(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 103746817 B
(45)授权公告日 2018.01.09

(21)申请号 201410055563.0

(22)申请日 2014.02.18

(65)同一申请的已公布的文献号
申请公布号 CN 103746817 A

(43)申请公布日 2014.04.23

(73)专利权人 互联网域名系统北京市工程研究中心有限公司
地址 101408 北京市怀柔区雁栖经济开发区杨雁路88号一层D9
专利权人 北龙中网(北京)科技有限责任公司

(72)发明人 刘硕

(74)专利代理机构 北京万慧达知识产权代理有限公司 11111
代理人 张金芝 杨颖

(51)Int.Cl.
H04L 9/32(2006.01)
H04L 9/08(2006.01)
H04L 29/12(2006.01)

(56)对比文件
CN 103314566 A,2013.09.18,
US 2012017090 A1,2012.01.19,
CN 101336535 A,2008.12.31,
CN 102769529 A,2012.11.07,
Joe Gersch, Dan Massey.Deploying DNS Security(DNSSEC) in Large-Scale Operational Environments.《cybersecurity applications & conference for homeland security》.2009,169-180.

审查员 从文

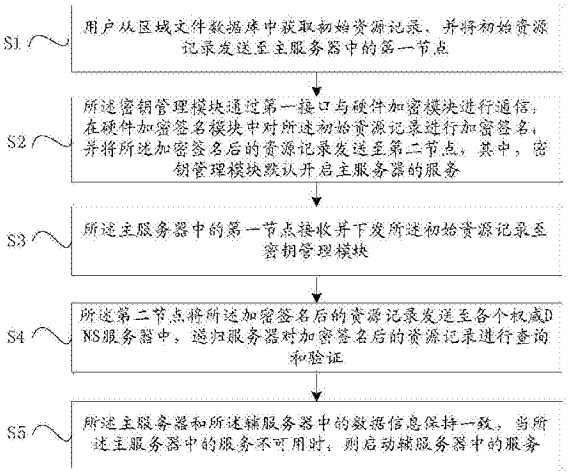
权利要求书2页 说明书6页 附图2页

(54)发明名称

DNSSEC签名方法及其系统

(57)摘要

本发明提供一种DNSSEC签名方法及其系统，用户从区域文件数据库中获取初始资源记录，并将初始资源记录发送至主服务器中的第一节点；主服务器中的第一节点接收并下发初始资源记录至密钥管理模块；密钥管理模块通过第一接口与硬件加密签名模块进行通信，在硬件加密模块中对初始资源记录进行加密签名，并将加密签名后的资源记录发送至第二节点；第二节点将加密签名后的资源记录发送至各个权威DNS服务器中，递归服务器对加密签名后的资源记录进行查询和验证；主服务器和辅服务器中的数据信息保持一致，当主服务器中的服务不可用时，则启动辅服务器中的服务，并通过动态监控和主辅服务器的智能切换来保证DNSSEC数据的连续性和完整性。



CN 103746817 B

1.一种DNSSEC签名方法，其特征在于，采用主服务器和辅服务器，所述主服务器中包括：第一节点、密钥管理模块和第二节点；所述辅服务器中包括：第一节点、密钥管理模块和第二节点，包括：

用户从区域文件数据库中获取初始资源记录，并将初始资源记录发送至主服务器中的第一节点；

所述主服务器中的第一节点接收并下发所述初始资源记录至密钥管理模块；

所述密钥管理模块通过第一接口与硬件加密签名模块进行通信，在硬件加密签名模块中对所述初始资源记录进行加密签名，并将所述加密签名后的资源记录发送至第二节点，其中，密钥管理模块默认开启主服务器的服务；

所述第二节点将所述加密签名后的资源记录发送至各个权威DNS服务器中，递归服务器对加密签名后的资源记录进行查询和验证；

所述主服务器和所述辅服务器中的数据信息保持一致，当所述主服务器中的服务不可用时，则启动辅服务器中的服务；

所述主服务器的第二节点从属于所述主服务器的第一节点，所述辅服务器的第二节点从属于所述辅服务器的第一节点；

所述主服务器和所述辅服务器中的第二节点同时作为下一级的第一节点，默认下一级节点首先去请求主服务器中的第二节点，当主服务器的服务不可用时，则从辅服务器中的第二节点获取资源记录。

