(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 112889253 A
(43)申请公布日 2021.06.01

(21)申请号 201980069131.6
(22)申请日 2019.10.07
(30)优先权数据
16/166,973 2018.10.22 US
(85)PCT国际申请进入国家阶段日
2021.04.20
(86)PCT国际申请的申请数据
PCT/US2019/054967 2019.10.07
(87)PCT国际申请的公布数据
WO2020/086252 EN 2020.04.30
(71)申请人 思科技术公司
地址 美国加利福尼亚州
(72)发明人 戈文德·普拉萨德·夏尔马
贾维德·阿斯加尔
普拉布·巴拉坎南
斯里达尔·瓦莱帕利
(74)专利代理机构 北京东方亿思知识产权代理有限责任公司 11258
代理人 郭妍
(51)Int.Cl.
H04L 29/06(2006.01)
H04L 9/08(2006.01)
H04L 9/32(2006.01)
H04L 12/46(2006.01)

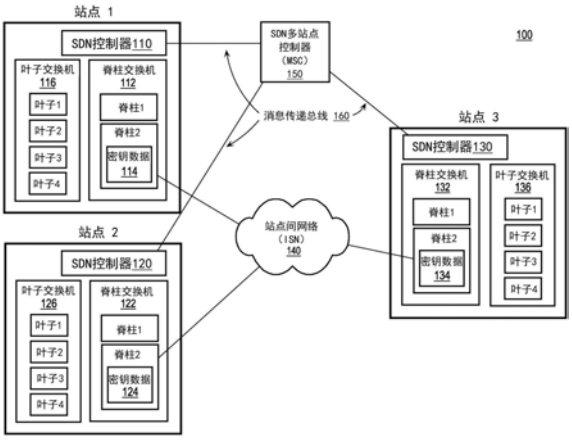
权利要求书9页 说明书11页 附图11页

(54)发明名称

用于多站点数据中心的安全密码密钥分发和管理的上游方案

(57)摘要

一种基于软件定义联网(SDN)的“上游”方案是一种基于控制器的解决方案,其为多站点数据中心提供了安全密钥分发和管理。该方案使用SDN多站点控制器(MSC),该SDN MSC充当多站点数据中心中的站点处的SDN控制器之间的中介并且管理密钥到站点的分发。该方案不取决于任何特定的路由协议,例如边界网关协议(BGP),并且很适合于多播流加密,这是通过允许同一密钥被用于从一上游源站点发送到下游站点的所有复制封包来实现的。该方案以安全方式分发密钥,确保了在站点之间传送的数据是以安全方式完成的,并且支持了带有差错处理的密钥更新。



CN 112889253 A

1.一种对多站点数据中心环境中的站点之间的数据交换提供改进的计算机实现的方法,所述计算机实现的方法包括:

由包括多个站点的多站点数据中心中的软件定义联网(SDN)多站点控制器(MSC)经由安全消息传递总线从所述多个站点中的第一站点接收向所述多个站点分发第一密钥以用于对由所述多个站点从所述第一站点接收的加密封包进行解密的请求,其中,所述请求指定了具有所述第一密钥所对应的第一值的关联号(AN);

响应于所述SDN MSC接收到向所述多个站点分发所述第一密钥以用于对由所述多个站点从所述第一站点接收的加密封包进行解密的请求,所述SDN MSC经由所述安全消息传递总线向所述多个站点中的第二站点和第三站点提供所述第一密钥和具有所述第一密钥所对应的第一值的AN以用于对从所述第一站点接收的加密封包进行解密;

由所述SDN MSC经由所述安全消息传递总线从所述多个站点中的所述第二站点和所述第三站点接收对于所述第一密钥已被成功部署在所述多个站点中的所述第二站点和所述第三站点处的确认;并且

响应于所述SDN MSC经由所述安全消息传递总线从所述多个站点中的所述第二站点和所述第三站点接收到对于所述第一密钥已被成功部署在所述第二站点和所述第三站点处以用于对从所述第一站点接收的加密封包进行解密的确认,所述SDN MSC生成并向所述第一站点发送对于所述第一密钥已被成功部署在所述多个站点中的所述第二站点和所述第三站点处的认定,

其中,响应于所述第一站点接收到对于所述第一密钥已被成功部署在所述多个站点中的所述第二站点和所述第三站点处的认定,所述第一站点使用所述第一密钥来生成被所述第一站点发送到所述多个站点中的所述第二站点和所述第三站点的加密封包的第一集合,其中,来自所述加密封包的第一集合的每个加密封包的媒体访问控制安全性(MACsec)头部包括与所述第一站点相对应的安全信道识别符(SCI)和具有所述第一值的AN,并且其中,所述第二站点和所述第三站点处的一个或多个网络交换机使用来自所述加密封包的第一集合的每个加密封包的MACsec头部中的与所述第一站点相对应的SCI和具有所述第一值的AN,来从多个密钥中选择所述第一密钥,以对从所述第一站点接收的加密封包的第一集合进行解密。

2.如权利要求1所述的计算机实现的方法,还包括:

由所述SDN MSC经由所述安全消息传递总线从所述多个站点中的所述第一站点接收向所述多个站点分发第二密钥以用于对由所述多个站点从所述第一站点接收的加密封包进行解密的请求,其中,所述请求指定了具有所述第二密钥所对应的第二值的AN;

响应于所述SDN MSC接收到向所述多个站点分发所述第二密钥以用于对由所述多个站点从所述第一站点接收的加密封包进行解密的请求,所述SDN MSC经由所述安全消息传递总线向所述多个站点中的所述第二站点和所述第三站点分发所述第二密钥和具有所述第二密钥所对应的第二值的AN以用于对由所述多个站点中的所述第二站点和所述第三站点从所述第一站点接收的加密封包进行解密;

由所述SDN MSC经由所述安全消息传递总线从所述多个站点中的所述第二站点和所述第三站点接收对于所述第二密钥已被成功部署在所述多个站点中的所述第二站点和所述第三站点处的确认;并且

响应于所述SDN MSC经由所述安全消息传递总线从所述多个站点中的所述第二站点和所述第三站点接收到对于所述第二密钥已被成功部署在所述第二站点和所述第三站点处以用于对从所述第一站点接收的加密封包进行解密的确认,所述SDN MSC生成并向所述第一站点发送对于所述第二密钥已被成功部署在所述多个站点中的所述第二站点和所述第三站点处的认定,

其中,响应于所述第一站点接收到对于所述第二密钥已被成功部署在所述多个站点中的所述第二站点和所述第三站点处的认定,所述第一站点使用所述第二密钥来生成被所述第一站点发送到所述多个站点中的所述第二站点和所述第三站点的加密封包的第二集合,其中,来自所述加密封包的第二集合的每个加密封包的MACsec头部包括与所述第一站点相对应的SCI和具有所述第二值的AN,并且其中,所述第二站点和所述第三站点处的所述一个或多个网络交换机使用来自所述加密封包的第二集合的每个加密封包的MACsec头部中的与所述第一站点相对应的SCI和具有所述第二值的AN,来从所述多个密钥中选择所述第二密钥,以对从所述第一站点接收的加密封包的第二集合进行解密。

3.如权利要求2所述的计算机实现的方法,其中:

所述第二站点或所述第三站点处的所述一个或多个网络交换机从所述第一站点接收一个或多个额外加密封包,每个额外加密封包的MACsec头部具有与所述第一站点相对应的SCI和具有所述第一值的AN,并且

所述第二站点或所述第三站点处的所述一个或多个网络交换机使用来自所述多个密钥的所述第一密钥而不是所述第二密钥,来基于含有具有所述第一值而不是所述第二值的AN的所述一个或多个加密封包的MACsec头部对所述一个或多个额外加密封包进行解密。

4.如前述任一权利要求所述的计算机实现的方法,还包括:

由所述SDN MSC经由所述安全消息传递总线从所述多个站点中的所述第一站点接收向所述多个站点分发第二密钥以用于对由所述多个站点从所述第一站点接收的加密封包进行解密的请求,其中,所述请求指定了具有所述第二密钥所对应的第二值的AN;

响应于所述SDN MSC接收到向所述多个站点分发所述第二密钥以用于对由所述多个站点从所述第一站点接收的加密封包进行解密的请求,所述SDN MSC经由所述安全消息传递总线向所述多个站点中的所述第二站点和所述第三站点分发所述第二密钥和具有所述第二密钥所对应的第二值的AN以用于对由所述多个站点中的所述第二站点和所述第三站点从所述第一站点接收的加密封包进行解密;

由所述SDN MSC经由所述安全消息传递总线从所述多个站点中的所述第二站点或所述第三站点中的一个或多个接收指示出所述第二密钥没有被成功部署在所述多个站点中的所述第二站点或所述第三站点处的差错消息;并且

响应于所述SDN MSC经由所述安全消息传递总线从所述多个站点中的所述第二站点或所述第三站点中的一个或多个接收到指示出所述第二密钥没有被成功部署在所述多个站点中的所述第二站点或所述第三站点处的差错消息,所述SDN MSC生成并向所述第一站点发送指出所述第二密钥没有被成功部署在所述多个站点中的所述第二站点或所述第三站点中的一个或多个处的通知,

其中,响应于所述第一站点接收到指出所述第二密钥没有被成功部署在所述多个站点中的所述第二站点或所述第三站点中的一个或多个处的通知,所述第一站点使用所述第一

密钥而不是所述第二密钥来生成被所述第一站点发送到所述多个站点中的所述第二站点和所述第三站点的加密封包的第二集合,其中,来自所述加密封包的第二集合的每个加密封包的MACsec头部包括与所述第一站点相对应的SCI和具有所述第一值的AN,并且其中,所述第二站点和所述第三站点处的所述一个或多个网络交换机使用来自所述加密封包的第二集合的每个加密封包的MACsec头部中的与所述第一站点相对应的SCI和具有所述第一值的AN,来从所述多个密钥中选择所述第一密钥而不是所述第二密钥,以对从所述第一站点接收的加密封包的第二集合进行解密。

5.如前述任一权利要求所述的计算机实现的方法,还包括:

由包括多个站点的多站点数据中心中的所述SDN MSC经由所述安全消息传递总线从所述多个站点中的所述第一站点接收向所述多个站点中的第四站点分发第四密钥以用于对由所述第四站点从所述第一站点接收的加密封包进行解密的请求,其中,所述请求指定了具有所述第四密钥所对应的第一值的关联号(AN);

响应于所述SDN MSC接收到向所述第四站点分发所述第四密钥以用于对由所述第四站点从所述第一站点接收的加密封包进行解密的请求,所述SDN MSC经由所述安全消息传递总线向所述第四站点提供所述第四密钥和具有所述第一密钥所对应的第一值的AN以用于对从所述第一站点接收的加密封包进行解密;

由所述SDN MSC经由所述安全消息传递总线从所述第四站点接收对于所述第四密钥已被成功部署在所述第四站点处的确认;并且

响应于所述SDN MSC经由所述安全消息传递总线从所述第四站点接收到对于所述第四密钥已被成功部署在所述第四站点处以用于对从所述第一站点接收的加密封包进行解密的确认,所述SDN MSC生成并向所述第一站点发送对于所述第四密钥已被成功部署在所述第四站点处的认定,

其中,响应于所述第一站点接收到对于所述第四密钥已被成功部署在所述第四站点处的认定,所述第一站点使用所述第四密钥来生成被所述第一站点发送到所述第四站点的加密封包的第四集合,其中,来自所述加密封包的第四集合的每个加密封包的MACsec头部包括与所述第一站点相对应的SCI和具有所述第一值的AN,并且其中,所述第四站点处的一个或多个网络交换机使用来自所述加密封包的第一集合的每个加密封包的MACsec头部中的与所述第一站点相对应的SCI和具有所述第一值的AN,来从多个密钥中选择所述第四密钥,以对从所述第一站点接收的加密封包的第四集合进行解密。

6.如前述任一权利要求所述的计算机实现的方法,其中:

所述多个站点的每个站点和所述SDN MSC实现表述性状态转移(REST)应用程序接口(API),

所述多个站点的每个站点与所述SDN MSC之间的通信遵守所述REST API,并且

所述消息传递总线是利用传输层安全性(TLS)实现的。

7.如前述任一权利要求所述的计算机实现的方法,其中,所述加密封包的第一集合是加密虚拟可扩展局域网(VXLAN)封包的第一集合。

8.如前述任一权利要求所述的计算机实现的方法,其中,所述第一站点生成被提供到所述SDN MSC的所述第一密钥。

9.一种装置,包括:

一个或多个处理器,以及

存储指令的一个或多个存储器,所述指令当被所述一个或多个处理器处理时,使得:

由包括多个站点的多站点数据中心中的软件定义联网(SDN)多站点控制器(MSC)经由安全消息传递总线从所述多个站点中的第一站点接收向所述多个站点分发第一密钥以用于对由所述多个站点从所述第一站点接收的加密封包进行解密的请求,其中,所述请求指定了具有所述第一密钥所对应的第一值的关联号(AN);

响应于所述SDN MSC接收到向所述多个站点分发所述第一密钥以用于对由所述多个站点从所述第一站点接收的加密封包进行解密的请求,所述SDN MSC经由所述安全消息传递总线向所述多个站点中的第二站点和第三站点提供所述第一密钥和具有所述第一密钥所对应的第一值的AN以用于对从所述第一站点接收的加密封包进行解密;

由所述SDN MSC经由所述安全消息传递总线从所述多个站点中的所述第二站点和所述第三站点接收对于所述第一密钥已被成功部署在所述多个站点中的所述第二站点和所述第三站点处的确认;并且

响应于所述SDN MSC经由所述安全消息传递总线从所述多个站点中的所述第二站点和所述第三站点接收到对于所述第一密钥已被成功部署在所述第二站点和所述第三站点处以用于对从所述第一站点接收的加密封包进行解密的确认,所述SDN MSC生成并向所述第一站点发送对于所述第一密钥已被成功部署在所述多个站点中的所述第二站点和所述第三站点处的认定,

