(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 109688012 A
(43)申请公布日 2019.04.26

(21)申请号 201811639905.8

(22)申请日 2018.12.29

(71)申请人 杭州趣链科技有限公司
地址 310012 浙江省杭州市西湖区文三路199号13幢201室

(72)发明人 邱炜伟 李启雷 李伟 梁秀波 尹可挺 马晓敏

(74)专利代理机构 杭州求是专利事务所有限公司 33200
代理人 邱启旺

(51)Int.Cl.
H04L 12/24(2006.01)
H04L 9/32(2006.01)

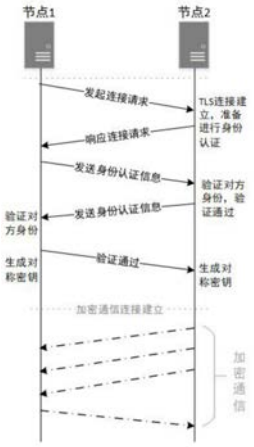
权利要求书2页 说明书5页 附图2页

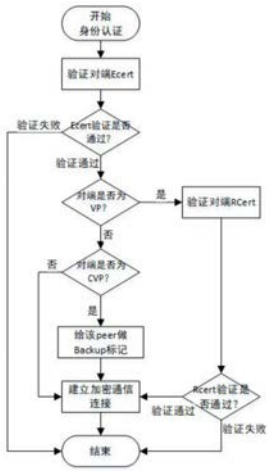
(54)发明名称

一种联盟链节点热备切换的方法

(57)摘要

本发明公开了一种联盟链节点热备切换的方法。节点热备切换的步骤具体为:候选节点与共识节点建立连接;共识节点实时将其网络配置及其共识路由表信息发送给候选节点进行备份;候选节点对共识节点进行故障检测,决定是否触发节点升级替换的过程;候选节点线上升级为共识节点,根据备份的网络配置去连接区块链网络的共识节点,同时将自身共识状态初始化到共识节点宕机时的状态,以此完成替换。该方法在由多个机构参与组成的联盟区块链网络中,机构的共识节点发生异常宕机,在不引入人工操作的前提下,自动完成候选节点线上升级为共识节点,保证了在不影响区块链网络共识效率的基础上,避免了机构内共识节点发生单点故障。





CN 109688012 A

1.一种联盟链节点热备切换的方法,其特征在于,包括如下步骤:

(1)候选节点网络配置:候选节点本质上是一个特殊的记账节点,持有线下第三方认证中心颁发的ECert和RCert证书;候选节点在启动之前,需要在其网络配置文件中指定它是哪个共识节点的候选节点。

(2)候选节点与共识节点建立连接:候选节点向共识节点发起建立连接请求,在物理连接建立完成以后,开始进行双方身份认证,若身份认证不通过,则连接建立失败;若身份认证通过,并且共识节点确认对端为其候选节点,则对其做Backup标记且放入候选列表中。

(3)候选节点对共识节点网络配置进行备份:在候选节点与共识节点的连接建立完成以后,共识节点每次网络连接信息发生变更,均会通知候选节点进行更新备份;备份的数据包括:区块链网络中的其他共识节点的地址连接信息、与共识节点相连的记账节点的地址连接信息、共识节点的候选列表。其中,记账节点包括候选节点,因为候选节点是特殊的记账节点。

(4)候选节点对共识节点进行故障检测:候选节点采用keepalive+超时的机制来判断共识节点是否存活,以此来决定是否触发节点升级替换操作;根据候选节点在候选列表中的位置来决定升级替换优先级,只有当排在前面的候选节点失效的时候,后面的候选节点才可触发升级替换。

(5)候选节点断开现有网络连接:当通过心跳、故障检测等方法确定共识节点发生异常宕机以后,候选节点的自动升级替换操作被触发;这是候选节点进行升级替换的第一步。

(6)候选节点更新线上网络配置文件:候选节点读取备份的网络配置文件,更新线上网络配置信息,作为步骤(8)网络连接建立的基础。

(7)注册并启动共识服务:启动了共识服务以后,这个节点就拥有了共识投票的功能,但是还未与共识网络的其他节点建立连接。

(8)候选节点建立共识网络连接:候选节点更新自己的身份信息,根据最新网络配置信息向其他节点发起建立连接请求,这些节点包括原来与共识节点相连的其他共识节点和记账节点,连接建立过程同步骤(2)。