2.根据权利要求1所述的DNSSEC签名方法，其特征在于，还包括：

当所述主服务器中的密钥管理模块的文件发生变化时，通过定时同步程序将所述变化实时同步至所述辅服务器中的密钥管理模块中，以使所述主服务器中的密钥管理模块与所述辅服务器中的密钥管理模块中的数据信息相同。

3.根据权利要求2所述的DNSSEC签名方法，其特征在于，所述主服务器中的第一节点和所述辅服务器中的第一节点所使用的初始资源记录和序列值相同，且资源记录的更新和序列值的增加保持一致。

4.根据权利要求3所述的DNSSEC签名方法，其特征在于，所述主服务器和所述辅服务器的数据信息保持一致，包括：

所述主服务器中的第一节点的数据信息和所述辅服务器中的第一节点的数据信息一致；所述主服务器中的密钥管理模块的数据信息和所述辅服务器中的密钥管理模块的数据信息一致。

5.根据权利要求4所述的DNSSEC签名方法，其特征在于，当所述主服务器中的服务不可用时，则启动辅服务器中的服务包括：

当所述主服务器中的第一节点、密钥管理模块和第二节点的服务不可用时，所述辅服务器的密钥管理实时收到所述辅服务器的第一节点的初始资源记录，通过第一接口与硬件加密签名模块进行通信，在硬件加密签名模块中对所述初始资源记录进行加密签名，并将所述加密签名后的资源记录发送至第二节点。

6.根据权利要求1所述的DNSSEC签名方法，其特征在于，当辅服务器中的密钥管理模块关闭的状态下，辅服务器中的第二节点的序列值小于主服务器中的第二节点的序列值。

7.一种DNSSEC签名系统，包括主服务器、辅服务器、硬件加密签名模块，所述主服务器

中包括：第一节点、密钥管理模块和第二节点；所述辅服务器中包括：第一节点、密钥管理模块和第二节点，包括：

用户从区域文件数据库中获取初始资源记录，并将初始资源记录发送至主服务器中的第一节点；

所述主服务器中的第一节点接收并下发所述初始资源记录至密钥管理模块；

所述密钥管理模块通过第一接口与硬件加密签名模块进行通信，在硬件加密签名模块中对所述初始资源记录进行加密签名，并将所述加密签名后的资源记录发送至第二节点，其中，密钥管理模块默认开启主服务器的服务；

所述第二节点将所述加密签名后的资源记录发送至各个权威DNS服务器中，递归服务器对加密签名后的资源记录进行查询和验证；

所述主服务器和所述辅服务器中的数据信息保持一致，当所述主服务器中的服务不可用时，则启动辅服务器中的服务；

所述主服务器和所述辅服务器中的第二节点同时作为下一级的第一节点，默认下一级节点首先去请求主服务器中的第二节点，当主服务器的服务不可用时，则从辅服务器中的第二节点获取资源记录。

8.根据权利要求7所述的DNSSEC签名系统，其特征在于，还包括：

定时同步模块，用于当所述主服务器中的密钥管理模块的文件发生变化时，通过定时同步程序将所述变化实时同步至所述辅服务器中的密钥管理模块中，以使所述主服务器中的密钥管理模块与所述辅服务器中的密钥管理模块中的数据信息相同。

9.根据权利要求8所述的DNSSEC签名系统，其特征在于，还包括：

实时监控模块，用于实时监控主服务器中的第一节点、密钥管理模块和第二节点，

当所述主服务器中的服务不可用时，则启动辅服务器中的服务包括：

当所述主服务器中的第一节点、密钥管理模块和第二节点的服务不可用时，所述辅服务器的密钥管理实时收到所述辅服务器的第一节点的初始资源记录，通过第一接口与硬件加密签名模块进行通信，在硬件加密签名模块中对所述初始资源记录进行加密签名，并将所述加密签名后的资源记录发送至第二节点。

DNSSEC签名方法及其系统

技术领域

[0001] 本发明属于计算机技术领域，具体涉及一种DNSSEC签名方法及其系统。

背景技术

[0002] 域名系统(Domain Name System，简称DNS)，与互联网的其他协议或系统一样，在一个可信的、纯净的环境里运行得很好。但由于互联网环境异常复杂，充斥着各种欺诈、攻击，DNS协议的脆弱性也就浮出水面。对DNS的攻击可能导致互联网大面积的瘫痪，DNS的最大缺陷是解析的请求者无法验证它所收到的应答信息的真实性。