其中,响应于所述第一站点接收到对于所述第一密钥已被成功部署在所述多个站点中的所述第二站点和所述第三站点处的认定,所述第一站点使用所述第一密钥来生成被所述第一站点发送到所述多个站点中的所述第二站点和所述第三站点的加密封包的第一集合,其中,来自所述加密封包的第一集合的每个加密封包的媒体访问控制安全性(MACsec)头部包括与所述第一站点相对应的安全信道识别符(SCI)和具有所述第一值的AN,并且其中,所述第二站点和所述第三站点处的一个或多个网络交换机使用来自所述加密封包的第一集合的每个加密封包的MACsec头部中的与所述第一站点相对应的SCI和具有所述第一值的AN,来从多个密钥中选择所述第一密钥,以对从所述第一站点接收的加密封包的第一集合进行解密。

10.如权利要求9所述的装置,其中,所述一个或多个存储器存储额外指令,所述额外指令当被所述一个或多个处理器处理时,使得:

由所述SDN MSC经由所述安全消息传递总线从所述多个站点中的所述第一站点接收向所述多个站点分发第二密钥以用于对由所述多个站点从所述第一站点接收的加密封包进行解密的请求,其中,所述请求指定了具有所述第二密钥所对应的第二值的AN;

响应于所述SDN MSC接收到向所述多个站点分发所述第二密钥以用于对由所述多个站点从所述第一站点接收的加密封包进行解密的请求,所述SDN MSC经由所述安全消息传递总线向所述多个站点中的所述第二站点和所述第三站点分发所述第二密钥和具有所述第二密钥所对应的第二值的AN以用于对由所述多个站点中的所述第二站点和所述第三站点从所述第一站点接收的加密封包进行解密;

由所述SDN MSC经由所述安全消息传递总线从所述多个站点中的所述第二站点和所述第三站点接收对于所述第二密钥已被成功部署在所述多个站点中的所述第二站点和所述

第三站点处的确认;并且

响应于所述SDN MSC经由所述安全消息传递总线从所述多个站点中的所述第二站点和所述第三站点接收到对于所述第二密钥已被成功部署在所述第二站点和所述第三站点处以用于对从所述第一站点接收的加密封包进行解密的确认,所述SDN MSC生成并向所述第一站点发送对于所述第二密钥已被成功部署在所述多个站点中的所述第二站点和所述第三站点处的认定,

其中,响应于所述第一站点接收到对于所述第二密钥已被成功部署在所述多个站点中的所述第二站点和所述第三站点处的认定,所述第一站点使用所述第二密钥来生成被所述第一站点发送到所述多个站点中的所述第二站点和所述第三站点的加密封包的第二集合,其中,来自所述加密封包的第二集合的每个加密封包的MACsec头部包括与所述第一站点相对应的SCI和具有所述第二值的AN,并且其中,所述第二站点和所述第三站点处的所述一个或多个网络交换机使用来自所述加密封包的第二集合的每个加密封包的MACsec头部中的与所述第一站点相对应的SCI和具有所述第二值的AN,来从所述多个密钥中选择所述第二密钥,以对从所述第一站点接收的加密封包的第二集合进行解密。

11.如权利要求10所述的装置,其中:

所述第二站点或所述第三站点处的所述一个或多个网络交换机从所述第一站点接收一个或多个额外加密封包,每个额外加密封包的MACsec头部具有与所述第一站点相对应的SCI和具有所述第一值的AN,并且

所述第二站点或所述第三站点处的所述一个或多个网络交换机使用来自所述多个密钥的所述第一密钥而不是所述第二密钥,来基于含有具有所述第一值而不是所述第二值的AN的所述一个或多个加密封包的MACsec头部对所述一个或多个额外加密封包进行解密。

12.如权利要求9至11的任何一项所述的装置,其中,所述一个或多个存储器存储额外指令,所述额外指令当被所述一个或多个处理器处理时,使得:

由所述SDN MSC经由所述安全消息传递总线从所述多个站点中的所述第一站点接收向所述多个站点分发第二密钥以用于对由所述多个站点从所述第一站点接收的加密封包进行解密的请求,其中,所述请求指定了具有所述第二密钥所对应的第二值的AN;

响应于所述SDN MSC接收到向所述多个站点分发所述第二密钥以用于对由所述多个站点从所述第一站点接收的加密封包进行解密的请求,所述SDN MSC经由所述安全消息传递总线向所述多个站点中的所述第二站点和所述第三站点分发所述第二密钥和具有所述第二密钥所对应的第二值的AN以用于对由所述多个站点中的所述第二站点和所述第三站点从所述第一站点接收的加密封包进行解密;

由所述SDN MSC经由所述安全消息传递总线从所述多个站点中的所述第二站点或所述第三站点中的一个或多个接收指示出所述第二密钥没有被成功部署在所述多个站点中的所述第二站点或所述第三站点处的差错消息;并且

响应于所述SDN MSC经由所述安全消息传递总线从所述多个站点中的所述第二站点或所述第三站点中的一个或多个接收到指示出所述第二密钥没有被成功部署在所述多个站点中的所述第二站点或所述第三站点处的差错消息,所述SDN MSC生成并向所述第一站点发送指出所述第二密钥没有被成功部署在所述多个站点中的所述第二站点或所述第三站点中的一个或多个处的通知,

其中,响应于所述第一站点接收到指出所述第二密钥没有被成功部署在所述多个站点中的所述第二站点或所述第三站点中的一个或多个处的通知,所述第一站点使用所述第一密钥而不是所述第二密钥来生成被所述第一站点发送到所述多个站点中的所述第二站点和所述第三站点的加密封包的第二集合,其中,来自所述加密封包的第二集合的每个加密封包的MACsec头部包括与所述第一站点相对应的SCI和具有所述第一值的AN,并且其中,所述第二站点和所述第三站点处的所述一个或多个网络交换机使用来自所述加密封包的第二集合的每个加密封包的MACsec头部中的与所述第一站点相对应的SCI和具有所述第一值的AN,来从所述多个密钥中选择所述第一密钥而不是所述第二密钥,以对从所述第一站点接收的加密封包的第二集合进行解密。

13.如权利要求9至12的任何一项所述的装置,其中,所述一个或多个存储器存储额外指令,所述额外指令当被所述一个或多个处理器处理时,使得:

由包括多个站点的多站点数据中心中的所述SDN MSC经由所述安全消息传递总线从所述多个站点中的所述第一站点接收向所述多个站点中的第四站点分发第四密钥以用于对由所述第四站点从所述第一站点接收的加密封包进行解密的请求,其中,所述请求指定了具有所述第四密钥所对应的第一值的关联号(AN);

响应于所述SDN MSC接收到向所述第四站点分发所述第四密钥以用于对由所述第四站点从所述第一站点接收的加密封包进行解密的请求,所述SDN MSC经由所述安全消息传递总线向所述第四站点提供所述第四密钥和具有所述第一密钥所对应的第一值的AN以用于对从所述第一站点接收的加密封包进行解密;

由所述SDN MSC经由所述安全消息传递总线从所述第四站点接收对于所述第四密钥已被成功部署在所述第四站点处的确认;并且

响应于所述SDN MSC经由所述安全消息传递总线从所述第四站点接收到对于所述第四密钥已被成功部署在所述第四站点处以用于对从所述第一站点接收的加密封包进行解密的确认,所述SDN MSC生成并向所述第一站点发送对于所述第四密钥已被成功部署在所述第四站点处的认定,

其中,响应于所述第一站点接收到对于所述第四密钥已被成功部署在所述第四站点处的认定,所述第一站点使用所述第四密钥来生成被所述第一站点发送到所述第四站点的加密封包的第四集合,其中,来自所述加密封包的第四集合的每个加密封包的MACsec头部包括与所述第一站点相对应的SCI和具有所述第一值的AN,并且其中,所述第四站点处的一个或多个网络交换机使用来自所述加密封包的第一集合的每个加密封包的MACsec头部中的与所述第一站点相对应的SCI和具有所述第一值的AN,来从多个密钥中选择所述第四密钥,以对从所述第一站点接收的加密封包的第四集合进行解密。

14.如权利要求9至13的任何一项所述的装置,其中:

所述多个站点的每个站点和所述SDN MSC实现表述性状态转移(REST)应用程序接口(API),

所述多个站点的每个站点与所述SDN MSC之间的通信遵守所述REST API,并且

所述消息传递总线是利用传输层安全性(TLS)实现的。

15.如权利要求9至14的任何一项所述的装置,其中,所述加密封包的第一集合是加密虚拟可扩展局域网(VXLAN)封包的第一集合。

16.如权利要求9至15的任何一项所述的装置,其中,所述第一站点生成被提供到所述SDN MSC的所述第一密钥。

17.存储指令的一个或多个非暂态计算机可读介质,所述指令当被一个或多个处理器处理时,使得:

一个或多个处理器,以及

存储指令的一个或多个存储器,所述指令当被所述一个或多个处理器处理时,使得:

由包括多个站点的多站点数据中心中的软件定义联网(SDN)多站点控制器(MSC)经由安全消息传递总线从所述多个站点中的第一站点接收向所述多个站点分发第一密钥以用于对由所述多个站点从所述第一站点接收的加密封包进行解密的请求,其中,所述请求指定了具有所述第一密钥所对应的第一值的关联号(AN);

响应于所述SDN MSC接收到向所述多个站点分发所述第一密钥以用于对由所述多个站点从所述第一站点接收的加密封包进行解密的请求,所述SDN MSC经由所述安全消息传递总线向所述多个站点中的第二站点和第三站点提供所述第一密钥和具有所述第一密钥所对应的第一值的AN以用于对从所述第一站点接收的加密封包进行解密;

由所述SDN MSC经由所述安全消息传递总线从所述多个站点中的所述第二站点和所述第三站点接收对于所述第一密钥已被成功部署在所述多个站点中的所述第二站点和所述第三站点处的确认;并且

响应于所述SDN MSC经由所述安全消息传递总线从所述多个站点中的所述第二站点和所述第三站点接收到对于所述第一密钥已被成功部署在所述第二站点和所述第三站点处以用于对从所述第一站点接收的加密封包进行解密的确认,所述SDN MSC生成并向所述第一站点发送对于所述第一密钥已被成功部署在所述多个站点中的所述第二站点和所述第三站点处的认定,

其中,响应于所述第一站点接收到对于所述第一密钥已被成功部署在所述多个站点中的所述第二站点和所述第三站点处的认定,所述第一站点使用所述第一密钥来生成被所述第一站点发送到所述多个站点中的所述第二站点和所述第三站点的加密封包的第一集合,其中,来自所述加密封包的第一集合的每个加密封包的媒体访问控制安全性(MACsec)头部包括与所述第一站点相对应的安全信道识别符(SCI)和具有所述第一值的AN,并且其中,所述第二站点和所述第三站点处的一个或多个网络交换机使用来自所述加密封包的第一集合的每个加密封包的MACsec头部中的与所述第一站点相对应的SCI和具有所述第一值的AN,来从多个密钥中选择所述第一密钥,以对从所述第一站点接收的加密封包的第一集合进行解密。

18.如权利要求17所述的一个或多个非暂态计算机可读介质,还包括额外指令,所述额外指令当被所述一个或多个处理器处理时,使得:

由所述SDN MSC经由所述安全消息传递总线从所述多个站点中的所述第一站点接收向所述多个站点分发第二密钥以用于对由所述多个站点从所述第一站点接收的加密封包进行解密的请求,其中,所述请求指定了具有所述第二密钥所对应的第二值的AN;

响应于所述SDN MSC接收到向所述多个站点分发所述第二密钥以用于对由所述多个站点从所述第一站点接收的加密封包进行解密的请求,所述SDN MSC经由所述安全消息传递总线向所述多个站点中的所述第二站点和所述第三站点分发所述第二密钥和具有所述第

二密钥所对应的第二值的AN以用于对由所述多个站点中的所述第二站点和所述第三站点从所述第一站点接收的加密封包进行解密；

由所述SDN MSC经由所述安全消息传递总线从所述多个站点中的所述第二站点和所述第三站点接收对于所述第二密钥已被成功部署在所述多个站点中的所述第二站点和所述第三站点处的确认;并且

响应于所述SDN MSC经由所述安全消息传递总线从所述多个站点中的所述第二站点和所述第三站点接收到对于所述第二密钥已被成功部署在所述第二站点和所述第三站点处以用于对从所述第一站点接收的加密封包进行解密的确认,所述SDN MSC生成并向所述第一站点发送对于所述第二密钥已被成功部署在所述多个站点中的所述第二站点和所述第三站点处的认定,

其中,响应于所述第一站点接收到对于所述第二密钥已被成功部署在所述多个站点中的所述第二站点和所述第三站点处的认定,所述第一站点使用所述第二密钥来生成被所述第一站点发送到所述多个站点中的所述第二站点和所述第三站点的加密封包的第二集合,其中,来自所述加密封包的第二集合的每个加密封包的MACsec头部包括与所述第一站点相对应的SCI和具有所述第二值的AN,并且其中,所述第二站点和所述第三站点处的所述一个或多个网络交换机使用来自所述加密封包的第二集合的每个加密封包的MACsec头部中的与所述第一站点相对应的SCI和具有所述第二值的AN,来从所述多个密钥中选择所述第二密钥,以对从所述第一站点接收的加密封包的第二集合进行解密。

19.如权利要求18所述的一个或多个非暂态计算机可读介质,其中：

所述第二站点或所述第三站点处的所述一个或多个网络交换机从所述第一站点接收一个或多个额外加密封包,每个额外加密封包的MACsec头部具有与所述第一站点相对应的SCI和具有所述第一值的AN,并且

所述第二站点或所述第三站点处的所述一个或多个网络交换机使用来自所述多个密钥的所述第一密钥而不是所述第二密钥,来基于含有具有所述第一值而不是所述第二值的AN的所述一个或多个加密封包的MACsec头部对所述一个或多个额外加密封包进行解密。

20.如权利要求17至19的任何一项所述的一个或多个非暂态计算机可读介质,还包括额外指令,所述额外指令当被所述一个或多个处理器处理时,使得：

由所述SDN MSC经由所述安全消息传递总线从所述多个站点中的所述第一站点接收向所述多个站点分发第二密钥以用于对由所述多个站点从所述第一站点接收的加密封包进行解密的请求,其中,所述请求指定了具有所述第二密钥所对应的第二值的AN;