2.如权利要求1所述的一种联盟链节点热备切换的方法,其特征在于,所述的步骤(1)中,我们根据证书的不同来确定节点拥有不同的权限,持有ECert表明节点有准入区块链网络的权限,持有RCert表明节点拥有参与共识投票的权限;共识节点持有ECert和RCert;记账节点持有ECert;候选节点持有ECert和RCert,但是RCert仅作为一个备份存在,在节点进行身份升级之前,它没有任何作用;另外,一个候选节点只能指定一个共识节点去获取相关网络连接信息。

3.如权利要求1所述的一种联盟链节点热备切换的方法,其特征在于,所述的步骤(2)中,一个共识节点可以与多个它的候选节点建立连接。

4.如权利要求1所述的一种联盟链节点热备切换的方法,其特征在于,所述的步骤(3)中,候选节点将接收到的网络配置信息持久化在备份网络配置文件中,不会影响候选节点目前线上自己的网路配置,只有当候选节点被触发去做升级替换的时候,线上的网络配置文件才会被备份的网络配置文件所替换,在节点完成升级替换以后,备份的网络配置文件才被删除。

5.如权利要求1所述的一种联盟链节点热备切换的方法,其特征在于,所述的步骤(4)

中,keepalive用来做候选节点与共识节点间的心跳检测,判断共识节点是否存活;超时机制主要用来判断当前命中的进行升级替换的候选节点是否失效,如果候选节点失效,候选列表也需要进行更新,将失效的候选节点从候选列表中移除。

6.如权利要求1所述的一种联盟链节点热备切换的方法,其特征在于,所述的步骤(5)中,候选节点本质上是一个特殊的记账节点,它可能与一个或多个共识节点建立了连接,因此在做线上升级之前需要先断开其与其他共识节点的连接。

7.如权利要求1所述的一种联盟链节点热备切换的方法,其特征在于,所述的步骤(8)中,由于建立连接的过程需要进行身份认证,因此候选节点在开始建立连接之前首先得更新自己的身份信息,这些身份信息需要与指定共识节点一一对应,在本系统中主要为hostname信息,保证节点升级替换后,节点唯一标识保持不变,这样,对于共识网络的其他节点来说,就好像只是某个共识节点发生了短暂地断开,网络连接发生了替换而已。完成身份信息更新以后,候选节点根据最新网络配置向其他节点发起连接。

一种联盟链节点热备切换的方法

技术领域

[0001] 本发明涉及去中心化的区块链CA证书体系，尤其涉及一种联盟链节点热备切换的方法。

背景技术

[0002] 随着区块链技术的普及，人们逐渐意识到它可为传统行业带来安全可靠、简化流程、节约成本和增强信任等优点，可以弥补多方协作带来效率低、成本高、操作风险大等缺点，所以备受需要多方对等合作企业的青睐。由于多方协作往往需要严格的身份认证和专门的准入、准出授权机制，因此联盟区块链也成为他们的主要选择。

[0003] 在联盟区块链中，为了防止受到其他企业节点出现拜占庭行为的影响，企业开发的业务应用交易往往是发送到自己部署的节点上去处理。目前在联盟区块链中，如果某个机构的节点出现异常宕机或者节点所在服务器出现硬件错误，虽然对于有一定容错性的区块链网络来说不会因为这个节点的宕机而受到影响，但对于企业来说，需要以最快的速度去恢复节点服务。目前常采用的恢复方法有以下两种：

[0004] 由机房运维人员线下操作节点启动前的相关配置，重新启动节点，如果是存储设备发生致命错误导致数据丢失，需要涉及新节点同步区块链网络数据。

[0005] 使用多个共识节点做数据与服务的备份，当一个共识节点出现异常的时候，上层应用感知以后切换服务节点。

[0006] 以上两种方法都存在一定的缺点，第一种方法由于引入人工操作，可能会导致节点服务长时间无法恢复，这对于与其相互通信的智能合约应用是极其不利的。另外，如果全网数据量极大，节点数据同步所花费的时间难以估计，会导致节点处于暂时不可用状态。第二种方法虽然具有快速恢复的优点，但是为了保证企业间共识投票的公平性，所有参与企业都必须部署同等数量共识节点，共识节点数量的增加将对共识效率产生极大的影响。