[0003] 域名系统的安全协议(DNS Security Extensions，简称DNSSEC)给解析服务器提供了防止上当受骗的武器，即一种可以验证应答信息真实性和完整性的机制。现有DNS服务普遍缺少DNSSEC功能，国内普及度更是极低，只能通过软件方式在测试床进行试验，达到生产环境运行标准的高性能DNSSEC服务目前还没有。

发明内容

[0004] 本发明提供一种DNSSEC签名方法及其系统，其可以解决生产环境中DNSSEC硬件冗余部署的问题，通过动态监控和主辅服务器的智能切换来保证DNSSEC数据的连续性和完整性。

[0005] 为实现上述目的，本发明提供一种DNSSEC签名方法，采用主服务器和辅服务器，所述主服务器中包括：第一节点、密钥管理模块和第二节点；所述辅服务器中包括：第一节点、密钥管理模块和第二节点，包括：

[0006] 用户从区域文件数据库中获取初始资源记录，并将初始资源记录发送至主服务器中的第一节点；

[0007] 所述主服务器中的第一节点接收并下发所述初始资源记录至密钥管理模块；

[0008] 所述密钥管理模块通过第一接口与硬件加密签名模块进行通信，在硬件加密签名模块中对所述初始资源记录进行加密签名，并将所述加密签名后的资源记录发送至第二节点，其中，密钥管理模块默认开启主服务器的服务；

[0009] 所述第二节点将所述加密签名后的资源记录发送至各个权威DNS服务器中，递归服务器对加密签名后的资源记录进行查询和验证；

[0010] 所述主服务器和所述辅服务器中的数据信息保持一致，当所述主服务器中的服务不可用时，则启动辅服务器中的服务。

[0011] 进一步地，该方法还包括：

[0012] 当所述主服务器中的密钥管理模块的文件发生变化时，通过定时同步程序将所述变化实时同步至所述辅服务器中的密钥管理模块中，以使所述主服务器中的密钥管理模块与所述辅服务器中的密钥管理模块中的数据信息相同。

[0013] 进一步地，所述主服务器中的第一节点和所述辅服务器中的第一节点所使用的初始资源记录和序列值相同，且资源记录的更新和序列值的增加保持一致。

[0014] 进一步地，所述主服务器和所述辅服务器的数据信息保持一致，包括：

[0015] 所述主服务器中的第一节点的数据信息和所述辅服务器中的第一节点的数据信息一致；所述主服务器中的密钥管理模块的数据信息和所述辅服务器中的密钥管理模块的数据信息一致。

[0016] 进一步地，当所述主服务器中的服务不可用时，则启动辅服务器中的服务包括：

[0017] 当所述主服务器中的第一节点、密钥管理模块和第二节点的服务不可用时，所述辅服务器的密钥管理实时收到所述辅服务器的第一节点的初始资源记录，通过第一接口与硬件加密签名模块进行通信，在硬件加密签名模块中对所述初始资源记录进行加密签名，并将所述加密签名后的资源记录发送至第二节点。

[0018] 进一步地，所述主服务器和所述辅服务器中的第二节点同时作为下一级的第一节点，默认下一级节点首先去请求主服务器中的第二节点，当主服务器的服务不可用时，则从辅服务器中的第二节点获取资源记录。

[0019] 进一步地，当辅服务器中的密钥管理模块关闭的状态下，辅服务器中的第二节点的序列值小于主服务器中的第二节点的序列值。

[0020] 为实现上述目的，本发明提供一种DNSSEC签名系统，包括主服务器、辅服务器、硬件加密签名模块，所述主服务器中包括：第一节点、密钥管理模块和第二节点；所述辅服务器中包括：第一节点、密钥管理模块和第二节点，包括：

[0021] 用户从区域文件数据库中获取初始资源记录，并将初始资源记录发送至主服务器中的第一节点；

[0022] 所述主服务器中的第一节点接收并下发所述初始资源记录至密钥管理模块；

[0023] 所述密钥管理模块通过第一接口与硬件加密签名模块进行通信，在硬件加密签名模块中对所述初始资源记录进行加密签名，并将所述加密签名后的资源记录发送至第二节点，其中，密钥管理模块默认开启主服务器的服务；