响应于所述SDN MSC接收到向所述多个站点分发所述第二密钥以用于对由所述多个站点从所述第一站点接收的加密封包进行解密的请求,所述SDN MSC经由所述安全消息传递总线向所述多个站点中的所述第二站点和所述第三站点分发所述第二密钥和具有所述第二密钥所对应的第二值的AN以用于对由所述多个站点中的所述第二站点和所述第三站点从所述第一站点接收的加密封包进行解密;

由所述SDN MSC经由所述安全消息传递总线从所述多个站点中的所述第二站点或所述第三站点中的一个或多个接收指示出所述第二密钥没有被成功部署在所述多个站点中的所述第二站点或所述第三站点处的差错消息;并且

响应于所述SDN MSC经由所述安全消息传递总线从所述多个站点中的所述第二站点或

所述第三站点中的一个或多个接收到指示出所述第二密钥没有被成功部署在所述多个站点中的所述第二站点或所述第三站点处的差错消息,所述SDN MSC生成并向所述第一站点发送指出所述第二密钥没有被成功部署在所述多个站点中的所述第二站点或所述第三站点中的一个或多个处的通知,

其中,响应于所述第一站点接收到指出所述第二密钥没有被成功部署在所述多个站点中的所述第二站点或所述第三站点中的一个或多个处的通知,所述第一站点使用所述第一密钥而不是所述第二密钥来生成被所述第一站点发送到所述多个站点中的所述第二站点和所述第三站点的加密封包的第二集合,其中,来自所述加密封包的第二集合的每个加密封包的MACsec头部包括与所述第一站点相对应的SCI和具有所述第一值的AN,并且其中,所述第二站点和所述第三站点处的所述一个或多个网络交换机使用来自所述加密封包的第二集合的每个加密封包的MACsec头部中的与所述第一站点相对应的SCI和具有所述第一值的AN,来从所述多个密钥中选择所述第一密钥而不是所述第二密钥,以对从所述第一站点接收的加密封包的第二集合进行解密。

用于多站点数据中心的安全密码密钥分发和管理的上游方案

技术领域

[0001] 实施例总体涉及多站点数据中心，并且更具体而言，涉及用于多站点数据中心的密码密钥——本文也称为“密钥”——分发和管理的方案。

背景技术

[0002] 本部分中描述的方案是可以实行的方案，但不一定是先前已经设想到或者实行过的方案。因此，除非另有指明，否则本部分中描述的方案可能不是本申请中的权利要求的现有技术，并且并不因为被包括在本部分中就被承认为是现有技术。

[0003] 现在跨多个站点来实现许多数据中心，以解决IP移动性、灾难恢复、扩展和冗余问题。一些站点正被使用非阻塞交换机架构来实现，例如Clos网络。关于Clos网络拓扑，每个站点通常包括连接到大量叶子交换机的脊柱交换机，其中每个叶子交换机连接到物理服务器，每个物理服务器托管虚拟服务器/端点。作为一个示例，站点可包括一个或多个POD，其中每个POD包括大约8-16个脊柱交换机，这些脊柱交换机连接到大约500-1000个叶子交换机。在每个物理服务器托管大约20个虚拟服务器的情况下，每个叶子交换机连接到大约1000-2000个虚拟服务器/端点。站点是利用数据中心互连(data center interconnect，DCI)策略被连接的，例如虚拟可扩展局域网(Virtual Extensible Local Area Network，VXLAN)，其利用封装在第3层之上创建第2层逻辑网络，以支持站点之间的流量。

[0004] 多站点数据中心的问题之一是如何保证站点之间的通信的安全。现有的密钥分发和管理机制，例如IEEE的媒体访问控制安全性(Media Access Control Security，MACsec)标准，是基于控制平面的并且只适合于部署在第2层网络中的设备。它们不太适合于为使用第3层网络来提供站点之间的通信的多站点数据中心提供密钥分发和管理。

附图说明

[0005] 在附图中，相似的标号指代相似的元素。

[0006] 图1描绘了用于为多站点数据中心提供安全密钥分发和管理的示例布置。

[0007] 图2A和图2B包括描绘了上游密钥分配和分发方案的流程图。

[0008] 图3A描绘了在单个发送加密密钥的情境中用于在多站点数据中心中的站点之间交换数据的发送和接收密钥的密钥图。

[0009] 图3B描绘了在单个发送加密密钥的情境中用于在多站点数据中心中的站点之间交换数据的发送和接收密钥的密钥表。

[0010] 图4A描绘了在多个发送加密密钥的情境中用于在多站点数据中心中的站点之间交换数据的发送和接收密钥的密钥图。

[0011] 图4B描绘了在多个发送加密密钥的情境中用于在多站点数据中心中的站点之间交换数据的发送和接收密钥的密钥表。

[0012] 图5A描绘了SDN MSC 150将AN＝0的单个密钥K1从站点1到站点2和站点3的成功部署。

[0013] 图5B描绘了密钥K1到密钥K2的成功密钥更新。

[0014] 图5C描绘了因为站点3处的失败引起的密钥K2到密钥K3的不成功密钥更新，该失败阻止了新密钥K3的部署。

[0015] 图5D描绘了在多次密钥更新尝试之后AN＝0的新密钥K4的成功部署。

[0016] 图5E描绘了因为超时引起的密钥K2到密钥K3的不成功密钥更新。

[0017] 图6是其上可实现实施例的计算机系统的框图。

具体实施方式

[0018] 在接下来的描述中，出于说明目的，记载了许多具体细节以便提供对各种实施例的透彻理解。然而，本领域技术人员将会清楚，没有这些具体细节也可实现实施例。在其他情况中，以框图形式示出公知的结构和设备以避免不必要地模糊实施例。下面在接下来的章节中描述实施例的各种方面。

[0019] I.概述

[0020] II.架构

[0021] III.上游密钥分配和分发

[0022] IV.密钥更新

[0023] V.安全性和其他考虑

[0024] VI.示例用例

[0025] VII.实现示例

[0026] I.概述

[0027] 一种基于软件定义联网(Software-Defined Networking,SDN)的“上游”方案是一种基于控制器的解决方案，其为多站点数据中心提供了安全密钥分发和管理。该方案使用SDN多站点控制器(Multi-Site Controller,MSC)，该SDN MSC充当多站点数据中心中的各站点处的SDN控制器之间的中介并且管理密钥到站点的分发。该方案不取决于任何特定的路由协议，例如边界网关协议(Border Gateway Protocol,BGP)，并且除了单播以外还很适合于多播流加密，这是通过允许同一密钥被用于从一上游源站点发送到下游站点的所有复制封包来实现的。该方案以安全方式分发密钥，确保了在站点之间传送的数据是以安全方式完成的，并且支持了带有差错处理的密钥更新。与对于发送到下游站点的每个复制封包要求不同密钥的“下游”方案相比，该方案要求更少的计算和存储资源。此外，与“下游”方案相比，该方案对于用户来说是实现和理解起来更简单的，并且提供了更好的封包级可追溯性和故障排查。

[0028] II.架构

[0029] 图1描绘了用于为多站点数据中心提供安全密钥分发和管理的示例布置100。布置100包括三个站点，有时也称为“交付点”(pod)，在图1中标识为站点1、站点2和站点3，它们经由站点间网络(Inter-Site Network,ISN)140通信地耦合。每个站点分别包括SDN控制器110、120、130，脊柱交换机112、122、132，以及叶子交换机116、126、136。SDN控制器110、120、130——也称为应用策略基础设施控制器(Application Policy Infrastructure Controller,APIC)——监视和管理其各自的站点处的数据中心交换结构的操作并且可以用硬件、计算机软件或者硬件和计算机软件的任何组合来实现。如下文更详细描述的，SDN

控制器110、120、130被配置成有能力生成安全性关联密钥(Security Association Key，SAK)，下文也称为“密钥”，其在Cloudsec数据平面中被用于对在站点之间传输的数据加密和解密。此外，虽然SDN控制器110、120、130在附图中描绘时和在本文中描述时是在单个SDN控制器的情境中的，但这是为了说明而做的并且实施例不限于此示例，而是适用于SDN控制器110、120、130被实现为具有多个SDN控制器的SDN控制器集群。脊柱交换机112、122、132和叶子交换机116、126、136可由任何类型的网络交换机实现并且实施例不限于任何特定类型的网络交换机。根据一实施例，脊柱交换机112、122、132中的脊柱交换机脊柱2各自分别包括密钥数据114、124、134，密钥数据可包括用于对通过ISN 140发送和/或接收的封包加密和/或解密的密钥。密钥数据114、124、134可包括被脊柱交换机用来选择特定密钥来对加密的数据解密的其他信息，如下文更详细描述。

[0030] 每个站点可包括其他元素，包括硬件元素、软件元素以及硬件元素和软件元素的任何组合，这可依据特定实现方式而变化。例如，每个站点可包括连接到各个叶子交换机的硬件服务器，并且每个硬件服务器可托管多个虚拟服务器/端点，这些虚拟服务器/端点出于简洁目的在图1中没有描绘。ISN 140是提供多站点数据中心中的站点之间的连通性的外部公共网络。ISN 140可利用任何类型的DCI策略来实现，例如VXLAN，以支持站点之间的流量。

[0031] 布置100还包括SDN多站点控制器(MSC)150，其是在管理平面中连接SDN控制器110、120、130并且监视和管理站点间配置和操作的SDN控制器。根据一实施例，这包括在多站点数据中心的站点之间分发和管理密钥以使得能够为在云中通过第3层公共网络通信的DCI使能设备实现思科的Cloudsec加密，该加密将IEEE MACsec用于UDP封包，尤其是VXLAN封包。SDN MSC 150可以用硬件、计算机软件或者硬件和计算机软件的任何组合来实现。根据一实施例，SDN MSC 150经由消息传递总线160与SDN控制器110、120、130通信，该消息传递总线160可例如利用传输层安全性(Transport Layer Security，TLS)来实现。然而，实施例不限于使用TLS或TCP/IP网络，而是可使用任何类型的安全消息传递机制。根据一实施例，SDN控制器110、120、130和SDN MSC 150各自支持表述性状态转移(REpresentational State Transfer，REST)应用程序接口(Application Program Interface，API)，REST API可与数据中心中使用的基于应用中心基础设施(Application Centric Infrastructure，ACI)和非基于ACI的云SDN控制器相集成。

[0032] III.上游密钥分配和分发

[0033] 根据一实施例，上游密钥分配是由SDN MSC 150联合SDN控制器110、120、130实现的。图2A和图2B包括描绘了根据一实施例的上游密钥分配和分发方案的流程图200。在步骤202中，SDN MSC 150为每个参与的Cloudsec使能站点(例如图1的站点1、站点2和站点3)指派一个或多个唯一安全信道识别符(Secure Channel Identifier，SCI)。SCI是用于在数据平面中在共享相同的密码属性的参与Cloudsec设备之间建立的单向安全关联信道的唯一识别符，在该数据平面中SAK被用于对网络流量加密和解密。可能并非多站点数据中心中的所有站点都一定与多站点数据中心中的其他站点通信，并且SCI不需要被指派给非参与站点，或者没有使能Cloudsec的站点。SDN MSC 150可在下述情况下向特定站点指派单个SCI：单个安全信道将被用于该特定站点与多站点数据中心中的所有其他参与的Cloudsec使能站点之间的加密通信的情况。替代地，SDN MSC150可在下述情况下向特定站点指派多个

SCI:多个安全信道将被用于该特定站点与多站点数据中心中的其他参与的Cloudsec使能站点之间的加密通信的情况。SDN MSC 150可在本地为每个站点存储SCI,例如,存储在由SDN MSC 150维护的表格中。

[0034] 在步骤204中,站点——下文中称为“上游站点”——生成将被用于对由该上游站点发送的VXLAN封包有效载荷加密的本地对称密钥。此密钥也被接收站点——下文中称为“下游站点”——用来对加密的封包解密。例如,SDN控制器110生成用于对由站点1经由ISN 140发送到站点2和站点3的封包加密的密钥。此密钥也被站点2和站点3用来对经由ISN 140从站点1接收的加密封包解密。

[0035] 在步骤206中,上游站点将关联号(Association Number,AN)与生成的密钥关联起来。AN是SAK在安全性关联信道内的唯一识别符。例如,SDN控制器110将AN与生成的密钥相关联。AN被上游站点处的上游设备插入到加密封包的Cloudsec(MACsec)头部中,并且如下文更详细描述的,被下游站点处的下游设备用来与SCI相关联地确定用于对加密封包解密的正确密钥。根据一个实施例,AN具有值0或1,并且当密钥不再被使用时AN可被再使用。以这种方式使用AN允许了每个下游设备为每个SCI维护两个部署的密钥并且基于存储在接收到的封包的MACsec头部中的AN值与SCI相结合来选择用于对加密的VXLAN有效载荷解密的正确密钥。例如,密钥数据114、124、134可包括表格,其中该表格的每一行为SCI和AN的特定组合指定了密钥。根据本文描述的方案,该表格对于每个SCI可包括两个密钥,其中密钥之一对应于AN=0,并且另一密钥对应于AN=1。

[0036] 在步骤208中,上游站点将密钥和相应的SCI和AN提供给SDN MSC 150。例如,SDN控制器110将SDN MSC 150发出的密钥和相应的SCI以及关联的AN提供给SDN MSC 150。替代地,如果只有单个SCI被指派给了站点1,因为站点1将与所有其他站点使用单个安全信道,则SDN控制器110可只将密钥和关联的AN提供给SDN MSC 150,并且SDN MSC 150可基于来自SDN控制器110的通信来得出SCI。SDN MSC150可将密钥和相应的SCI和AN与站点1相关联地存储。例如,SDN MSC 150可将密钥和AN添加到表格中与SDN MSC 150发出给站点1的SCI相对应的行。

[0037] 在步骤210中,SDN MSC 150将密钥和相应的SCI和AN分发到每个下游站点。在本示例中,SDN MSC 150分别经由SDN控制器120、130将密钥和相应的SCI和AN分发到站点2和站点3。

[0038] 在步骤212中,每个下游站点利用密钥来配置其各自的交换机。这只需要对将从发送站点接收加密数据的交换机执行。例如,SDN控制器120将脊柱交换机122中的脊柱交换机脊柱2编程为使用密钥来对既是在与SCI相对应的安全信道上接收又在Cloudsec头部中具有AN的加密封包解密。如下文更详细描述的,对AN的使用允许了当前密钥被保留并且在替换密钥的部署没有成功时继续被用于对在多站点数据中心中的站点之间传输的封包的Cloudsec加密。

