许

SMP 请求被从受信任的端口发送，以及

在受信任的端口处接收 SMP 响应。

40. 一种非暂时性机器可读存储介质，其上存储有用于在中间件机器环境中提供基于交换机的子网管理数据包（SMP）业务保护的指令，所述指令在运行时导致系统执行下列步骤：

通过网络交换机，接收发往子网管理代理（SMA）的一个或多个 SMP；

通过所述网络交换机，检查所述一个或多个 SMP 是否包括正确的管理密钥；以及

当所述一个或多个 SMP 不包括正确的管理密钥时，通过所述网络交换机，阻止所述一个或多个 SMP 被转发到目的地 SMA。

41. 一种计算机程序，包括由一个或多个处理器运行以执行权利要求 1 到 10 或 21 到 30 中的任一项所述的方法的指令。

42. 一种计算机程序产品，包括存储有权利要求 41 的计算机程序的计算机可读介质。

43. 一种用于在中间件机器环境中提供子网管理数据包（SMP）防火墙限制的程序，其导致系统执行下列步骤：

在连接到 infiniband（IB）交织的主机通道适配器（HCA）上提供安全固件实现，其中所述 HCA 与主机相关联；

通过所述安全固件实现，接收至少一个 SMP，其中所述至少一个 SMP 是从所述主机接收的或者发往所述主机的；以及

通过所述安全固件实现，防止所述主机向所述 IB 交织发送所述至少一个 SMP 或接收发往所述主机的所述至少一个 SMP。

44. 一种用于在中间件机器环境中提供基于交换机的子网管理数据包（SMP）业务保护的程序，其导致系统执行下列步骤：

通过网络交换机，接收发往子网管理代理（SMA）的一个或多个 SMP；

通过所述网络交换机，检查所述一个或多个 SMP 是否包括正确的管理密钥；以及

当所述一个或多个 SMP 不包括正确的管理密钥时，通过所述网络交换机，阻止所述一个或多个 SMP 被转发到目的地 SMA。

中间件机器环境中支持子网管理数据包防火墙限制和业务保护中的至少一项的系统和方法

[0001] 版权声明

[0002] 本专利文献公开的一部分包含受版权保护的材料。版权所有者不反对任何人复制本专利文献或专利公开，只要它出现在专商局专利文件或记录中，但保留所有其他版权。

技术领域

[0003] 本发明总体上涉及诸如中间件之类的计算机系统和软件，特别地，涉及支持中间件机器环境。

背景技术

[0004] 互连网络在下一代超级计算机、群集以及数据中心中扮演着有益的角色。在高带宽和低延迟是关键要求的高性能计算领域，诸如 InfiniBand（IB）技术之类的高性能网络技术正在替代专有的或低性能的解决方案。例如，IB 安装用于诸如洛斯阿拉莫斯国家实验室的 Roadrunner、得克萨斯高级计算中心的 Ranger 以及尤里希研究中心的 JuRoPa 之类的超级计算机中。

[0005] IB 在 2000 年 10 月首先被标准化为称为未来 I/O 和下一代 I/O 的两种旧式技术的合并。由于其低延迟、高带宽以及主机侧处理资源的有效利用，高性能计算（HPC）界接受其作为构建大型可缩放计算机群集的解决方案。IB 的事实上的系统软件是 OpenFabrics Enterprise Distribution（OFED），其由专门的专业人员开发并由 OpenFabrics 联盟维护。OFED 是开源的，可用于 GNU/Linux 和 Microsoft Windows 二者。

发明内容

[0006] 此处描述了在中间件机器环境中提供子网管理数据包（SMP）防火墙限制的系统和方法。可以在主机通道适配器（HCA）上提供安全固件实现，其中 HCA 与中间件机器环境中的主机相关联。安全固件实现操作来接收来自主机或发往主机的至少一个 SMP，并且阻止所述主机发送或接收所述至少一个 SMP。此外，安全固件实现可包括可以代表主机与外部管理组件进行通信的代理功能。

[0007] 此处还描述了在中间件机器环境中提供基于交换机的子网管理数据包（SMP）业务保护的系统和方法。中间件机器环境包括操作来接收发往子网管理代理（SMA）组件的至少一个 SMP 的网络交换机。网络交换机可以检查至少一个 SMP 是否包括正确的管理密钥，并且当至少一个 SMP 不包括正确的管理密钥时，阻止至少一个 SMP 被转发到预定的 SMA。此外，网络交换机可以为每一个外部端口指定不同的管理密钥，并且可以对特定外部端口处的进入和外出 SMP 业务强制单独的限制。

附图说明

[0008] 图 1 示出了根据本发明一实施例在中间件机器平台中支持管理密钥保护模型的

图示。

[0009] 图 2 示出了根据本发明一实施例在中间件机器环境中提供 SMP 防火墙限制的图示。

[0010] 图 3 示出了根据本发明一实施例在中间件机器环境中提供 SMP 防火墙限制的示例性流程图。

[0011] 图 4 示出了根据本发明一实施例在中间件机器环境中提供基于交换机的 SMP 业务保护的图示。

[0012] 图 5 示出了根据本发明一实施例在中间件机器环境中提供基于交换机的 SMP 业务保护的示例性流程图。

具体实施方式

[0013] 此处描述了用于提供中间件机器或类似平台的系统和方法。根据本发明一实施例，系统包括高性能硬件例如 64 位处理器技术、高性能大容量存储器以及冗余 InfiniBand 和以太联网与应用程序服务器或诸如 WebLogic 套件之类的中间件环境的组合，以提供完整的 Java EE 应用程序服务器综合体，该综合体包括可以快速地提供并可以按需缩放的大规模并行存储器中网格（in-memory grid）。根据一实施例，系统可以部署为完全、半或四分之一机架或其他配置，其提供应用程序服务器网格、存储区域网络以及 InfiniBand（IB）网络。中间件机器软件可以提供应用程序服务器、中间件和其他功能，诸如，例如 WebLogic Server、JRockit 或 Hotspot JVM、Oracle Linux 或 Solaris 以及 Oracle VM。根据一实施例，系统可包括通过 IB 网络彼此通信的多个计算节点、IB 交换机网关以及存储器节点或单元。当实现为机架配置时，机架的未使用的部分可以是空的或用填充物来填充。

[0014] 根据本发明一实施例，此处称为“Sun Oracle Exalogic”或“Exalogic”的系统是用于托管诸如 Oracle Middleware SW 套件或 WebLogic 之类的中间件或应用程序服务器软件的易于部署的解决方案。如此处所描述的那样，根据一实施例，系统是包括一台或多台服务器、存储器单元、用于存储器联网的 IB 交织（fabric）、以及托管中间件应用程序所需的所有其他组件的“盒中网格”。可以使用例如 Real Application Cluster 以及 Exalogic Open 存储器，通过利用大规模平行网格架构，为各种类型的中间件应用程序提供显著的性能。系统提供改善的性能和线性 I/O 可缩放性，易于使用和管理，并提供任务关键的可用性和可靠性。