发明内容

[0007] 本发明的目的是针对现有技术的不足，提供一种联盟链节点热备切换的方法，使非验证节点线上升级为共识节点，完成权限升级与替换，实现在不影响共识效率的前提下，线上升级所花费时间为秒级。

[0008] 本发明的目的是通过以下技术方案来实现的：一种联盟链节点热备切换的方法，包括如下步骤：

[0009] (1)候选节点网络配置：候选节点本质上是一个特殊的记账节点，持有线下第三方认证中心颁发的ECert和RCert证书；候选节点在启动之前，需要在其网络配置文件中指定它是哪个共识节点的候选节点；

[0010] (2)候选节点与共识节点建立连接：候选节点向共识节点发起建立连接请求，在物理连接建立完成以后，开始进行双方身份认证，若身份认证不通过，则连接建立失败；若身份认证通过，并且共识节点确认对端为其候选节点，则对其做Backup标记且放入候选列表

中；

[0011] (3)候选节点对共识节点网络配置进行备份：在候选节点与共识节点的连接建立完成以后，共识节点每次网络连接信息发生变更，均会通知候选节点进行更新备份；备份的数据包括：区块链网络中的其他共识节点的地址连接信息、与共识节点相连的记账节点的地址连接信息、共识节点的候选列表。其中，记账节点包括候选节点，因为候选节点是特殊的记账节点；

[0012] (4)候选节点对共识节点进行故障检测：候选节点采用keepalive+超时的机制来判断共识节点是否存活，以此来决定是否触发节点升级替换操作；根据候选节点在候选列表中的位置来决定升级替换优先级，只有当排在前面的候选节点失效的时候，后面的候选节点才可触发升级替换；

[0013] (5)候选节点断开现有网络连接：当通过心跳、故障检测等确定共识节点发生异常宕机以后，候选节点的自动升级替换操作被触发；这是候选节点进行升级替换的第一步；

[0014] (6)候选节点更新线上网络配置文件：候选节点读取备份的网络配置文件，更新线上网络配置信息，作为步骤(8)网络连接建立的基础；

[0015] (7)注册并启动共识服务：启动了共识服务以后，这个节点就拥有了共识投票的功能，但是还未与共识网络的其他节点建立连接；

[0016] (8)候选节点建立共识网络连接：候选节点更新自己的身份信息，根据最新网络配置信息向其他节点发起建立连接请求，这些节点包括原来与共识节点相连的其他共识节点和记账节点，连接建立过程同步骤(2)。

[0017] 进一步地，所述的步骤(1)中，我们根据证书的不同来确定节点拥有不同的权限，持有ECert表明节点有准入区块链网络的权限，持有RCert表明节点拥有参与共识投票的权限；共识节点持有ECert和RCert；记账节点持有ECert；候选节点持有ECert和RCert，但是RCert仅作为一个备份存在，在节点进行身份升级之前，它没有任何作用；另外，一个候选节点只能指定一个共识节点去获取相关网络连接信息；

[0018] 进一步地，所述的步骤(2)中，一个共识节点可以与多个它的候选节点建立连接。

[0019] 进一步地，所述的步骤(3)中，候选节点将接收到的网络配置信息持久化在备份网络配置文件中，不会影响候选节点目前线上自己的网路配置，只有当候选节点被触发去做升级替换的时候，线上的网络配置文件才会被备份的网络配置文件所替换，在节点完成升级替换以后，备份的网络配置文件才被删除。

[0020] 进一步地，所述的步骤(4)中，keepalive用来做候选节点与共识节点间的心跳检测，判断共识节点是否存活；超时机制主要用来判断当前命中的进行升级替换的候选节点是否失效，如果候选节点失效，候选列表也需要进行更新，将失效的候选节点从候选列表中移除。