[0039] 在步骤214中,每个下游站点报告密钥在其本地交换机上的部署状态。例如,SDN控制器120向SDN MSC 150报告密钥在脊柱交换机脊柱2上的部署状态。部署状态可例如指示出密钥部署的状态以及成功或失败。在本示例中,SDN控制器130也向SDN MSC 150报告密钥在站点3上并且更具体而言是在脊柱交换机脊柱2上的部署状态。SDN MSC 150可使用超时来在下述情况下确定密钥的部署不成功:在指定的时间量内没有接收到部署状态消息的情

况。例如，如果SDN MSC 150在指定时间量内没有从站点3接收到部署状态消息，例如因为站点3上的差错、通信差错等等，则SDN MSC 150可确定密钥在站点3上的部署不成功。

[0040] 在步骤216中，SDN MSC 150将下游站点的密钥部署状态提供给上游站点。例如，SDN MSC 150向SDN控制器110报告站点2和站点3上的密钥的部署状态。这可利用单个消息来实现或者对于每个下游站点利用单独的消息来实现。例如，在向上游站点报告部署结果之前，SDN MSC 150可等待直到已从每个下游站点接收到部署响应为止。部署失败的数目不重要，因为即使在单个下游站点上部署密钥失败也意味着该密钥不能被使用。

[0041] 在步骤218中，上游站点检查下游站点的部署状态以确定密钥是否可被使用。在SDN MSC 150为每个下游站点发送单独的部署状态消息的情况下，则上游站点等待直到已针对每个下游站点接收到部署状态消息为止。

[0042] 在步骤220中，响应于密钥在所有下游站点上的成功部署，上游站点在其交换机上部署密钥以对由上游站点在安全信道上发送的封包加密。例如，SDN控制器110将脊柱交换机脊柱2编程为使用密钥来对由脊柱交换机脊柱2在安全信道上发送的VXLAN封包有效载荷加密。

[0043] 在步骤222中，响应于密钥在下游站点上的不成功部署，上游站点丢弃密钥。如果该密钥是上游站点部署的第一个密钥，则上游站点可取决于“安全模式”配置而采取不同的动作。例如，对于“必须安全”模式，上游站点可丢弃封包，直到密钥可被成功部署在所有下游站点上为止。替代地，对于“应当安全”模式，封包可在没有加密的情况下被发送到下游站点。如果该密钥不是上游站点部署的第一个密钥，则上游站点可继续使用当前密钥。

[0044] 图3A描绘了利用本文描述的方案在每个站点对应单个发送加密密钥的情境中用于在站点1、站点2和站点3之间交换数据的发送和接收密钥的密钥图。标签被表述为以下形式：<密钥类型>-<密钥ID>:AN，其中TX指的是发送或加密密钥，并且RX指的是接收或解密密钥。注意在单个发送密钥的情境中，一个密钥被用于对站点发送的数据加密，无论下游站点如何。图3B描绘了在每个站点对应单个发送加密密钥的情境中用于在站点1、站点2和站点3之间交换数据的发送和接收密钥的密钥表。

[0045] 图4A描绘了利用本文描述的方案在每个站点对应多个发送加密密钥的情境中用于在站点1、站点2和站点3之间交换数据的发送和接收密钥的密钥表。注意在多加密密钥的情境中，取决于下游站点，即，对于上游和下游站点的每个组合，一不同的密钥被用于对站点发送的数据加密。图4B描绘了在每个站点对应多个发送加密密钥的情境中用于在站点1、站点2和站点3之间交换数据的发送和接收密钥的密钥表。图3A、图3B、图4A和图4B中描绘的示例可被扩展到具有任何数目的站点的实现方式。

[0046] IV.密钥更新

[0047] 上文描述的用于创建和分发新密钥的方案适用于密钥更新场景。密钥更新，即，利用新的加密密钥替换当前加密密钥，可例如在当前密钥期满之前或之后、响应于第三方攻击、根据各种安全性策略等等而执行。与上文描述的新密钥场景中一样，当上游站点创建新密钥来替换现有密钥时，新密钥不被上游站点用来对封包加密，直到从SDN MSC 150接收到对于新密钥已被成功部署在所有参与站点上的确认为止。如果新密钥未被成功部署在任何参与站点上，则新密钥不被使用，并且可被丢弃，并且现有密钥继续被使用。

[0048] 根据一实施例，当新密钥被成功部署在下游站点上并且正被上游站点用来对封包

加密时，下游站点将旧密钥保持指定时间量。例如，SDN控制器110、120、130可将旧密钥分别在密钥数据114、124、134中保持指定时间量。这确保了利用旧密钥加密的无序封包可被下游站点解密，即使加密的封包是在使用替换密钥之后被接收到的。指定时间量可从策略获得和/或例如由管理用户配置。此外，根据一实施例，上游站点不会在安全性信道中再使用与较旧的工作密钥相关联的AN，除非新的密钥已被成功部署在安全信道中的所有下游站点处。

[0049] V.安全性和其他考虑

[0050] 如前文所描述，可通过利用TLS的消息传递总线160在站点即站点1、站点2、站点3与SDN MSC 150之间安全地交换数据。这包括密钥、SCI、AN和部署状态信息。根据一实施例，像MACsec密钥管理中使用的那样的密钥加密密钥(Key Encryption Key，KEK)被用于对站点之间交换的SAK——即密钥——加密以提供额外的安全性。KEK可被配置在SDN MSC 150处并且被分发到SDN控制器110、120、130。虽然在附图中描绘和在本文中描述实施例时是在数据中心中的ACI站点间安全性的情境中进行的，但实施例不限于此情境，而是适用于针对其他类型的IP流量流的非ACI云部署。

[0051] 在云部署中，本文描述的方案相比对每个下游站点使用不同的加密密钥的设备级控制平面方案(例如通过BGP的捎带(piggybacking over BGP)或者类似的)提供了许多益处。这些方案对于每个下游站点具有不同的MACsec头部，而利用本文描述的方案，相同的加密密钥和MACsec头部可被用于发送到不同下游站点的封包的每个拷贝中，使得本方案很适合于多播应用。将上游站点的分配的加密密钥和MACsec头部用于标记和加密提供了从源到目的地的封包的更好可追溯性并且提供了更容易的故障排查。本文描述的基于SDN控制器的方案也是更容易实现的。

[0052] VI.示例用例

[0053] 图5A-图5E描绘了本文描述的用于为多站点数据中心提供安全密钥分发和管理的方案的示例用例。这些用例示出了在站点1、站点2、站点3和SDN MSC 150之间交换的数据和消息。图5A描绘了SDN MSC 150将AN＝0的单个密钥K1从站点1成功部署到站点2和站点3。密钥K1由站点1生成并且带着AN被提供给SDN MSC 150，SDN MSC 150将密钥K1和AN分发到站点2和站点3。在站点1经由SDN MSC 150接收到对于密钥K1被成功部署在了站点2和站点3两者上的确认之后，站点1将密钥K1部署在其本地交换机上，例如，脊柱交换机脊柱2。VXLAN封包有效载荷被脊柱交换机脊柱2利用密钥K1加密并且SCI和AN被包括在MACsec头部中以允许站点2和站点3处的下游设备得出用于对加密的VXLAN封包有效载荷解密的正确解密密钥。

[0054] 图5B描绘了密钥K1到密钥K2的成功密钥更新。如前文所描述，密钥更新可出于各种各样的原因而发生，例如在当前密钥期满之前或之后，响应于第三方攻击，根据各种安全性策略，等等。注意在图5B中，在密钥K2的成功部署之后，站点2和站点3都具有两个部署的密钥：密钥K1，其中AN＝0；以及密钥K2，其中AN＝1。虽然密钥K2将被站点1处的上游设备用来对后续VXLAN封包有效载荷加密，但密钥K1仍可被站点2和站点3处的下游设备用来对利用密钥K1加密的无序封包解密。此外，密钥K1在密钥K2的部署不成功的情况下保持可用，并且封包继续被站点1处的上游设备利用密钥K1来加密。

[0055] 图5C描绘了因为站点3处的失败而引起的密钥K2到密钥K3的不成功密钥更新，该

失败阻止了新密钥K3的部署。在此示例中，站点1在使用密钥K2来对发送到站点2和站点3的封包加密并且尝试将带有AN＝0的新的密钥K3部署到站点2和站点3。在尝试了部署，并且站点3上发生部署新密钥K3的差错之后，站点2和站点3都有两个部署的密钥，但这些密钥是不同的，因为新密钥K3向站点2的部署是成功的。站点2具有密钥K3，其中AN＝0，以及密钥K2，其中AN＝1，而站点3具有密钥K1，其中AN＝0，以及密钥K2，其中AN＝1。在站点3部署新密钥K3失败之后，站点1继续使用密钥K2来对发送到站点2和站点3两者的封包加密。

[0056] 图5D描绘了在多次密钥更新尝试之后AN＝0的新密钥K4的成功部署。图5D中描绘的流程开始于图5C的流程结束时，此时站点1使用AN＝1的密钥K2来对发送到站点2和站点3的封包加密。站点2和3各自具有两个部署的密钥。站点2具有密钥K3，其中AN＝0，以及密钥K2，其中AN＝1，而站点3具有密钥K1，其中AN＝0，以及密钥K2，其中AN＝1。AN＝0的新密钥K4被成功部署在站点2和站点3两者处。由于新密钥K4的AN＝0，新的新密钥K4替换站点2处的密钥K3和站点3处的密钥K1。在新密钥K4的成功部署之后，站点2和站点3都具有相同的部署密钥:K4，其中AN＝0，以及密钥K2，其中AN＝1。站点1处的上游设备利用密钥K4对后续VXLAN封包加密并且将SCI和AN＝0包括在加密的封包的MACsec头部中以使得站点2和站点3处的下游设备，例如分别是脊柱交换机122、132中的脊柱交换机脊柱2，能够适当地选择密钥K4作为解密密钥来对加密的VXLAN封包解密。

[0057] 图5E描绘了因为超时引起的密钥K2到密钥K3的不成功密钥更新。这个示例与图5C的示例相同，只不过在此示例中，站点1在定时器期满之前没有从SDN MSC 150接收到关于密钥K3在站点3上的部署状态。在此情形中，执行的步骤与当站点1接收到对于站点3部署新密钥K3的确认失败时执行的相同，即，站点2部署了密钥K3，其中AN＝0，并且部署了密钥K2，其中AN＝1，而站点3部署了密钥K1，其中AN＝0，并且部署了密钥K2，其中AN＝1。站点1继续使用密钥K2来对发送到站点2和站点3两者的封包加密。

[0058] VII.实现示例

[0059] 根据一个实施例，本文描述的技术由至少一个计算设备实现。这些技术可完全或部分利用至少一个服务器计算机和/或其他计算设备的组合来实现，这些服务器计算机和/或其他计算设备利用网络来耦合，例如封包数据网络。计算设备可被硬连线来执行这些技术，或者可包括被持续性地编程来执行这些技术的数字电子设备，例如至少一个专用集成电路(ASIC)或者现场可编程门阵列(FPGA)，或者可包括被编程来根据固件、存储器、其他存储装置或者组合中的程序指令执行这些技术的至少一个通用硬件处理器。这种计算设备也可将定制的硬连线逻辑、ASIC或者FPGA与定制编程相组合来实现描述的技术。计算设备可以是服务器计算机、工作站、个人计算机、便携式计算机系统、手持设备、移动计算设备、可穿戴设备、身体安装或者可植入设备、智能电话、智能电器、联网设备、诸如机器人或者无人驾驶地面或航空载具之类的自主或半自主设备、包含硬连线的和/或程序逻辑来实现描述的技术的任何其他电子设备、数据中心中的一个或多个虚拟计算机器或实例、和/或服务器计算机和/或个人计算机的网络。

[0060] 图6是图示出可用来实现实施例的示例计算机系统的框图。在图6的示例中，用于以硬件、软件或者硬件和软件的组合实现公开的技术的计算机系统600和指令被示意性地例如表示为方框和圆圈，详细的程度与本公开所属领域的普通技术人员用来交流计算机架构和计算机系统实现方式的程度相当。

[0061] 计算机系统600包括输入/输出(I/O)子系统602,其可包括总线和/或其他(一个或多个)通信机构,用于通过电子信号路径在计算机系统600的组件之间传达信息和/或指令。I/O子系统602可包括I/O控制器、存储器控制器和至少一个I/O端口。电子信号路径在图中被示意性地例如表示为线条、单向箭头或者双向箭头。

[0062] 至少一个硬件处理器604耦合到I/O子系统602来处理信息和指令。硬件处理器604可包括例如通用微处理器或微控制器和/或专用微处理器,例如嵌入式系统或图形处理单元(GPU)或者数字信号处理器或ARM处理器。处理器604可包括集成算术逻辑单元(ALU)或者可耦合到单独的ALU。

[0063] 计算机系统600包括存储器606的一个或多个单元,例如主存储器,其耦合到I/O子系统602来电子数字地存储要被处理器604执行的数据和指令。存储器606可包括易失性存储器,例如各种形式的随机访问存储器(RAM)或其他动态存储设备。存储器606也可以用于在处理器604要执行的指令的执行期间存储临时变量或其他中间信息。这种指令当被存储在处理器604可访问的非暂态计算机可读存储介质中时,可致使计算机系统600成为被定制来执行指令中指定的操作的专用机器。

[0064] 计算机系统600还包括非易失性存储器,例如只读存储器(ROM)608或者耦合到I/O子系统602的其他静态存储设备,用于为处理器604存储信息和指令。ROM 608可包括各种形式的可编程ROM(PROM),例如可擦除PROM(EPROM)或电可擦除PROM(EEPROM)。持续性存储装置610的一单元可包括各种形式的非易失性RAM(NVRAM),例如闪速存储器,或者固态存储装置、磁盘或者诸如CD-ROM或DVD-ROM之类的光盘,并且可耦合到I/O子系统602,用于存储信息和指令。存储装置610是非暂态计算机可读介质的示例,其可用于存储指令和数据,这些指令和数据当被处理器604执行时使得执行计算机实现的方法来执行本文的技术。