[0015] M_Key 保护模型

[0016] 图 1 示出了根据本发明一实施例的中间件机器平台中支持管理密钥保护模型的图示。如图 1 所示，可以使用诸如 M_Key102 之类的管理密钥来保护 IB 交织（或 IB 子网）100。M_Key102 的值可以仅由交织管理员 110 知道，交织管理员 110 可以具有对交换机 103-104 以及 IB 子网 / 交织 100 中指定的子网管理器（SM）节点 101 的管理员访问权。M_Key102 的完整性取决于交织管理员 110 所使用的交织级别的管理密码的完整性以及 IB 子网 / 交织 100 中（例如，在数据中心中）的交换机 103-104 的物理访问保护。

[0017] 在 IB 交织 100 中，HCA121-124 中的安全 HCA 固件实现可以使各种交织节点的类型和身份被明确定义。HCA121-124 中的每一个可以实现子网管理代理（SMA）组件 131-134，其每一个都可以与 M_Key141-144 相关联。此外，连接的交换机 A-B103-104 可以由交织管

理员 110 控制。如此，任何非法 SMA 实现 131-134 都可以不损害交织管理员 110 定义的用于 IB 子网 / 交织 100 中的 M_Key102 值。

[0018] 在 2012 年 6 月 4 日提交的题为“SYSTEM AND METHOD FOR PROVIDING SECURE SUBNET MANAGEMENT AGENT(SMA)IN AN INFINIBAND(IB)NETWORK”的美国专利申请 13/487973 中提供了在中间件机器平台中使用安全 HCA 固件实现的各种实施例的额外描述，该申请通过引用合并于此。

[0019] 此外，交织管理员 110 可以确保，IB 子网 / 交织 100 的新 M_Key 值 102 带外 (out-of-band) 安装在交换机 103-104 上 (以及用于相关子网管理器实例 101)。另外，交织管理员 110 可以确保，在交换机 103-104 上有无限的 M_Key102 租用时间。如此，基于主机的软件 161-164，例如不同主机 111-114 上的基于主机的子网管理器 (包括操作系统 151-154)，不能劫持对 IB 子网 / 交织 100 中任何交换机 103-104 的控制。

[0020] 根据本发明一实施例，基于 IB 规范定义的访问限制，单个 M_Key102 值 (或单组 M_Key 值) 可以用于 IB 子网 / 交织 100 中的各种节点。当前 M_Key102 的正确值可能需要在读取或更新 M_Key102 之前指定，因为安全 HCA 固件可以确保分配给本地 HCA121-124 的“读取保护”M_Key 不暴露到基于本地主机的软件。

[0021] 另外，在 HCA 端口的当前 M_Key 值在运行时定义的情况下，不同主机 111-114 上的本地软件 161-164 能够通过设置其自己的 M_Key 值来劫持 HCA 端口。此外，主机本地软件 161-164 可以使 HCA 端口对于指定的子网管理器 101 是不可管理的，例如，在指定的子网管理器 101 设置用于 HCA121-124 的任何 M_Key102 之前。

[0022] 根据本发明一实施例，指定的子网管理器 101 可以忽略具有未知 M_Key 值的任何 HCA 端口，并保留对应的链路未被初始化。被劫持的 HCA 端口 M_Key 的唯一影响可以是，HCA 端口可能不操作，指定的子网管理器 101 可以防止基于主机的软件使用普通通信 (即，非 SMP/VL15 类的通信) 通过此 HCA 端口来进行通信。

[0023] 此外，当主机软件 111-114 破坏本地 HCA M_Key 值时，违规的主机软件能够用激活的本地标识符 (LID) 和分区成员资格使 HCA 端口进入操作状态。在这种情况下，如果连接到 HCA121-124 的交换机 103-104 上的交换机端口由损害了本地 HCA M_Key 值的主机软件 111-114 不知道的不同 M_Key 值控制，那么违规的主机软件 111-114 可能不能使链路进入允许正常数据业务的完全操作状态。

[0024] 根据本发明一实施例，IB 交织 100 可以防止各种主机 111-114 之间的直接路由 SMP，以便避免各种潜在的威胁情况。在一种情况下，在远程主机 112 和 / 或远程 HCA122 复位之后，主机 (例如主机 111) 可以使用直接路由 SMP 来劫持远程主机 (例如 112) 上的 HCA 端口的 M_Key。这会导致远程 HCA122 端口变得无法从 SM101 访问，并由此阻止远程主机 112 参与正常 IB 通信，即拒绝服务 (DoS) 攻击。在另一种情况下，当两个主机 (例如主机 111 和主机 114) 被黑客所破坏时，IB 交织 100 中的依赖于直接路由 SMP 的协作管理可以允许两个被损害的主机使用直接路由 SMP 来交换信息。

[0025] IB 交织 100 可以支持协作管理以用于在不同主机 111-114 之间交换信息而不依赖于直接路由 SMP。例如，主机的管理员可以访问因特网上的共享网络页面，代替依赖于 IB 交织 100 中的直接路由 SMP。从交织安全的角度来看，将直接路由 SMP 保留为 IB 交织上的安全漏洞可以视为比允许两个主机管理员访问因特网上的共享网络页面更差的情况。

[0026] 根据本发明一实施例，可以利用 M_Key102 上的有限的租用时间来设置 HCA 端口，例如，由于维护 M_Key102 租用时间长度的子网管理器 101 的高可得性顾虑。如此，M_Key102 可以过期，而不会有相关联的链路失效。因此，HCA121-124 的状态（例如分区成员资格）可以更新，而链路仍处于有效模式，所涉及的端口的 LID 路由仍可操作。然后，没有 M_Key 保护的 IB 交织 100 可以错误地允许被劫持的主机和其他分区中的主机之间的正常 IB 业务。

[0027] 此外，如果 M_Key102 在链路失效之前过期，则本地 HCA（例如 HCA121）和任何远程 HCA（例如 HCA124）可能被劫持，分区成员资格可能被修改。如果相关联的交换机端口（例如交换机 103-104 上的）没有被设置以执行分区强制，那么带有非请求的分区成员资格的业务可以到达交织中的任何其他节点。

[0028] 另外，IB 交织 100 内的子网管理器 101 可以依赖于指定的虚拟车道（VL），例如 VL15 缓冲，以便正确地监视和控制 IB 交织 100，并与 IB 交织 100 中的其他子网管理器协商。由于 IB 交织 100 内的 VL15 缓冲是共享资源，因此对来自任何主机的 SMP 的不受控制的使用可以表示 DoS 攻击。这会影响子网管理器 101 的操作，因为 IB 交织 100 内的 M_Key 保护可能会阻止主机改变任何节点上的任何 SMA 状态。如此，需要在 IB 交织 100 中提供 SMP 业务保护。