[0021] 进一步的，所述的步骤(5)中，候选节点本质上是一个特殊的记账节点，它可能与一个或多个共识节点建立了连接，因此在做线上升级之前需要先断开其与其他共识节点的连接。

[0022] 进一步的，所述的步骤(8)中，由于建立连接的过程需要进行身份认证，因此候选节点在开始建立连接之前首先得更新自己的身份信息，这些身份信息需要与指定共识节点一一对应，在本系统中主要为hostname信息，保证节点升级替换后，节点唯一标识保持不

变,这样,对于共识网络的其他节点来说,就好像只是某个共识节点发生了短暂地断开,网络连接发生了替换而已。完成身份信息更新以后,候选节点根据最新网络配置向其他节点发起连接。

[0023] 本发明的有益效果是:本发明应用于联盟链背景下的区块链网络上,保证了在不影响区块链网络共识效率、不引入人工操作的前提下对机构内共识节点自动进行热备切换,避免了机构内共识节点发生单点故障。对于传统区块链,一方面,随着区块链的运行,区块链的数据量将越来越大,当共识节点发生致命故障导致数据丢失的时候,启动一个新节点同步全网数据所花费的时间是无法预估的,可能导致节点短时间内无法处理交易。另一方面,BFT类算法在节点数量达到一定数目时共识效率下降,显然通过增加共识节点的方式也不是解决节点单点故障的最佳方法。而我们提出的联盟链节点热备切换方法则解决了这一问题,使得共识节点故障恢复所消耗的时间只需秒级。

附图说明

[0024] 图1是节点建立连接程图;

[0025] 图2是共识节点连接状态图;

[0026] 图3是候选节点升级替换后连接状态图;

具体实施方式

[0027] 下面根据附图和具体实施例详细描述本发明,本发明的目的和效果将变得更加明显。

[0028] 一种联盟链节点热备切换的方法,包括如下步骤:

[0029] (1)候选节点网络配置:候选节点本质上是一个特殊的记账节点,持有线下第三方认证中心颁发的ECert和RCert证书;候选节点在启动之前,需要在其网络配置文件中指定它是哪个共识节点的候选节点;

[0030] (2)候选节点与共识节点建立连接:候选节点向共识节点发起建立连接请求,在物理连接建立完成以后,开始进行双方身份认证,若身份认证不通过,则连接建立失败;若身份认证通过,并且共识节点确认对端为其候选节点,则对其做Backup标记且放入候选列表中;

[0031] (3)候选节点对共识节点网络配置进行备份:在候选节点与共识节点的连接建立完成以后,共识节点每次网络连接信息发生变更,均会通知候选节点进行更新备份;备份的数据包括:区块链网络中的其他共识节点的地址连接信息、与共识节点相连的记账节点的地址连接信息、共识节点的候选列表。其中,记账节点包括候选节点,因为候选节点是特殊的记账节点;

[0032] (4)候选节点对共识节点进行故障检测:候选节点采用keepalive+超时的机制来判断共识节点是否存活,以此来决定是否触发节点升级替换操作;根据候选节点在候选列表中的位置来决定升级替换优先级,只有当排在前面的候选节点失效的时候,后面的候选节点才可触发升级替换;

[0033] (5)候选节点断开现有网络连接:当通过心跳、故障检测等确定共识节点发生异常宕机以后,候选节点的自动升级替换操作被触发;这是候选节点进行升级替换的第一步;

[0034] (6)候选节点更新线上网络配置文件:候选节点读取备份的网络配置文件,更新线上网络配置信息,作为步骤(8)网络连接建立的基础;

[0035] (7)注册并启动共识服务:启动了共识服务以后,这个节点就拥有了共识投票的功能,但是还未与共识网络的其他节点建立连接;

[0036] (8)候选节点建立共识网络连接:候选节点更新自己的身份信息,根据最新网络配置信息向其他节点发起建立连接请求,这些节点包括原来与共识节点相连的其他共识节点和记账节点,连接建立过程同步骤(2)。