[0065] 存储器606、ROM 608或存储装置610中的指令可包括一个或多个指令集合,这些指令集合被组织为模块、方法、对象、函数、例程、或者调用。指令可被组织为一个或多个计算机程序、操作系统服务、或者包括移动app的应用程序。指令可包括操作系统和/或系统软件;一个或多个库来支持多媒体、编程或其他功能;数据协议指令或栈来实现TCP/IP、HTTP或其他通信协议;文件格式处理指令来解析或渲染利用HTML、XML、JPEG、MPEG或PNG编码的文件;用户界面指令来为图形用户界面(GUI)、命令行界面或者文本用户界面渲染或解释命令;应用软件,例如办公套件、互联网接入应用、设计和制造应用、图形应用、音频应用、软件工程应用、教育应用、游戏或杂项应用。指令可实现web服务器、web应用服务器或web客户端。指令可被组织为呈现层、应用层和数据存储层,例如使用结构化查询语言(SQL)或不使用SQL的关系数据库系统、对象存储、图形数据库、平面文件系统或其他数据存储。

[0066] 计算机系统600可经由I/O子系统602耦合到至少一个输出设备612。在一个实施例中,输出设备612是数字计算机显示器。可用于各种实施例中的显示器的示例包括触摸屏显示器或发光二极管(LED)显示器或液晶显示器(LCD)或电子纸显示器。取代显示设备或者除了显示设备以外,计算机系统600可包括其他(一个或多个)类型的输出设备612。其他输出设备612的示例包括打印机、票证打印机、绘图机、投影仪、声卡或显卡、扬声器、蜂鸣器或压电设备或其他音响设备、灯或LED或LCD指示器、触觉设备、致动器或者伺服系统。

[0067] 至少一个输入设备耦合到I/O子系统602来向处理器604传达信号、数据、命令选择或手势。输入设备614的示例包括触摸屏、麦克风、静态和视频数字相机、字母数字和其他

键、小键盘、键盘、绘图板、图像扫描仪、操纵杆、时钟、开关、按钮、刻度盘、滑块、和/或各种类型的传感器，例如力传感器、运动传感器、热量传感器、加速度计、陀螺仪、以及惯性测量单元(inertial measurement unit，IMU)传感器和/或各种类型的收发器，例如无线(比如蜂窝或Wi-Fi)、射频(RF)或红外(IR)收发器和全球定位系统(GPS)收发器。

[0068] 另一类型的输入设备是控制设备616，取代输入功能或者除了输入功能以外，其可执行光标控制或其他自动化控制功能，例如显示屏上的图形界面中的导引。控制设备616可以是触摸板、鼠标、轨迹球、或者光标方向键，用于向处理器604传达方向信息和命令选择并且用于控制显示器612上的光标移动。输入设备可具有两个轴上的至少两个自由度，即第一轴(例如，x)和第二轴(例如，y)，这允许了设备指定平面中的位置。另一类型的输入设备是有线、无线或光控制设备，例如操纵杆、魔杖、控制台、方向盘、踏板、变速杆机制或其他类型的控制设备。输入设备614可包括多种不同输入设备的组合，例如视频相机和深度传感器。

[0069] 在另一实施例中，计算机系统600可包括物联网(internet of things，IoT)设备，其中输出设备612、输入设备614和控制设备616中的一个或多个被省略。替代地，在这种实施例中，输入设备614可包括一个或多个相机、运动检测器、温度计、麦克风、地震检测器、其他传感器或检测器、测量设备或编码器，并且输出设备612可包括专用显示器，例如单行LED或LCD显示器、一个或多个指示器、显示面板、仪表、阀门、螺线管、致动器或伺服系统。

[0070] 当计算机系统600是移动计算设备时，输入设备614可包括全球定位系统(GPS)接收器，其耦合到GPS模块，该GPS模块能够对多个GPS卫星进行三角测量，从而确定和生成地理位置或定位数据，例如计算机系统600的地球物理位置的纬度-经度值。输出设备612可包括硬件、软件、固件和界面，用于生成位置报告封包、通知、脉冲或心跳信号、或者指定计算机系统600的位置的其他循环数据传输，单独地或者与其他专用数据相结合，针对的是主机624或服务器630。

[0071] 计算机系统600可利用定制的硬连线逻辑、至少一个ASIC或FPGA、固件和/或程序指令或逻辑来实现本文描述的技术，这些定制的硬连线逻辑、至少一个ASIC或FPGA、固件和/或程序指令或逻辑当被加载并且被与计算机系统结合来使用或执行时使得计算机系统或者将计算机系统编程为作为专用机器来操作。根据一个实施例，本文的技术是由计算机系统600响应于处理器604执行主存储器606中包含的至少一个指令的至少一个序列而执行的。这种指令可被从另一存储介质(例如存储装置610)读取到主存储器606中。对主存储器606中包含的指令的序列的执行使得处理器604执行本文描述的过程步骤。在替换实施例中，硬连线电路可取代软件指令或者与软件指令相结合被使用。

[0072] 术语“存储介质”在本文中用来指存储使得机器以特定方式操作的数据和/或指令的任何非暂态介质。这种存储介质可包括非易失性介质和/或易失性介质。非易失性介质例如包括光盘或磁盘，比如存储装置610。易失性介质包括动态存储器，比如存储器606。存储介质的常见形式例如包括硬盘、固态驱动器、闪存驱动器、磁数据存储介质、任何光或物理数据存储介质、存储器芯片，等等。

[0073] 存储介质与传输介质是有区别的，但可与传输介质结合使用。传输介质参与在存储介质之间传送信息。例如，传输介质包括同轴线缆、铜线和光纤，包括构成I/O子系统602的总线的导线。传输介质也可采取声波或光波的形式，例如在无线电波和红外数据通信期间生成的那些。

[0074] 在向处理器604运载至少一个指令的至少一个序列来执行时，可涉及可各种形式的介质。例如，指令可最初被承载在远程计算机的磁盘或固态驱动器上。远程计算机可将指令加载到其动态存储器中并且通过诸如光纤或者同轴线缆或者使用调制解调器的电话线之类的通信链路来发送指令。计算机系统600本地的调制解调器或路由器可接收通信链路上的数据并且将数据转换成可被计算机系统600读取的格式。例如，诸如射频天线或红外检测器之类的接收器可接收无线或光信号中承载的数据并且适当的电路可将该数据提供到I/O子系统602，例如将数据放置在总线上。I/O子系统602将数据运载到存储器606，处理器604从存储器606取回并执行指令。被存储器606接收的指令可以可选地在被处理器604执行之前或之后被存储在存储装置610上。

[0075] 计算机系统600还包括耦合到总线602的通信接口618。通信接口618提供到(一个或多个)网络链路620的双向数据通信耦合，网络链路620直接或间接连接到至少一个通信网络，例如网络622或者因特网上的公共或私有云。例如，通信接口618可以是以太网联网接口、综合服务数字网络(integrated-services digital network，ISDN)卡、线缆调制解调器、卫星调制解调器、或者提供到相应类型的通信线路的数据通信连接的调制解调器，所述通信线路例如是以太网线缆或者任何种类的金属线缆或者光纤线或者电话线。网络622广泛地表示局域网(LAN)、广域网(WAN)、校园网、互联网络或者这些的任何组合。通信接口618可包括LAN卡来提供到兼容的LAN的数据通信连接，或者被连线来根据蜂窝无线电话无线联网标准发送或接收蜂窝数据的蜂窝无线电话接口，或者被连线来根据卫星无线联网标准发送或接收数字数据的卫星无线电接口。在任何这种实现方式中，通信接口618通过运载表示各种类型的信息的数字数据流的信号路径发送和接收电信号、电磁信号或者光信号。

[0076] 网络链路620通常利用例如卫星、蜂窝、Wi-Fi或蓝牙技术间接地或者通过至少一个网络向其他数据设备提供电、电磁或光数据通信。例如，网络链路620可通过网络622向主机计算机624提供连接。

[0077] 此外，网络链路620可通过网络622提供连接，或者经由由互联网服务提供商(ISP)626操作的互联网设备和/或计算机提供到其他计算设备的连接。ISP 626通过被表示为互联网628的全球封包数据通信网络来提供数据通信服务。服务器计算机630可耦合到互联网628。服务器630广泛地表示任何计算机、数据中心、带有或不带有超级监督者的虚拟机或虚拟计算实例、或者执行诸如DOCKER或KUBERNETES之类的容器化程序系统的计算机。服务器630可表示电子数字服务，该电子数字服务是利用多于一个计算机或实例来实现的并且是通过传输web服务请求、HTTP有效载荷中的带有参数的统一资源定位符(URL)字符串、API调用、app服务调用、或其他服务调用来访问和使用的。计算机系统600和服务器630可形成分布式计算系统的元素，该分布式计算系统包括其他计算机、处理集群、服务器场或计算机的其他组织，它们合作来执行任务或执行应用或服务。服务器630可包括一个或多个指令集合，这些指令集合被组织为模块、方法、对象、函数、例程、或者调用。指令可被组织为一个或多个计算机程序、操作系统服务、或者包括移动app的应用程序。指令可包括操作系统和/或系统软件；一个或多个库来支持多媒体、编程或其他功能；数据协议指令或栈来实现TCP/IP、HTTP或其他通信协议；文件格式处理指令来解析或渲染利用HTML、XML、JPEG、MPEG或PNG编码的文件；用户界面指令来为图形用户界面(GUI)、命令行界面或者文本用户界面渲染或解释命令；应用软件，例如办公套件、互联网接入应用、设计和制造应用、图形应用、音频应

用、软件工程应用、教育应用、游戏或杂项应用。服务器630可包括web应用服务器，该web应用服务器托管呈现层、应用层和数据存储层，例如使用结构化查询语言(SQL)或不使用SQL的关系数据库系统、对象存储、图形数据库、平面文件系统或其他数据存储。

[0078] 计算机系统600可通过(一个或多个)网络、网络链路620和通信接口618发送消息和接收数据和指令，包括程序代码。在因持网示例中，服务器630可通过因特网628、ISP626、本地网络622和通信接口618发送所请求的应用程序的代码。接收到的代码可在其被接收到时被处理器604执行，和/或被存储在存储装置610或其他非易失性存储装置中以便以后执行。

[0079] 本部分中描述的指令的执行可以以被执行并且由程序代码及其当前活动构成的计算机程序的实例的形式实现进程。取决于操作系统(OS)，进程可由同时执行指令的多个执行线程构成。在此上下文中，计算机程序是指令的被动集合，而进程可以是这些指令的实际执行。若干个进程可与同一程序相关联；例如，打开同一程序的若干个实例经常意味着多于一个进程在被执行。多任务处理可被实现来允许多个进程共享处理器604。虽然每个处理器604或者处理器的核心每次执行单个任务，但计算机系统600可被编程为实现多任务处理来允许每个处理器在被执行的任务之间切换，而不必等待每个任务完成。在一实施例中，切换可在任务执行输入/输出操作时执行，在任务指示出其可被切换时执行，或者在硬件中断时执行。可以实现时间共享来通过迅速地执行情境切换以同时提供多个进程的并发执行的外观，从而来允许交互式用户应用的快速响应。在一实施例中，为了安全性和可靠性，操作系统可防止独立进程之间的直接通信，提供经严格调解和控制的进程间通信功能。

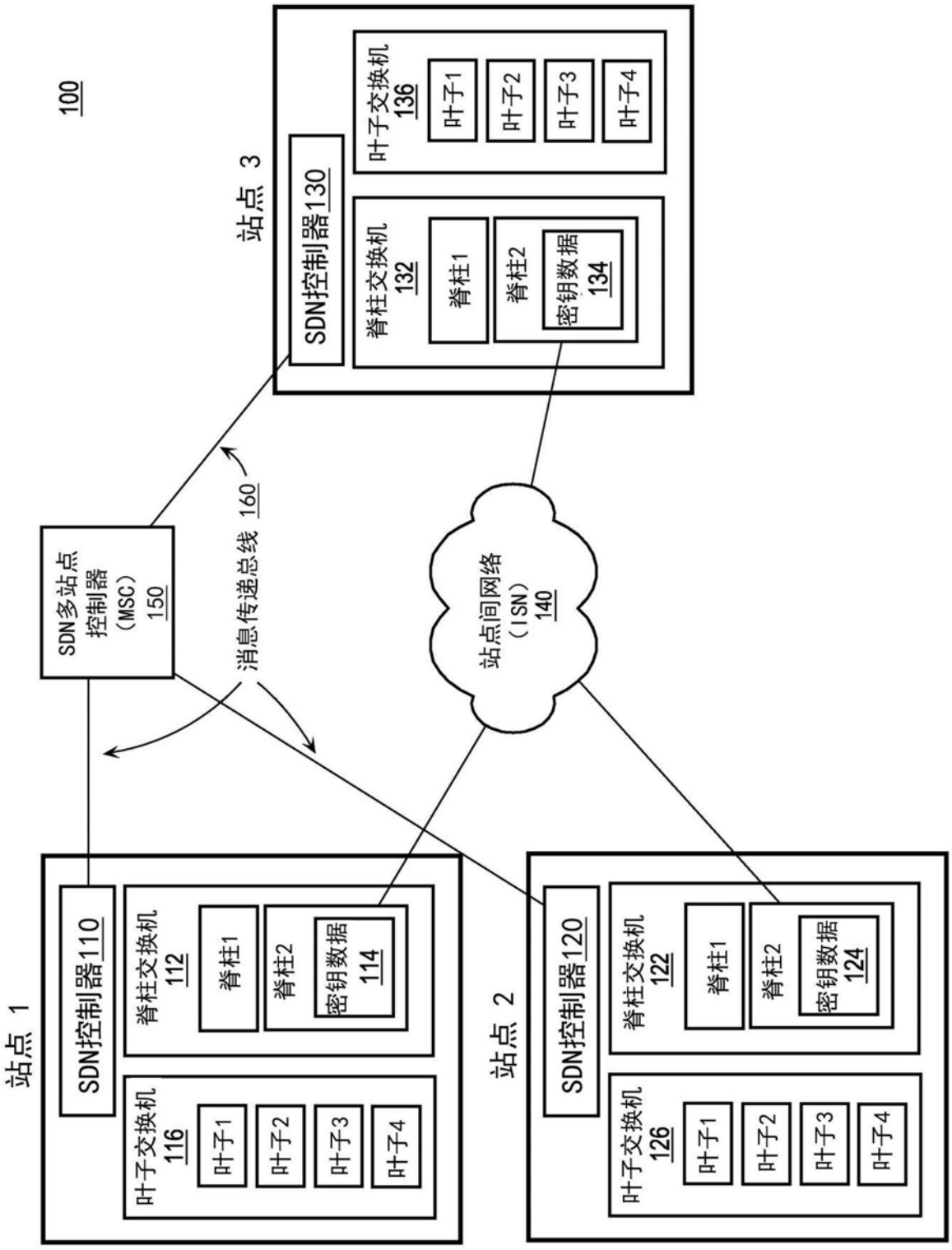

100
站点 1
SDN控制器110
脊柱交换机112
脊柱1
脊柱2
密钥数据114
叶子交换机116
叶子1
叶子2
叶子3
叶子4
站点 2
SDN控制器120
脊柱交换机122
脊柱1
脊柱2
密钥数据124
叶子交换机126
叶子1
叶子2
叶子3
叶子4
站点 3
SDN控制器130
脊柱交换机132
脊柱1
脊柱2
密钥数据134
叶子交换机136
叶子1
叶子2
叶子3
叶子4
SDN多站点控制器（MSC）150
消息传递总线 160
站点间网络（ISN）140