[0029] 根据本发明一实施例，M_Key102 可由交织管理员 110 创建和管理，并且存储在交换机 A-B103-104 和 / 或 HCA121-124 上的安全存储器中。交换机 A-B103-104 或 HCA121-124 上的微处理器可以访问存储器，以便读出 M_Key102 或将 M_Key102 写入到存储器中。

[0030] SMP 防火墙限制

[0031] 根据本发明一实施例，安全 HCA 固件可以使用 SMP 防火墙限制，以防止基于主机的软件劫持本地或远程 HCA 端口。SMP 防火墙限制可以防止主机软件在交织上发出 SMP 请求，并可以拒绝否则将被转发到主机软件的任何 SMP。

[0032] 图 2 示出了根据本发明一实施例在中间件机器环境中提供 SMP 防火墙限制的图示。如图 2 所示，中间件机器环境 200 可以包括一个或多个主机 203-204 以及与子网管理器 201 相关联的 IB 交织 210。每一个主机 203-204 都通过实现了 HCA 固件 215-216 的 HCA211-212 连接到 IB 交织 210。

[0033] HCA 固件 215-216 可包括 SMP 防火墙组件 213-214，它们可以有效地防止任何基于 SMP 的拒绝服务（DoS）攻击，例如以子网管理器 201 的操作为目标，并允许来自交织 200 中的受信任节点合法地使用基于 SMP 的工具。HCA SMP 防火墙组件 213-214 可以防止主机堆栈软件 205-206 向 IB 交织 210 发送 SMP220。此外，为了防止远程节点例如主机 204 的信息被非法提供给本地主机软件，例如主机软件 205，安全 HCA 固件 215 可以拒绝从 IB 交织 210 接收到的 SMP230，否则其将被转发到主机软件 205。

[0034] 另外，SMP 防火墙组件 213-214 还可以防止主机堆栈软件 205-206 的各种基于 SMP 的操作，例如，当子网管理器 201 不可操作时观察本地连接的交换机端口的身份。此外，可以防止来自子网管理器 201 或交织中的其他合法组件的与主机堆栈软件 205 的任何基于 SMP 的通信。

[0035] 根据本发明一实施例，安全 HCA 固件 215-216 可以实现特定规则，作为 SMP 防火墙组件 213-214 的一部分，以便确保对于主机堆栈软件 205-206，合法的操作被允许。这些规则允许特定的基于 SMP 的请求和响应类型被以严格控制的速率发送和接收。此外，这些规

则可以定义用于直接路由和 LID 路由 SMP 二者的源和目的地限制。

[0036] 另外，这些规则可以允许对当前正在控制与 HCA 实例 211-212 相关联的物理主机 203 和 204 的 OS207 和 208 或管理程序实例的基于 SMP 的认证。在 2012 年 6 月 4 日提交的题为“SYSTEM AND METHOD FOR AUTHENTICATING IDENTITY OF DISCOVERED COMPONENT IN AN INFINIBAND(IB)NETWORK”的美国专利申请 13/488040 中提供了在中间件机器平台中认证所发现的组件的各种实施例的进一步描述，该申请通过引用合并于此。

[0037] 根据本发明一实施例，安全 HCA 固件 215 可以实现代理功能 217-218，以便确保对于主机堆栈软件 205-206，合法的操作被允许。诸如子网管理器 201 之类的外部管理组件可以通过代理功能 217-218 向主机堆栈软件 205-206 发送供应商 SMP221。主机堆栈软件 205-206 可以通过 HCA 固件 215-216 和主机堆栈软件 205-206 之间的本地带外接口 223-224 与代理功能 217-218 进行通信。然后，此代理功能 217-218 可以代表主机堆栈软件 205-206 来负责实施特定的合法操作，并代表远程交织管理组件例如子网管理器 201 来负责与主机堆栈软件 205-206 进行通信。

[0038] 安全 HCA 固件 215-216 可以保护 IB 交织 210 免于未授权的对配置信息的检索，例如防止本地主机软件观察有关远程 IB 节点的信息，诸如可以潜在地用作针对远程 IB 节点的 DOS 攻击的基础的全局唯一标识符(GUID)、LID 以及分区成员资格。此外，安全 HCA 固件 215-216 还允许本地 HCA211-212 通过限制观察可以被用来允许与有效子网管理器背后的远程节点的正常数据通信的有关远程节点的信息的能力，来适当地保护其本地 M_Key202 设置免于被本地主机访问。

[0039] 另外，安全 HCA 固件 215-216 还可以防止旧式基于 SMP 的诊断和监视工具从不受信任的主机使用(或不能工作)，因为安全 HCA 可以阻止从不受信任的主机发送的任何 SMP 操作。此外，M_Key 方案还可以与完全读保护一起使用，这可以限制使用依赖于 SMP 的旧式工具的能力。

[0040] 此外，安全 HCA 固件 215 还可保护 IB 交织 200 免于不受信任的主机之间进行的未授权的基于 SMP 的通信。安全 HCA 固件 215 可以保护 IB 交织 210 免于未授权的 SMP 业务，其可能对例如以 SM201 的操作为目标的 DoS 攻击敏感。各种准入控制策略可以将不同主机 203-204 的 SMP 注入速率限制到可接受的水平。可另选地，单个子网的配置可以阻止来自未受信任的主机的所有 SMP 操作，例如使用安全 HCA 固件中的 SMP 阻止特征，以便进一步防止 DOS 攻击。

[0041] 另外，安全 HCA 固件 215 可以保护 IB 交织 210 免受针对子网管理员(SA)访问权的 DoS 攻击。安全 HCA 固件 215 可以保证访问 SA 的 QoS/ 公平性和可缩放性。此外，为了提供 DoS 保护，SM201 可以被允许关闭正在生成 SA 请求的“过载”的 HCA 端口，例如，超出某时间间隔的请求速率阈值。

[0042] 图 3 示出了根据本发明一实施例在中间件机器环境中提供 SMP 防火墙限制的示例性流程图。如图 3 所示，在步骤 301 中，可以在连接到 infiniband (IB)交织的主机通道适配器(HCA)上提供安全固件实现，其中 HCA 与主机相关联。然后，在步骤 302 中，安全固件实现可以接收至少一个 SMP，其中该至少一个 SMP 要么被从主机接收到，要么以主机为目的地。另外，在步骤 303 中，安全固件实现可以阻止主机向 IB 交织发送该至少一个 SMP 或接收以主机为目的地的该至少一个 SMP。

[0043] 基于交换机的代理 M_key 保护

[0044] 根据本发明的一实施例，可以在 IB 交织中的中间交换机节点中执行对 SMP 的 M_Key 检查，以确保本地交换机 M_Key 设置可以保护没有建立 M_Key 的远程 HCA 端口。