[0037] 进一步地,所述的步骤(1)中,我们根据证书的不同来确定节点拥有不同的权限,持有ECert表明节点有准入区块链网络的权限,持有RCert表明节点拥有参与共识投票的权限;共识节点持有ECert和RCert;记账节点持有ECert;候选节点持有ECert和RCert,但是RCert仅作为一个备份存在,在节点进行身份升级之前,它没有任何作用;另外,一个候选节点只能指定一个共识节点去获取相关网络连接信息;

[0038] 进一步地,所述的步骤(2)中,一个共识节点可以与多个它的候选节点建立连接。由图1可知,对于请求建立连接的节点1来说,首先,向节点2发起建立连接的请求,节点2响应连接请求后,节点1与节点2就建立起了传输层加密连接,可以开始进一步身份认证以及密钥协商。节点1将自己的ECert、RCert以及是否为CVP等身份认证信息发送给节点2。节点2接收到消息后,首先,验证节点1的ECert,若ECert验证失败,则断开连接;若ECert验证通过并且身份认证信息中有RCert,说明对端节点是一个VP节点,验证RCert证书合法性,如果验证失败则断开连接,如果验证通过则两个节点生成一对共享密钥,可以开始进行安全加密通信;若ECert验证通过并且身份认证信息中没有RCert,则说明对端节点是一个NVP节点,如果它是一个CVP,则对其做标记并且有序放到候选列表中,同样生成一对共享密钥,可以开始进行安全加密通信。

[0039] 进一步的,所述的步骤(3)中,CVP将接收到的网络配置信息持久化在备份网络配置文件中,不会影响CVP目前线上自己的网路配置,只有当CVP被触发去做升级替换的时候,线上的网络配置文件才会被备份的网络配置文件所替换,在节点完成升级替换以后,备份的网络配置文件才被删除。

[0040] 进一步的,所述的步骤(4)中,keepalive用来做候选节点与共识节点间的心跳检测,判断共识节点是否存活;超时机制主要用来判断当前命中的进行升级替换的候选节点是否失效,如果候选节点失效,候选列表也需要进行更新,将失效的候选节点从候选列表中移除。

[0041] 可能出现多种故障情况,我们以图2为例来说明各个故障情况下系统的处理方式。由图可知该VP0目前与两个普通NVP以及两个CVP相连,VP0维护的候选列表中按序存放着CVP-1和CVP-2的信息,候选列表的先后顺序决定着VP0异常停机的时候由谁来触发升级。

[0042] 场景一:VP0异常宕机

[0043] VP0异常宕机后,它与NVP-1、NVP-2、CVP-1和CVP-2的连接均断开。此时,从候选列表可知,CVP-1在发现VP0心跳丢失超过一定时间后,马上进行升级替换。虽然CVP-2在心跳检测的过程中也发现了VP0的异常,但是由于自己不是候选列表首位,因此不会触发升级,而是等待CVP-1完成升级替换,后文将讨论VP0和CVP-1同时异常宕机的情况。

[0044] 场景二:CVP-1异常宕机

[0045] 这个场景下VP0依旧是正常工作的,所以不会发生升级替换的过程。然而此时,由于CVP-1已经停机,VP0候选列表的首位已经失效,此时如果依旧保持着失效的信息对于VP0来说是非常不利的。因此,VP0发现CVP-1停机以后,将CVP-1从候选列表中删除,同时将最新网络连接信息发送给其他CVP。

[0046] 场景三:VP0和CVP-1同时宕机

[0047] 由于VP0与首位候选节点CVP-1都出现了停机,因此,需要其他CVP来升级替换VP0。我们为系统提供一个可配置的超时时间,使得非首位的候选节点在超时时间内都检测不到新验证节点的存在时,则认为节点升级替换过程发生超时,需要下一位候选节点去做升级替换,被命中的候选节点在做升级替换之前,更新自己的候选列表,删除已知失效的候选节点信息。