图1

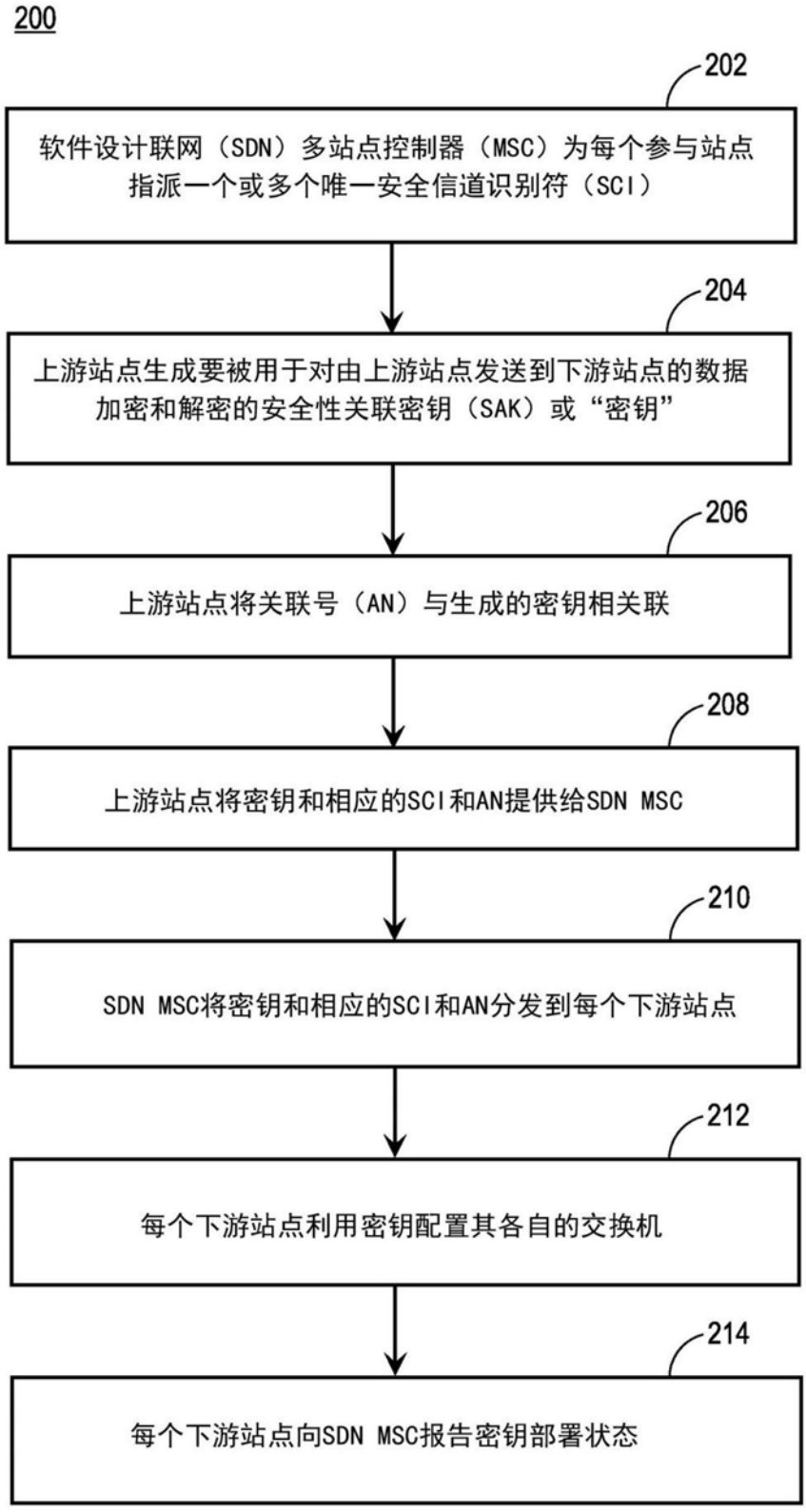

200
202
软件设计联网（SDN）多站点控制器（MSC）为每个参与站点指派一个或多个唯一安全信道识别符（SCI）
204
上游站点生成要被用于对由上游站点发送到下游站点的数据加密和解密的安全性关联密钥（SAK）或“密钥”
206
上游站点将关联号（AN）与生成的密钥相关联
208
上游站点将密钥和相应的SCI和AN提供给SDN MSC
210
SDN MSC将密钥和相应的SCI和AN分发到每个下游站点
212
每个下游站点利用密钥配置其各自的交换机
214
每个下游站点向SDN MSC报告密钥部署状态

图2A

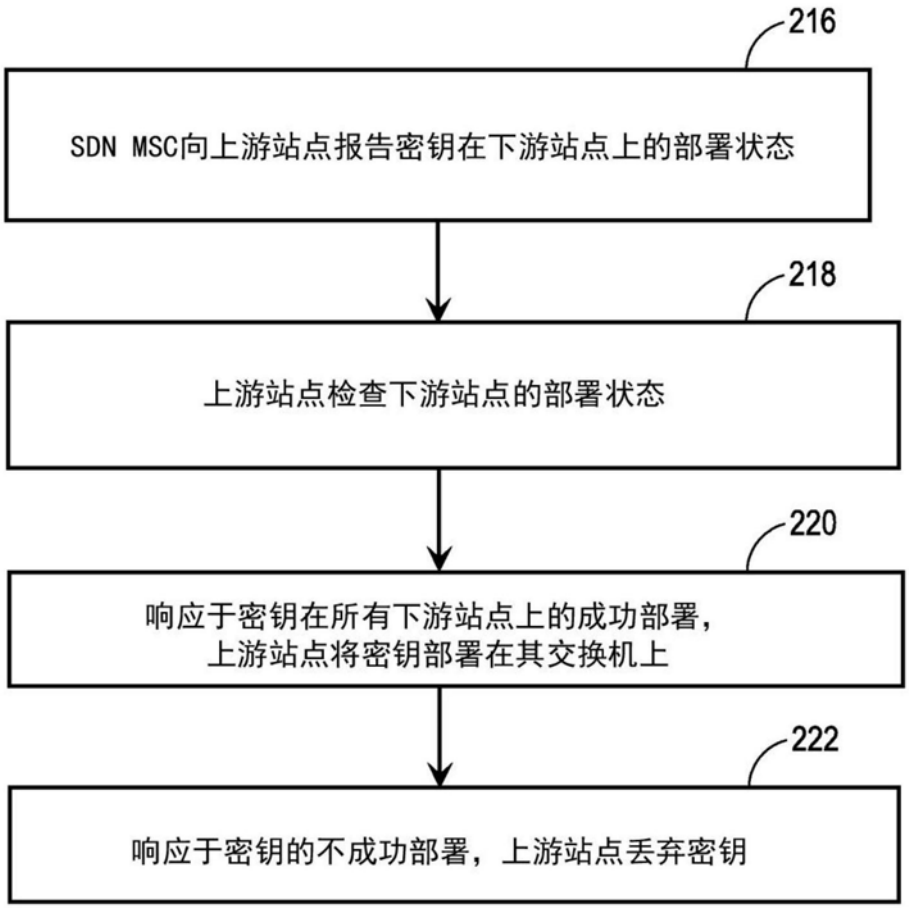

216
SDN MSC向上游站点报告密钥在下游站点上的部署状态
218
上游站点检查下游站点的部署状态
220
响应于密钥在所有下游站点上的成功部署，
上游站点将密钥部署在其交换机上
222
响应于密钥的不成功部署，上游站点丢弃密钥

图2B

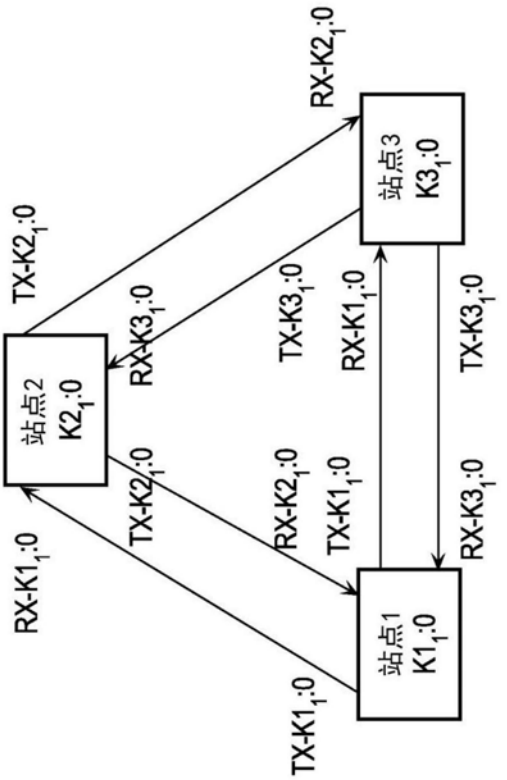


图3A

生成的站点密钥(密钥ID:AN)	远程站点	使用的TX密钥	使用的RX密钥
在站点1处 $K1_1$:0	站点2	$K1_1$:0	$K2_1$:0
	站点3	$K1_1$:0	$K3_1$:0
在站点2处 $K2_1$:0	站点1	$K2_1$:0	$K1_1$:0
	站点3	$K2_1$:0	$K3_1$:0
在站点3处 $K3_1$:0	站点1	$K3_1$:0	$K1_1$:0
	站点2	$K3_1$:0	$K2_1$:0

图3B

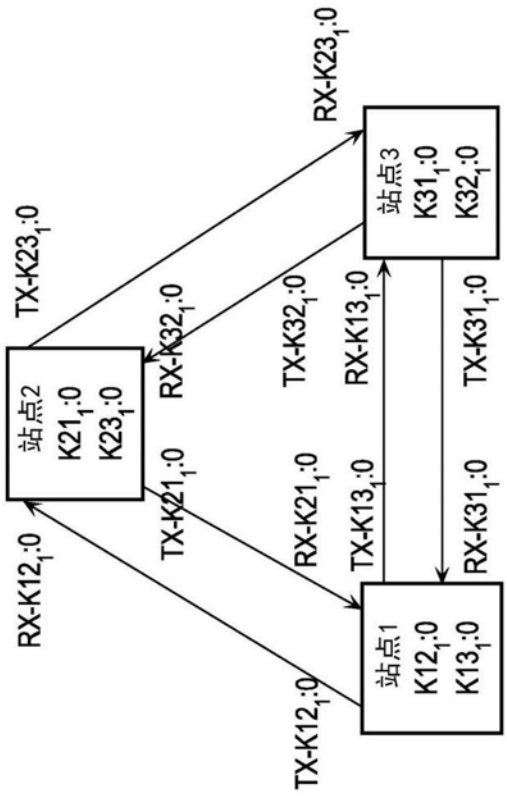


图4A

生成的站点密钥（密钥ID:AN）	远程站点	使用的TX密钥	使用的RX密钥
在站点1处	站点2	$K12_1:0$	$K21_1:0$
	站点3	$K13_1:0$	$K31_1:0$
在站点2处	站点1	$K21_1:0$	$K21_1:0$
	站点3	$K23_1:0$	$K23_1:0$
在站点3处	站点1	$K31_1:0$	$K13_1:0$
	站点2	$K32_1:0$	$K23_1:0$