[0045] 图 4 示出了根据本发明一实施例在中间件机器环境中提供基于交换机的 SMP 业务保护的图示。如图 4 所示，中间件机器环境 400 可以包括通过 HCA402 连接到主机 403 的 IB 交换机 401。主机 403 可包括在操作系统 407 上运行的主机堆栈软件 405。IB 交换机 401 可包括一个或多个交换机端口 411-416，每一个交换机端口都可以用于与 IB 交织 400 中的单独的节点或实体进行连接，例如交换机端口 411 与 HCA402 连接。

[0046] 在 HCA402 上的固件 404 中实现的子网管理代理（SMA）组件 406 可以通过交换机端口 411 与 IB 交织 400 中的其他节点进行通信。此外，IB 交织 400 中指定的子网管理器 408 还可以使用特定交换机端口例如端口 411 用于向任何 SMA406 发送直接路由 SMP 请求以及从 SMA406 接收直接路由 SMP 响应。

[0047] 交换机 401 可以阻止不想要的 SMP 业务出现在 IB 交织 400 中，无需依赖于要求所有 HCA 都具有带 SMP 控制的受信任的固件。例如，交换机 401 可以过滤与 IB 交织 400 的交织策略不一致的直接路由 SMP 业务。

[0048] 交换机 401 可以使用过滤方案来阻止远程 HCA 端口 402 被入侵者劫持。过滤方案可以基于标识以设置 SMA406 属性为目标的任何直接路由 SMP 请求。另外，过滤方案可以与目的地无关，对所有直接路由 SMP 请求执行相同的 M_Key 检查，并可以要求直接路由 SMP 请求包括用于本地交换机 401 的正确的 M_Key409，与 SMP 针对的目的地无关。

[0049] 单个 M_Key409 可以用在包括交换机 401 和直接连接到交换机 401 的 HCA 端口 402 的 IB 交织 400 中。如果主机堆栈软件 405 能够损害保护本地 HCA402 的 M_Key419，那么主机堆栈软件 405 也可能损害保护本地交换机 401 的 M_Key409，因为 IB 交织 400 中的 SMP 业务包括本地交换机 M_Key409。

[0050] 根据本发明一实施例，交换机 401 的实现可以为每一个外部端口指定可选的 M_Key 值，例如用于外部端口 411-416 的 M_Key421-426。另外，交换机 401 的实现可以确保，从交换机端口例如交换机端口 411 发出的任何 SMP 以及从此端口接收到的任何 SMP 都具有与为交换机端口 411 指定的 M_Key421 匹配的 M_Key 值。此外，网络交换机 401 还可以对从外部端口 414 发送的 SMP420 和在外部端口 414 处接收到的 SMP410 强制单独的限制。

[0051] 利用此机制，合法的子网管理器 408 可以确保，所有潜在不受信任的远程 HCA 端口或其他潜在不受信任的远程端口只有在指定了与交换机端口相关联的正确的本地 M_Key 时才可被允许发出 SMP。此外，访问远程端口的尝试可能需要具有子网管理器 408 为该端口定义的 M_Key，而与远程端口的 M_Key 是否被劫持无关。另外，此机制还可以指定定义远程端口可以多快地生成 SMP 的 SMP 速率，以防止或降低交织中来自不受信任的端口基于 SMP 的 DoS 攻击的机率。

[0052] 2004 年 6 月 2 日提交并且在 2008 年 7 月 8 日公告的题为“SYSTEM AND METHOD FOR AUTHENTICATING NODES IN A COMMUNICATION NETWORK”的美国专利 No.7398394 中提供了在中间件机器平台中使用 SMP 过滤的各种实施例的额外描述，该申请通过引用合并于此。

[0053] 根据本发明一实施例，过滤方案可以基于将交换机端口声明为“受信任的”或者

“不受信任的”，来阻止非法的基于主机－主机的直接路由 SMP 业务。对交换机端口或连接到交换机端口的实体是否受信任的判断可以基于输入到本地交换机 401 的显式策略或者远程端口的自动认证。

[0054] 如图 4 所示，交换机端口 411、413-414 以及 416 是受信任的交换机端口，而交换机端口 412 和 415 是不受信任的。过滤方案可以仅允许 SMP 请求从受信任的端口发送（离开交换机），由受信任的端口接收 SMP 响应（进入交换机）。另外，只有一开始就从受信任的端口进入子网的 SMA 请求可以被允许外出到不受信任的端口。如此，可以使过滤方案独立于任何当前 M_Key 设置，还可以与上面的基于 M_Key 的过滤方案一起使用。

[0055] 根据本发明一实施例，在整个 IB 子网／交织 400 中使用单个 M_Key409 或单组 M_Key 的能力取决于是否 IB 交织 400 中的所有节点是受信任的并且不向没有所要求的特权的任何实体暴露在使用中的 M_Key。子网管理器 408 在请求中包括当前 M_Key 的先决条件是，子网管理器 408 可以确信，目标和任何中间代理不会损害 M_Key 的完整性。在一示例中，可以在在任何 SMP 中包括当前 M_Key 之前建立这样的信任性。如此，交织配置可以要求在可以发生任何基于 M_Key 的通信之前，IB 交织中的所有节点（包括 HCA）被认证（或声明）为受信任的，而不是先验地假设所有 SMA 实例都是可信任的。

[0056] 根据本发明一实施例，可以提供通过交换机管理接口来发送和接收基于供应商的 SMP 的机制。这样的机制允许交换机嵌入式认证机制作为交换机本地软件的一部分来操作，由此与嵌入式子网管理器以及嵌入式交换机驱动器和 SMA 堆栈协调地操作。

[0057] 图 5 示出了根据本发明一实施例在中间件机器环境中提供基于交换机的 SMP 业务保护的示例性流程图。如图 5 所示，在步骤 501 中，网络交换机可以接收发往子网管理代理（SMA）的一个或多个 SMP。然后在步骤 502 中，网络交换机可以检查一个或多个 SMP 是否包括正确的管理密钥。另外，在步骤 503 中，当一个或多个 SMP 不包括正确的管理密钥时，网络交换机可以阻止所述一个或多个 SMP 被转发到目的地 SMA。

[0058] 一般而言，本发明涉及在运行于一个或多个微处理器上的中间件机器环境中提供子网管理数据包（SMP）防火墙限制的系统，包括：

[0059] 用于在连接到 infiniband（IB）交织的主机通道适配器（HCA）上提供安全固件实现的装置，其中所述 HCA 与主机相关联；

[0060] 用于通过所述安全固件实现来接收至少一个 SMP 的装置，其中所述至少一个 SMP 是从所述主机接收的或者发往所述主机的；以及

[0061] 用于通过所述安全固件实现来防止所述主机向所述 IB 交织发送所述至少一个 SMP 或接收发往所述主机的所述至少一个 SMP 的装置。

[0062] 所述系统还包括用于在所述安全固件实现中包括 SMP 防火墙组件的装置。

[0063] 所述系统还包括用于允许所述 SMP 防火墙组件阻止一个或多个基于 SMP 的操作的装置。

[0064] 所述系统还包括用于允许所述 SMP 防火墙组件阻止主机软件和子网管理器之间的基于 SMP 的通信的装置。

[0065] 所述系统还包括用于实现特殊规则作为所述 SMP 防火墙组件的一部分的装置。

[0066] 所述系统还包括用于允许所述特殊规则定义特定的基于 SMP 的请求和响应类型以严格控制的速率发送和接收，和／或为直接路由 SMP 和本地标识符路由 SMP 二者定义源