[0048] 这三个场景下,候选节点升级替换后的网络连接状态如图3所示。

[0049] 进一步的,所述的步骤5)中,CVP本质上是一个NVP,它可能与多个VP建立了连接,因此在做线上升级之前需要先断开其与其他VP节点的连接。

[0050] 进一步的,所述的步骤8)中,由于建立连接的过程需要进行身份认证,因此CVP在开始建立连接之前首先得更新自己的身份信息,这些身份信息需要与VP0一一对应,在本系统中主要为hostname信息,保证节点升级替换后,节点唯一标识保持不变,这样,对于共识网络的其他节点来说,就好像只是VP0发生了短暂地断开,网络连接发生了替换而已。完成身份信息更新以后,CVP根据最新网络配置向其他节点发起连接。

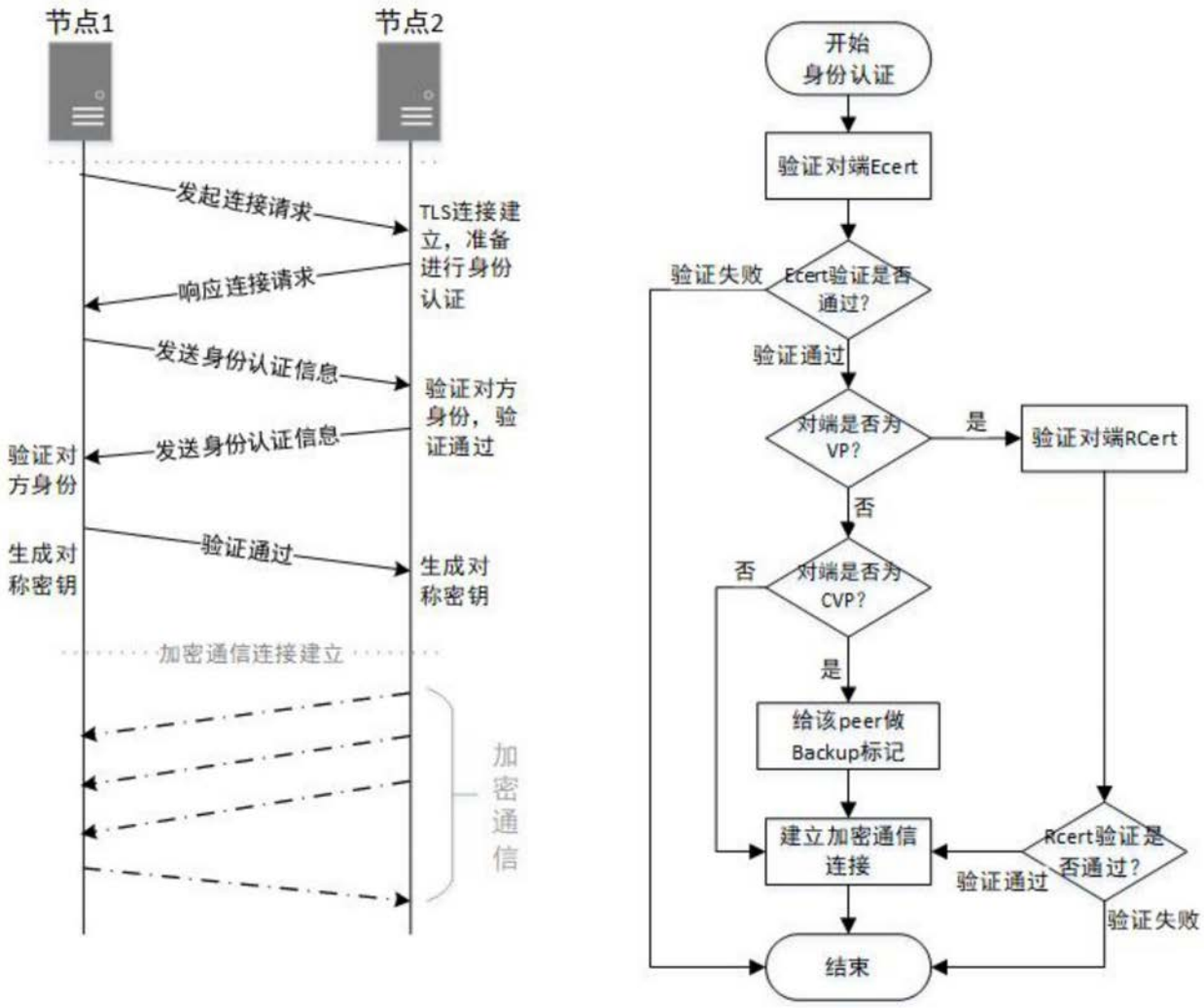

节点1
节点2
发起连接请求
TLS连接建立，准备进行身份认证
响应连接请求
发送身份认证信息
验证对方身份，验证通过