图4B

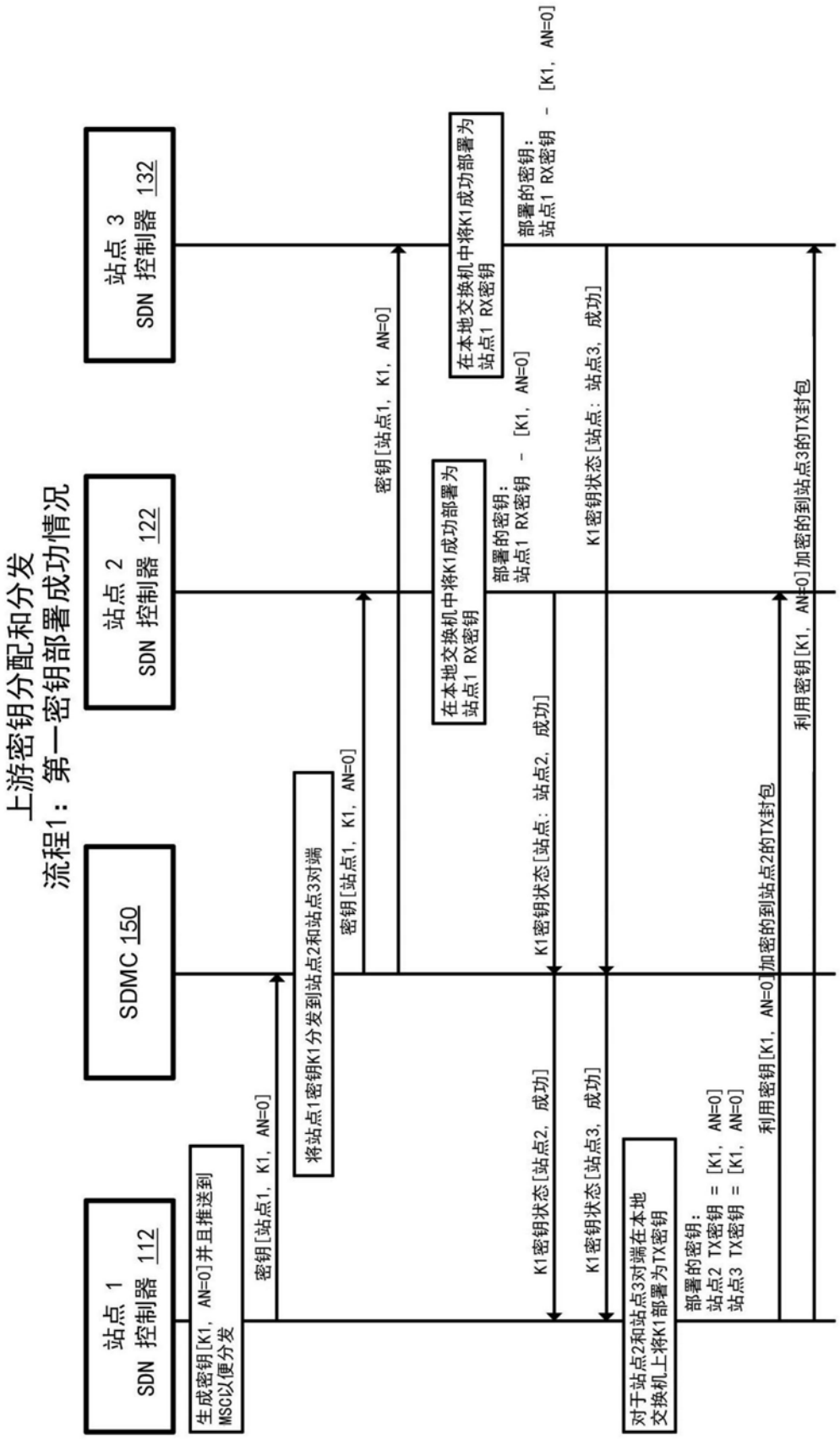

上游密钥分配和分发
流程1：第一密钥部署成功情况
站点 1
SDN 控制器 112
SDMC 150
站点 2
SDN 控制器 122
站点 3
SDN 控制器 132
生成密钥[K1，AN=0]并且推送到MSC以便分发
密钥[站点1，K1，AN=0]
将站点1密钥K1分发到站点2和站点3对端
密钥[站点1，K1，AN=0]
密钥[站点1，K1，AN=0]
在本地交换机中将K1成功部署为站点1 RX密钥
部署的密钥：
站点1 RX密钥 - [K1，AN=0]
在本地交换机中将K1成功部署为站点1 RX密钥
部署的密钥：
站点1 RX密钥 - [K1，AN=0]
K1密钥状态[站点：站点2，成功]
K1密钥状态[站点：站点3，成功]
K1密钥状态[站点2，成功]
K1密钥状态[站点3，成功]
对于站点2和站点3对端在本地交换机上将K1部署为TX密钥
部署的密钥：
站点2 TX密钥 = [K1，AN=0]
站点3 TX密钥 = [K1，AN=0]
利用密钥[K1，AN=0]加密的到站点2的TX封包
利用密钥[K1，AN=0]加密的到站点3的TX封包

图5A

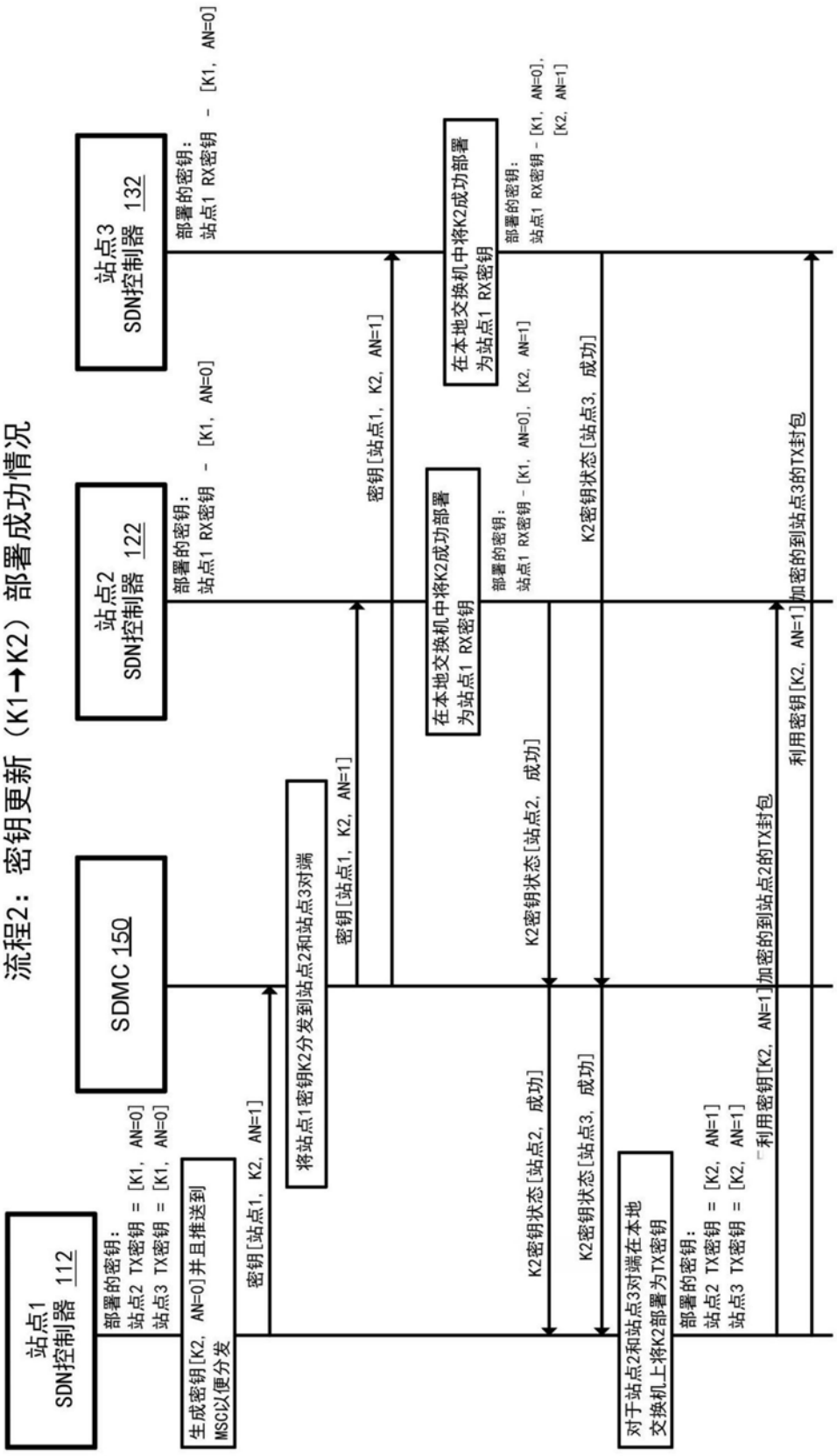

上游密钥分配和分发
流程2：密钥更新（K1→K2）部署成功情况
站点1
SDN控制器 112
SDMC 150
站点2
SDN控制器 122
站点3
SDN控制器 132
部署的密钥：
站点2 TX密钥 = [K1, AN=0]
站点3 TX密钥 = [K1, AN=0]
生成密钥[K2, AN=0]并且推送到MSC以便分发
密钥[站点1, K2, AN=1]
将站点1密钥K2分发到站点2和站点3对端
部署的密钥：
站点1 RX密钥 - [K1, AN=0]
密钥[站点1, K2, AN=1]
部署的密钥：
站点1 RX密钥 - [K1, AN=0]
在本地交换机中将K2成功部署为站点1 RX密钥
K2密钥状态[站点2, 成功]
在本地交换机中将K2成功部署为站点1 RX密钥
部署的密钥：
站点1 RX密钥 - [K1, AN=0], [K2, AN=1]
K2密钥状态[站点2, 成功]
K2密钥状态[站点3, 成功]
K2密钥状态[站点3, 成功]
对于站点2和站点3对端在本地交换机上将K2部署为TX密钥
部署的密钥：
站点2 TX密钥 = [K2, AN=1]
站点3 TX密钥 = [K2, AN=1]
利用密钥[K2, AN=1]加密的到站点2的TX封包
利用密钥[K2, AN=1]加密的到站点3的TX封包

图5B

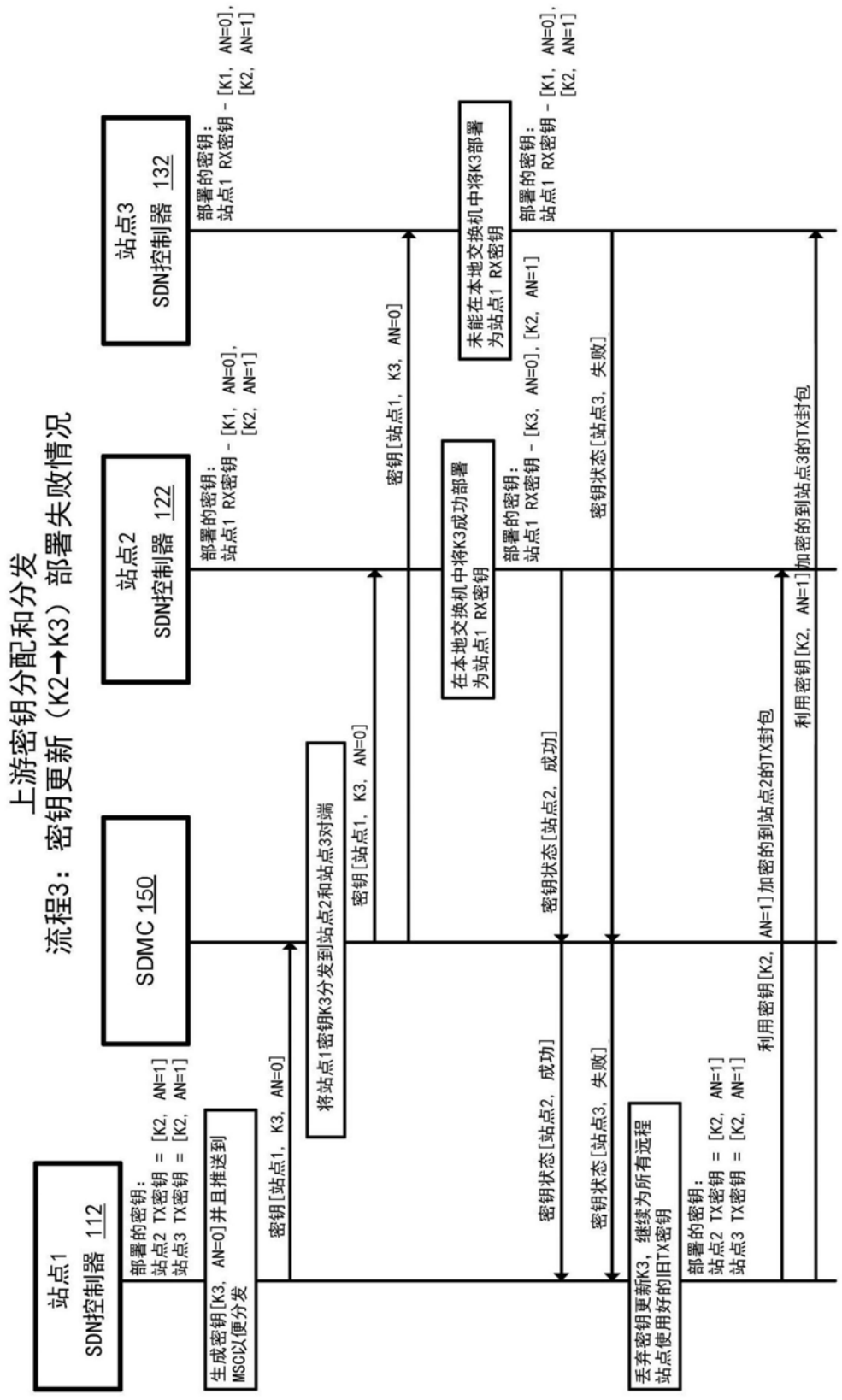

上游密钥分配和分发
流程3：密钥更新（K2→K3）部署失败情况
站点1
SDN控制器 112
SDMC 150
站点2
SDN控制器 122
站点3
SDN控制器 132
部署的密钥：
站点2 TX密钥 = [K2, AN=1]
站点3 TX密钥 = [K2, AN=1]
生成密钥[K3, AN=0]并且推送到MSC以便分发
密钥[站点1, K3, AN=0]
将站点1密钥K3分发到站点2和站点3对端
部署的密钥：
站点1 RX密钥 - [K1, AN=0], [K2, AN=1]
部署的密钥：
站点1 RX密钥 - [K1, AN=0], [K2, AN=1]
密钥[站点1, K3, AN=0]
在本地交换机中将K3成功部署为站点1 RX密钥
密钥状态[站点2, 成功]
部署的密钥：
站点1 RX密钥 - [K3, AN=0], [K2, AN=1]
未能在本地交换机中将K3部署为站点1 RX密钥
部署的密钥：
站点1 RX密钥 - [K1, AN=0], [K2, AN=1]
密钥状态[站点3, 失败]
密钥状态[站点2, 成功]
密钥状态[站点3, 失败]
丢弃密钥更新K3，继续为所有远程站点使用好的旧TX密钥
部署的密钥：
站点2 TX密钥 = [K2, AN=1]
站点3 TX密钥 = [K2, AN=1]
利用密钥[K2, AN=1]加密的到站点2的TX封包
利用密钥[K2, AN=1]加密的到站点3的TX封包