和目的地限制的装置。

[0067] 所述系统还包括用于允许所述安全固件实现包括代理功能的装置，其中所述代理功能可以通过本地带外接口来接收与所述主机软件的通信。

[0068] 所述系统还包括用于允许子网管理器通过所述代理功能来向所述主机软件发送 SMP 的装置。

[0069] 所述系统还包括用于阻止从远程 IB 节点对配置信息的未经授权的检索的装置。

[0070] 所述系统还包括用于允许子网管理器关闭正在生成子网管理员（SA）请求的过载的 HCA 端口的装置。

[0071] 一般而言，本发明涉及用于阻止基于子网管理数据包（SMP）的攻击的方法，包括：

[0072] 通过安全固件实现，接收至少一个 SMP，其中所述至少一个 SMP 是从主机接收的或者发往主机的；以及

[0073] 通过所述安全固件实现，防止所述主机向 IB 交织发送所述至少一个 SMP 或接收发往所述主机的所述至少一个 SMP。

[0074] 所述方法还包括在所述安全固件实现中包括 SMP 防火墙组件。

[0075] 所述方法还包括允许所述 SMP 防火墙组件阻止一个或多个基于 SMP 的操作。

[0076] 所述方法还包括允许所述 SMP 防火墙组件阻止主机软件和子网管理器之间的基于 SMP 的通信。

[0077] 所述方法还包括实现特殊规则作为所述 SMP 防火墙组件的一部分。

[0078] 所述方法还包括允许所述特殊规则定义特定的基于 SMP 的请求和响应类型以严格控制的速率发送和接收，和 / 或为直接路由 SMP 和本地标识符路由 SMP 二者定义源和目的地限制。

[0079] 所述方法还包括允许所述安全固件实现包括代理功能，其中所述代理功能可以通过本地带外接口来接收与所述主机软件的通信。

[0080] 一般而言，本发明涉及用于阻止基于子网管理数据包（SMP）的攻击的系统，包括：

[0081] 用于通过安全固件实现，接收至少一个 SMP 的装置，其中所述至少一个 SMP 是从主机接收的或者发往主机的；以及

[0082] 用于通过所述安全固件实现，防止所述主机向 IB 交织发送所述至少一个 SMP 或接收发往所述主机的所述至少一个 SMP 的装置。

[0083] 所述系统还包括用于在所述安全固件实现中包括 SMP 防火墙组件的装置。

[0084] 所述系统还包括用于允许所述 SMP 防火墙组件阻止一个或多个基于 SMP 的操作的装置。

[0085] 所述系统还包括用于允许所述 SMP 防火墙组件阻止主机软件和子网管理器之间基于 SMP 的通信的装置。

[0086] 所述系统还包括用于实现特殊规则作为所述 SMP 防火墙组件的一部分的装置。

[0087] 所述系统还包括用于允许所述特殊规则定义特定的基于 SMP 的请求和响应类型以严格控制的速率发送和接收，和 / 或为直接路由 SMP 和本地标识符路由 SMP 二者定义源和目的地限制的装置。

[0088] 所述系统还包括用于允许所述安全固件实现包括代理功能的装置，其中所述代理功能可以通过本地带外接口来接收与所述主机软件的通信。

[0089] 一般而言，本发明涉及在运行于一个或多个微处理器上的中间件机器环境中提供基于交换机的子网管理数据包（SMP）业务保护的方法，包括：

[0090] 用于通过网络交换机，接收发往子网管理代理（SMA）组件的一个或多个 SMP 的装置；

[0091] 用于通过所述网络交换机，检查所述一个或多个 SMP 是否包括正确的管理密钥的装置；以及

[0092] 用于当所述一个或多个 SMP 不包括正确的管理密钥时，通过所述网络交换机阻止所述一个或多个 SMP 被转发到目的地 SMA 组件的装置。

[0093] 所述系统还包括用于根据交织策略过滤所述一个或多个 SMP 的装置。

[0094] 所述系统还包括用于允许所述一个或多个 SMP 中的每一个都是直接路由 SMP 的装置。

[0095] 所述系统还包括用于允许子网管理器使用一个或多个 SMP 来通过所述网络交换机上的特定交换机端口与子网管理代理（SMA）组件进行通信的装置。

[0096] 所述系统还包括用于为所述网络交换机上的每一个外部端口定义不同的管理密钥的装置。

[0097] 所述系统还包括用于允许所述网络交换机对从外部端口向所述 SMA 组件发送的 SMP 以及在所述外部端口从所述 SMA 组件接收到的 SMP 强制单独的限制的装置。

[0098] 所述系统还包括用于通过子网管理器，确保与所述 SMA 组件相关联的不受信任的远程主机通道适配器（HCA）只有在指定了正确的管理密钥的情况下才能发出一个或多个 SMP 的装置。

[0099] 所述系统还包括用于指定定义远程 HCA 端口被允许多快地生成 SMP 的 SMP 速率的装置。

[0100] 所述系统还包括用于声明一个或多个交换机端口被信任并允许下列各项的装置：

[0101] SMP 请求被从受信任的端口发送，以及

[0102] 在受信任的端口处接收 SMP 响应。

[0103] 所述系统还包括用于只允许 SMA 组件请求从受信任的端口发送到不受信任的端口的装置。

[0104] 一般而言，本发明涉及在一个或多个微处理器上运行的网络交换机，包括：

[0105] 用于接收发往子网管理代理（SMA）组件的一个或多个 SMP 的装置；

[0106] 用于检查所述一个或多个 SMP 是否包括正确的管理密钥的装置；以及

[0107] 用于当至少一个 SMP 不包括所述正确的管理密钥时，阻止所述一个或多个 SMP 被转发到目的地 SMA 组件的装置。

[0108] 本发明可以使用一个或多个常规通用或专用数字计算机、计算设备、机器或微处理器，包括一个或多个处理器、存储器和 / 或根据本公开的教导编程的计算机可读存储介质，来方便地实现。对于软件领域的技术人员而言显而易见的是，可由有经验的程序员基于本发明的教导轻松地准备适当的软件代码。

[0109] 在某些实施例中，本发明包括计算机程序产品，该产品是其中存储了指令的存储介质或计算机可读介质，这些指令可以用来对计算机进行编程，以执行本发明的任何过程。

存储介质可以包括但不限于任何类型的盘，包括软盘、光盘、DVD、CD-ROM、微驱动，以及磁光盘、ROM、RAM、EPROM、EEPROM、DRAM、VRAM、闪存设备、磁卡或光卡、纳米系统（包括分子存储器IC）、适于存储指令和／或数据的任何类型的介质或设备。