发送身份认证信息
验证对方身份
生成对称密钥
验证通过
生成对称密钥
加密通信连接建立
加密通信
开始
身份认证
验证对端Ecert
验证失败
Ecert验证是否通过?
验证通过
对端是否为VP?
是
验证对端RCert
否
否
对端是否为CVP?
是
给该peer做Backup标记
建立加密通信连接
Rcert验证是否通过?
验证通过
验证失败
结束

图1

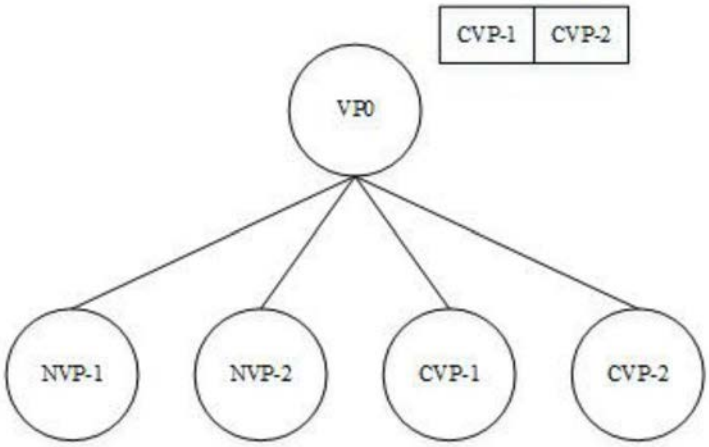

CVP-1
CVP-2
VP0
NVP-1
NVP-2
CVP-1
CVP-2

图2

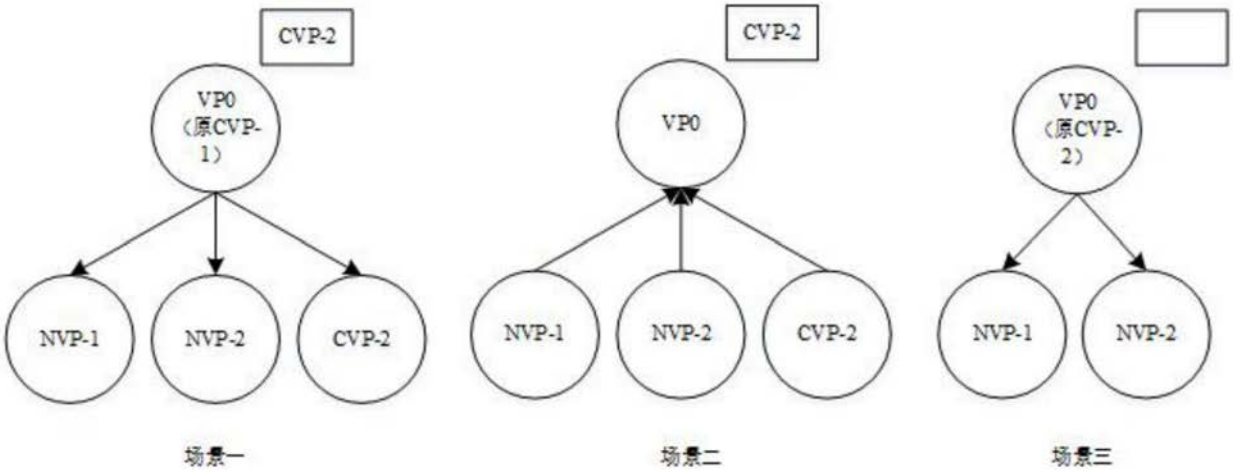

CVP-2
VP0
（原CVP-
1）
NVP-1
NVP-2
CVP-2
场景一
CVP-2
VP0
NVP-1
NVP-2
CVP-2
场景二
VP0
（原CVP-
2）
NVP-1
NVP-2
场景三

图3