图5C

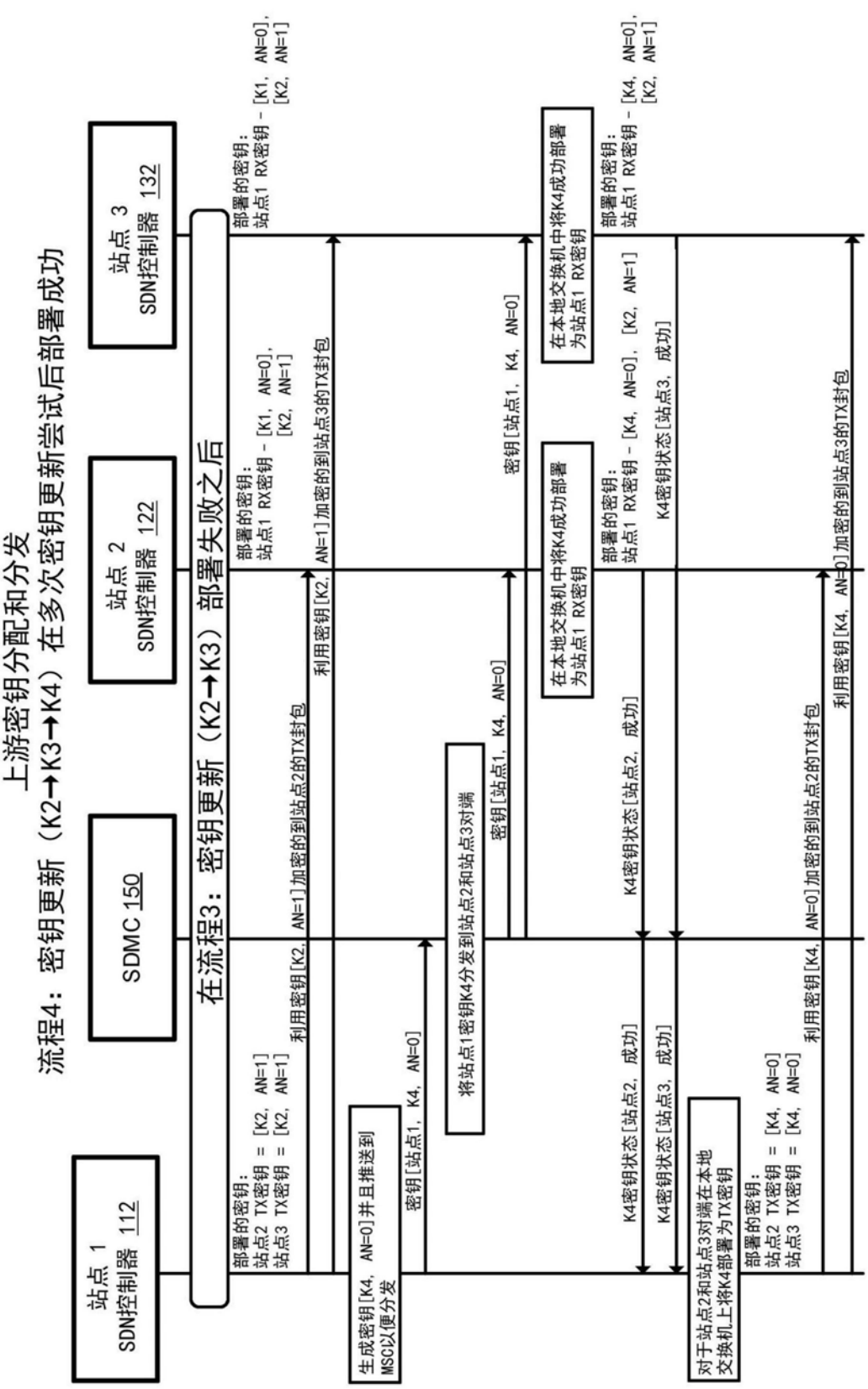

上游密钥分配和分发
流程4：密钥更新（K2→K3→K4）在多次密钥更新尝试后部署成功
站点 1
SDN控制器 112
SDMC 150
站点 2
SDN控制器 122
站点 3
SDN控制器 132
在流程3：密钥更新（K2→K3）部署失败之后
部署的密钥：
站点2 TX密钥 = [K2, AN=1]
站点3 TX密钥 = [K2, AN=1]
利用密钥[K2, AN=1]加密的到站点2的TX封包
部署的密钥：
站点1 RX密钥 - [K1, AN=0], [K2, AN=1]
利用密钥[K2, AN=1]加密的到站点3的TX封包
生成密钥[K4, AN=0]并且推送到MSC以便分发
密钥[站点1, K4, AN=0]
将站点1密钥K4分发到站点2和站点3对端
密钥[站点1, K4, AN=0]
在本地交换机中将K4成功部署为站点1 RX密钥
部署的密钥：
站点1 RX密钥 - [K4, AN=0], [K2, AN=1]
K4密钥状态[站点2, 成功]
K4密钥状态[站点3, 成功]
在本地交换机中将K4成功部署为站点1 RX密钥
部署的密钥：
站点1 RX密钥 - [K4, AN=0], [K2, AN=1]
K4密钥状态[站点3, 成功]
K4密钥状态[站点2, 成功]
对于站点2和站点3对端在本地交换机上将K4部署为TX密钥
部署的密钥：
站点2 TX密钥 = [K4, AN=0]
站点3 TX密钥 = [K4, AN=0]
利用密钥[K4, AN=0]加密的到站点2的TX封包
利用密钥[K4, AN=0]加密的到站点3的TX封包

图5D

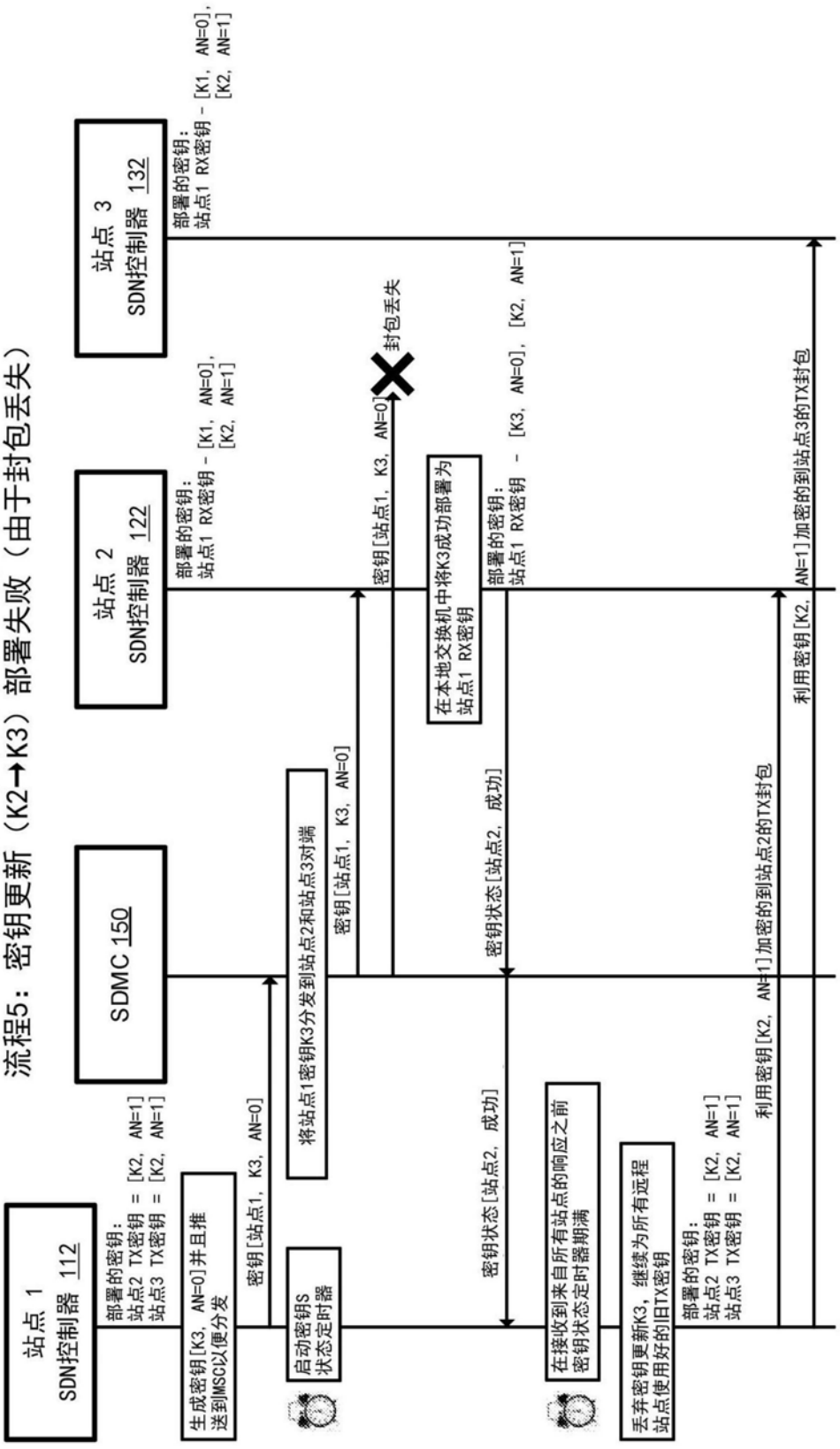

上游密钥分配和分发
流程5：密钥更新（K2→K3）部署失败（由于封包丢失）
站点 1
SDN控制器 112
SDMC 150
站点 2
SDN控制器 122
站点 3
SDN控制器 132
部署的密钥：
站点2 TX密钥 = [K2, AN=1]
站点3 TX密钥 = [K2, AN=1]
部署的密钥：
站点1 RX密钥 - [K1, AN=0], [K2, AN=1]
部署的密钥：
站点1 RX密钥 - [K1, AN=0], [K2, AN=1]
生成密钥[K3, AN=0]并且推送到MSC以便分发
密钥[站点1, K3, AN=0]
将站点1密钥K3分发到站点2和站点3对端
密钥[站点1, K3, AN=0]
封包丢失
在本地交换机中将K3成功部署为站点1 RX密钥
部署的密钥：
站点1 RX密钥 - [K3, AN=0], [K2, AN=1]
启动密钥S状态定时器
密钥状态[站点2, 成功]
密钥状态[站点2, 成功]
在接收到来自所有站点的响应之前密钥状态定时器期满
丢弃密钥更新K3，继续为所有远程站点使用好的旧TX密钥
部署的密钥：
站点2 TX密钥 = [K2, AN=1]
站点3 TX密钥 = [K2, AN=1]
利用密钥[K2, AN=1]加密的到站点2的TX封包
利用密钥[K2, AN=1]加密的到站点3的TX封包

图5E

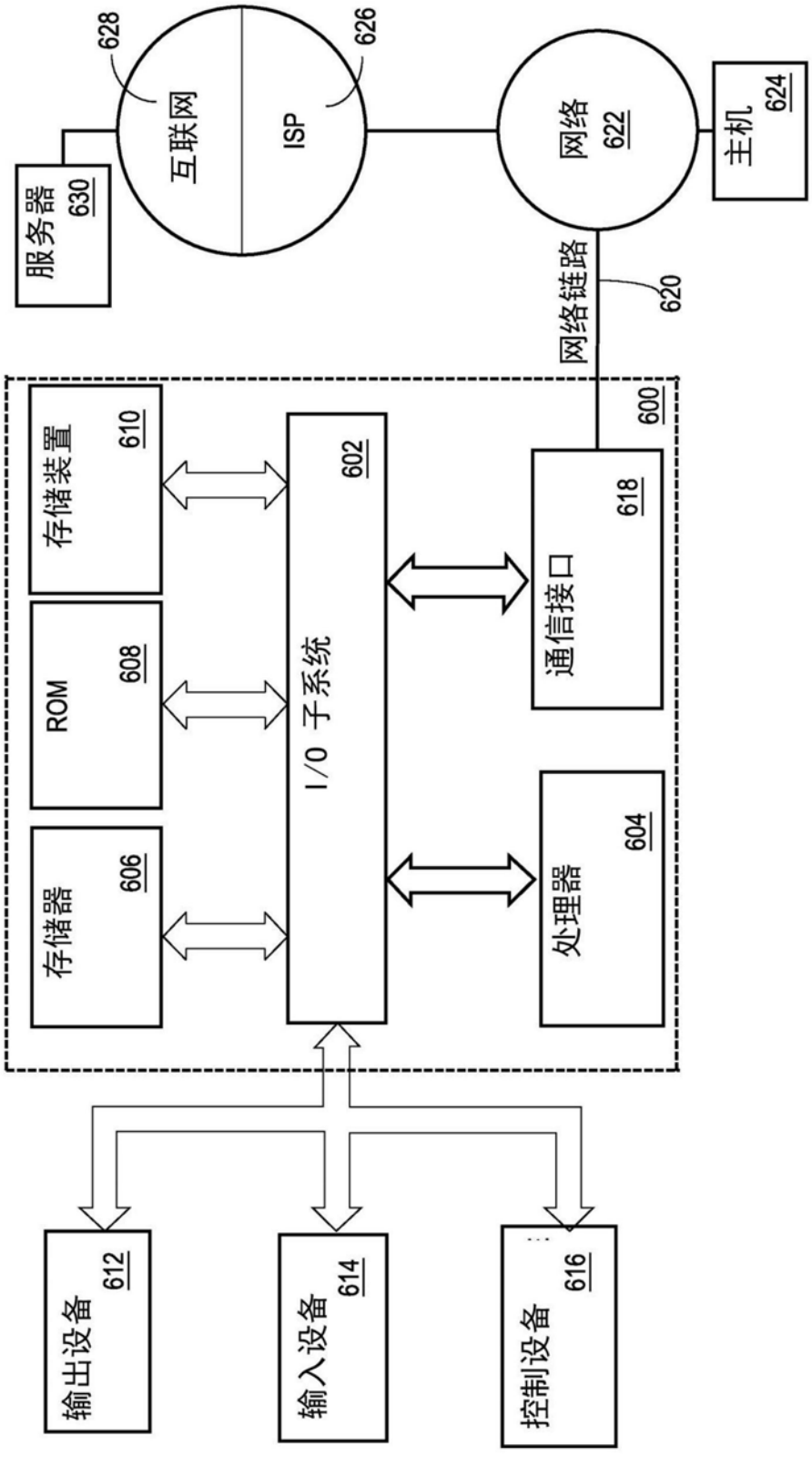

628
互联网
ISP
626
服务器
630
网络
622
主机
624
网络链路
620
600
存储装置
610
602
618
通信接口
ROM
608
I/O 子系统
存储器
606
处理器
604
输出设备
612
输入设备
614
控制设备
616

图6