[0110] 前面对本发明的描述仅用于说明和示范。它不是详尽的说明或将本发明限于所公开的准确形式。本技术技术人员将认识到，可以进行许多修改。所选择和描述的实施例只是为了最好地说明本发明的原理以及其实际应用，并使本技术技术人员理解，带有适合于特定用途的各种修改的各实施例的本发明也是可以接受的。本发明的范围由下面的权利要求以及它们的等效内容进行定义。

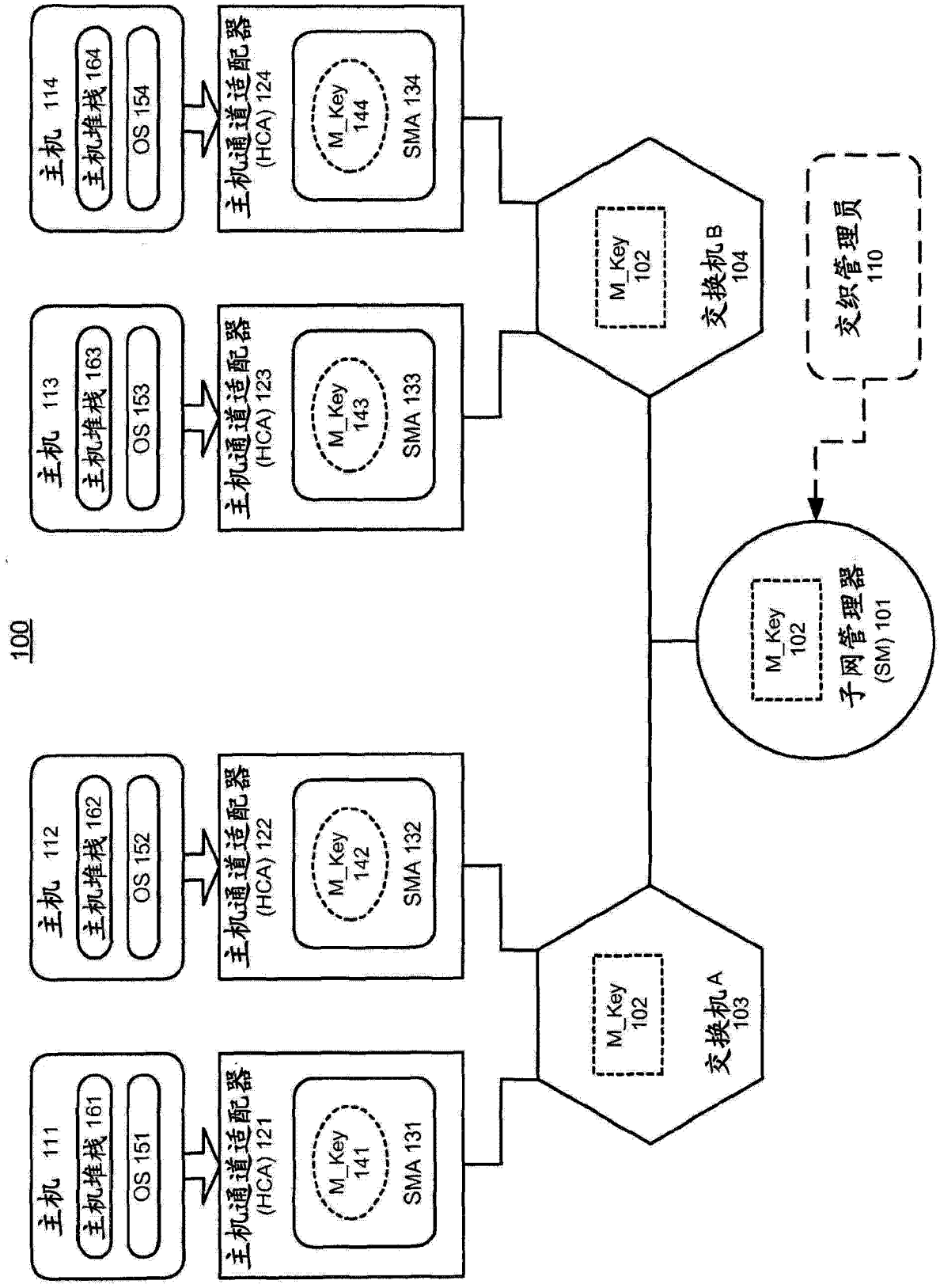

100
主机 111
主机堆栈 161
OS 151
主机通道适配器 (HCA) 121
M_Key 141
SMA 131
主机 112
主机堆栈 162
OS 152
主机通道适配器 (HCA) 122
M_Key 142
SMA 132
主机 113
主机堆栈 163
OS 153
主机通道适配器 (HCA) 123
M_Key 143
SMA 133
主机 114
主机堆栈 164
OS 154
主机通道适配器 (HCA) 124
M_Key 144
SMA 134
交换机 A 103
M_Key 102
交换机 B 104
M_Key 102
子网管理器 (SM) 101
M_Key 102
交织管理员 110

图 1

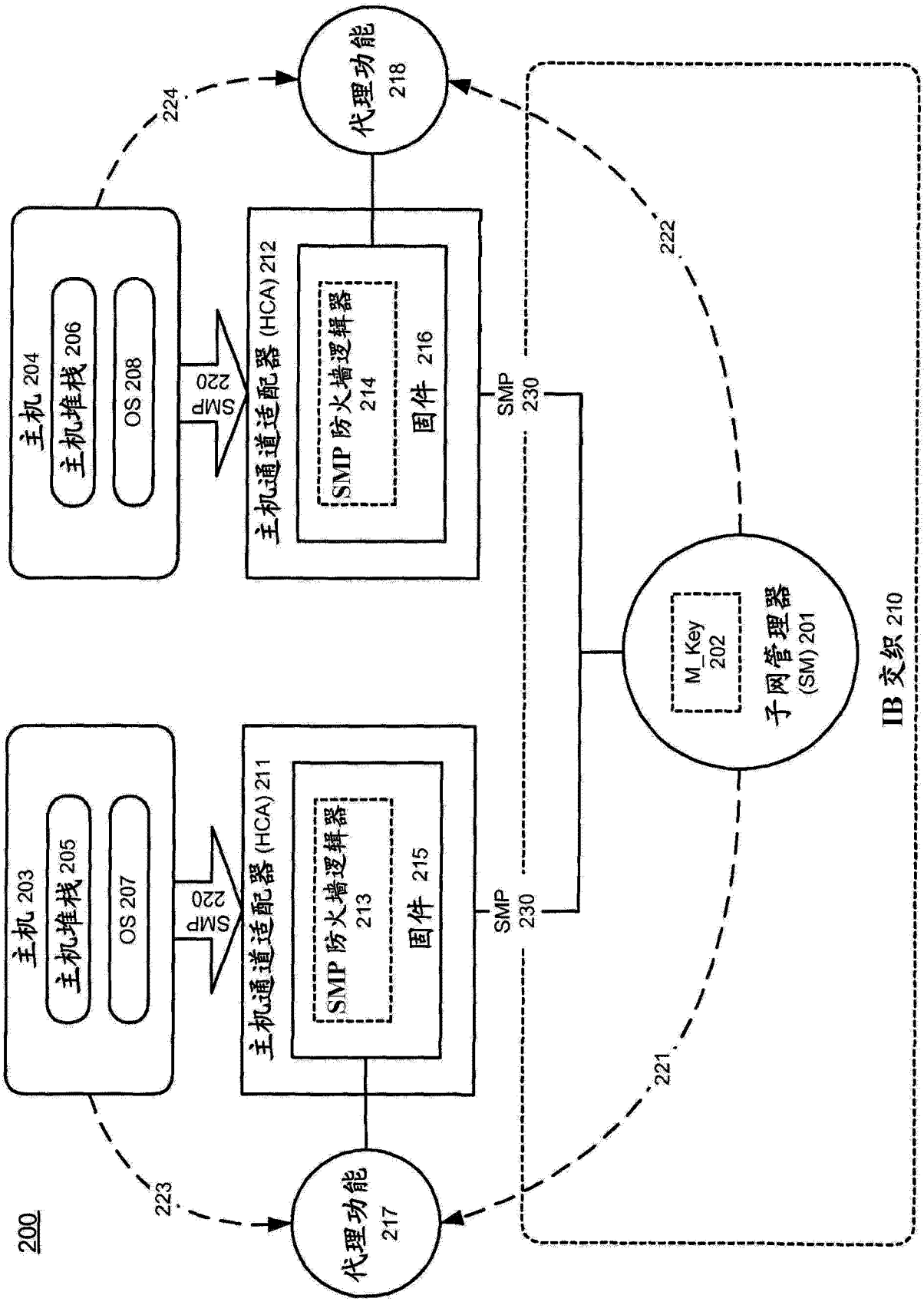

200
主机 203
主机堆栈 205
OS 207
SMP 220
主机通道适配器 (HCA) 211
SMP 防火墙逻辑器 213
固件 215
SMP 230
代理功能 217
223
主机 204
主机堆栈 206
OS 208
SMP 220
主机通道适配器 (HCA) 212
SMP 防火墙逻辑器 214
固件 216
SMP 230
代理功能 218
224
222
221
M_Key 202
子网管理器 (SM) 201
IB 交织 210

图 2

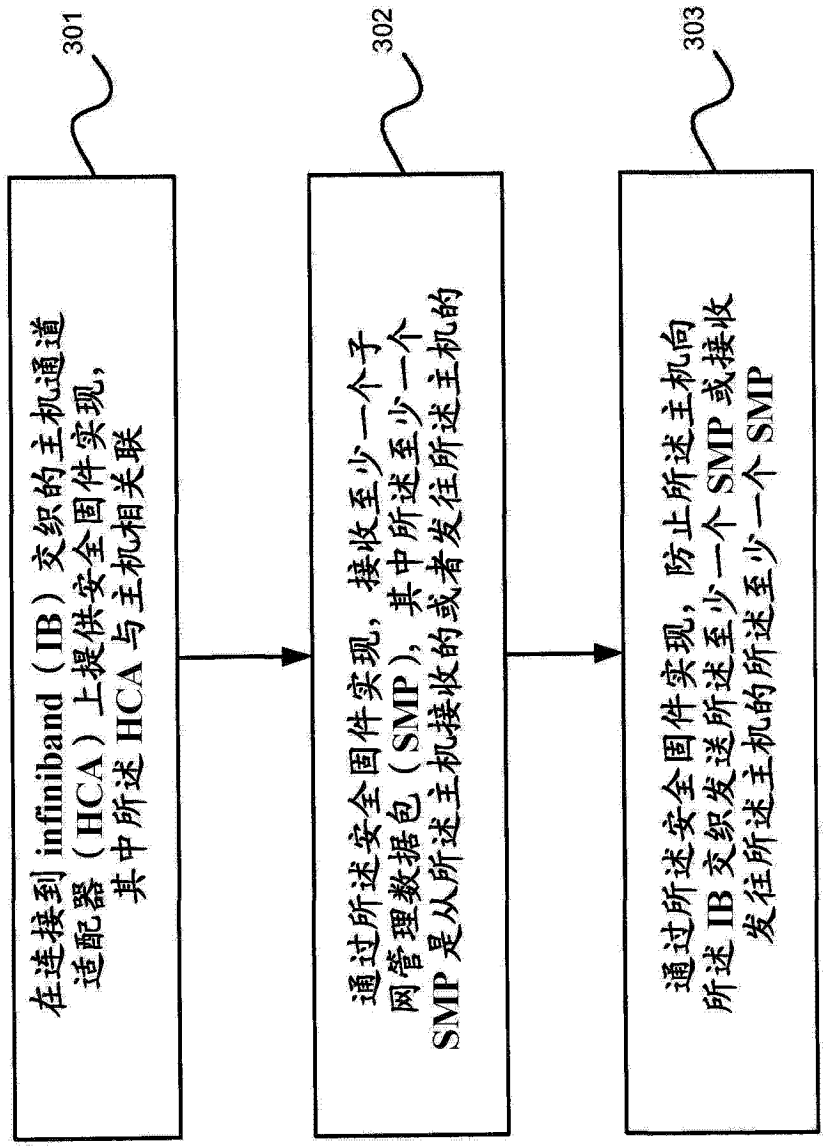

301
在连接到 infiniband（IB）交织的主机通道适配器（HCA）上提供安全固件实现，其中所述 HCA 与主机相关联
302
通过所述安全固件实现，接收至少一个子网管理数据包（SMP），其中所述至少一个 SMP 是从所述主机接收的或者发往所述主机的
303
通过所述安全固件实现，防止所述主机向所述 IB 交织发送所述至少一个 SMP 或接收发往所述主机的所述至少一个 SMP

图 3

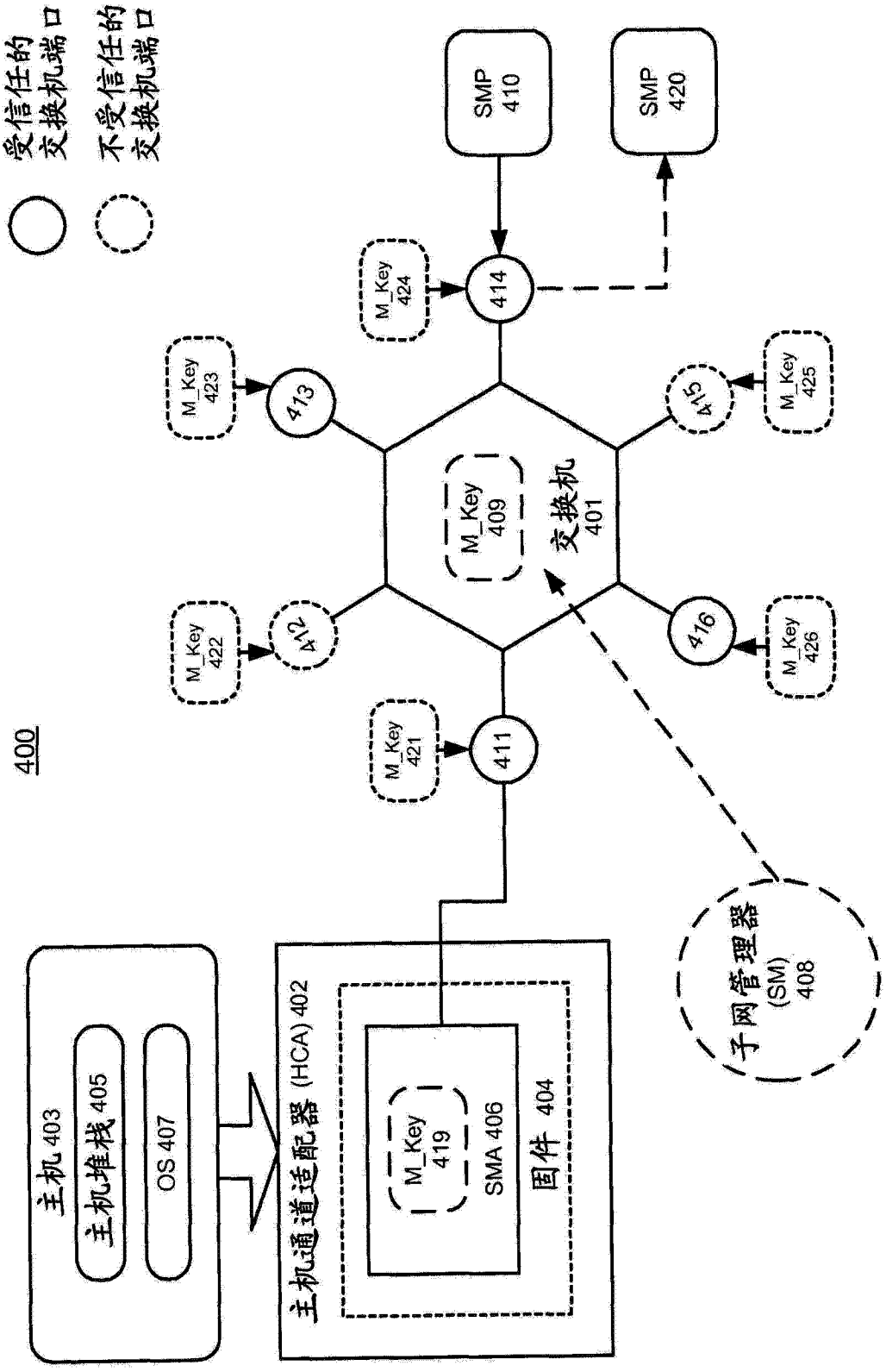

受信任的交换机端口
不受信任的交换机端口
400
SMP 410
SMP 420
M_Key 424
414
M_Key 423
413
M_Key 425
415
M_Key 409
交换机 401
M_Key 422
412
416
M_Key 426
M_Key 421
411
主机 403
主机堆栈 405
OS 407
主机通道适配器 (HCA) 402
M_Key 419
SMA 406
固件 404
子网管理器 (SM) 408

图 4

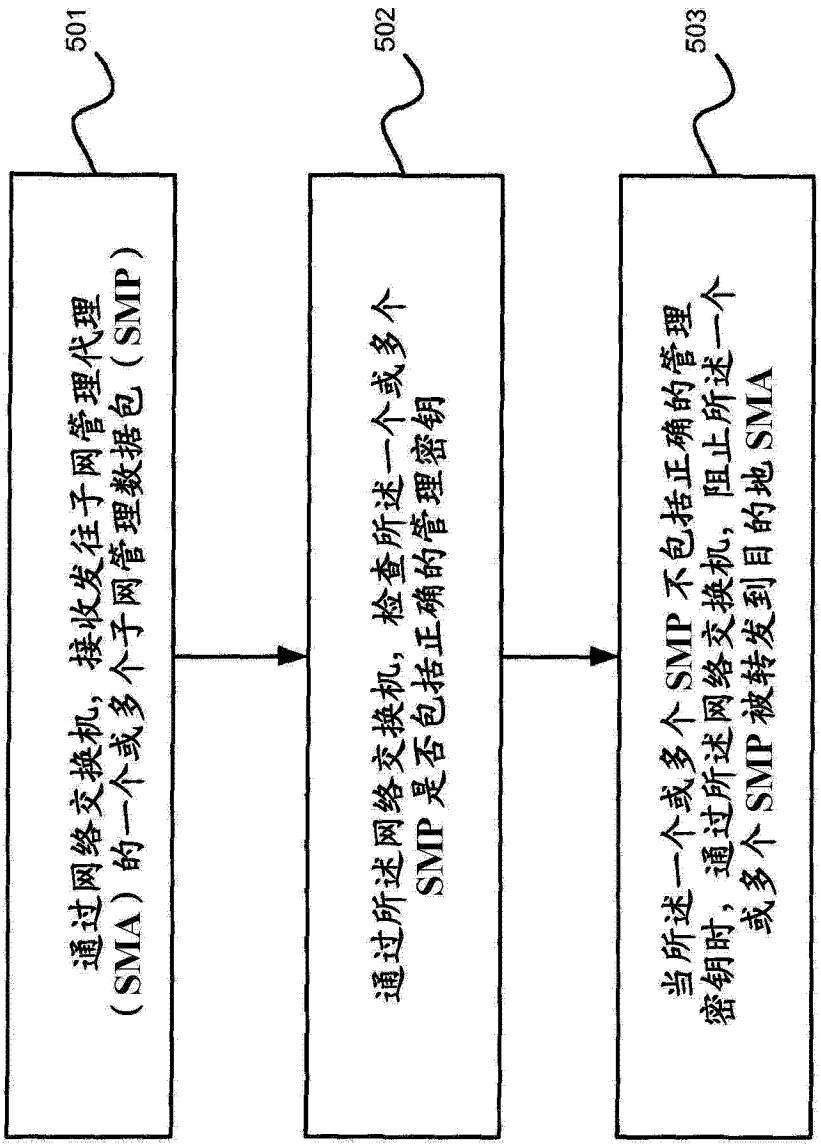

501
通过网络交换机，接收发往子网管理代理（SMA）的一个或多个子网管理数据包（SMP）
502
通过所述网络交换机，检查所述一个或多个SMP是否包括正确的管理密钥
503
当所述一个或多个SMP不包括正确的管理密钥时，通过所述网络交换机，阻止所述一个或多个SMP被转发到目的地SMA

图 5