[0024] 所述第二节点将所述加密签名后的资源记录发送至各个权威DNS服务器中，递归服务器对加密签名后的资源记录进行查询和验证；

[0025] 所述主服务器和所述辅服务器中的数据信息保持一致，当所述主服务器中的服务不可用时，则启动辅服务器中的服务。

[0026] 进一步地，还包括：

[0027] 定时同步模块，用于当所述主服务器中的密钥管理模块的文件发生变化时，通过定时同步程序将所述变化实时同步至所述辅服务器中的密钥管理模块中，以使所述主服务器中的密钥管理模块与所述辅服务器中的密钥管理模块中的数据信息相同。

[0028] 进一步地，还包括：

[0029] 实时监控模块，用于实时监控主服务器中的第一节点、密钥管理模块和第二节点，

[0030] 当所述主服务器中的服务不可用时，则启动辅服务器中的服务包括：

[0031] 当所述主服务器中的第一节点、密钥管理模块和第二节点的服务不可用时，所述辅服务器的密钥管理实时收到所述辅服务器的第一节点的初始资源记录，通过第一接口与硬件加密签名模块进行通信，在硬件加密签名模块中对所述初始资源记录进行加密签名，并将所述加密签名后的资源记录发送至第二节点。

[0032] 本发明提供的DNSSEC签名方法及其系统中，通过采用硬件加密签名模块

(Hardware Security Module,简称HSM)与pkcs#11接口来保证数据加密过程中的机密性、密钥的不可导出性,有效的防止了密钥的泄露。本发明的技术方案解决了生产环境中DNSSEC硬件冗余部署的问题,通过动态监控和主辅服务器的智能切换来保证DNSSEC数据的连续性和完整性。

附图说明

[0033] 图1为本发明实施例一提供的DNSSEC签名方法的流程示意图;

[0034] 图2为本发明实施例二提供的DNSSEC签名系统的结构示意图;

[0035] 图3为DNSSEC签名系统的应用示意图。

具体实施方式

[0036] 为使本领域技术人员更好地理解本发明的技术方案,下面结合附图和具体实施方式对本发明作进一步详细描述。

[0037] 图1为本发明实施例一提供的DNSSEC签名方法的流程示意图,如图1所示,该DNSSEC签名方法采用主服务器和辅服务器,所述主服务器中包括:第一节点、密钥管理模块和第二节点;所述辅服务器中包括:第一节点、密钥管理模块和第二节点;该方法包括:

[0038] 步骤S1、用户从区域文件数据库中获取初始资源记录,并将初始资源记录发送至主服务器中的第一节点。

[0039] 具体地,用户从区文件数据库中获取资源记录,资源记录以初始资源记录的形式存在于第一节点(master)中。

[0040] 主服务器中的用户和辅服务器中的用户保证两个第一节点中的资源记录最新并且一致,首先保证两个第一节点使用的原始区的区文件内容和序列值完全相同,主服务器和辅服务器中的两个用户通过区文件数据库中新增的资源记录按顺序更新对应的主服务器和辅服务器中的第一节点的数据。

[0041] 由于第一节点采用nsupdate更新机制,nsupdate是一个动态的DNS更新工具,其可以向DNS服务器提交更新资源记录的请求,它可以从区文件中添加或删除资源记录,而不需要手动进行编辑区文件,从而保证了主服务器和辅服务器两边的更新数据量和序列值的增加规律是一致的。

[0042] 如果任何一个第一节点服务不可用时,对应的用户将无法更新,直到第一节点恢复正常,如果更新记录失败,通过用户的事务保证机制,用户继续尝试更新,从而保证了区数据不会丢失。

[0043] 步骤S2、所述主服务器中的第一节点接收并下发所述初始资源记录至密钥管理模块。

[0044] 具体地,主服务器中的第一节点接收到新的资源记录后会通过增量区域传输(Incremental Zone Transfer,简称IXFR)机制及时下发给密钥管理模块。密钥管理模块负责维护各个区域的密钥的生命周期管理,包括密钥的轮转和区参数的配置。密钥管理模块执行接收和下发数据对的通信采用IXFR机制,可以实时对新的数据进行“接收-签名-下发”的操作,能够提高对大区数据的处理的效率。

[0045] 步骤S3、所述密钥管理模块通过第一接口与硬件加密签名模块进行通信,在硬件

加密签名模块中对所述初始资源记录进行加密签名，并将所述加密签名后的资源记录发送至第二节点，其中，密钥管理模块默认开启主服务器的服务。

[0046] 具体地，密钥管理模块(opendnssec)通过第一接口(pkcs#11)与硬件加密签名模块(Hardware Security Module，简称HSM)进行通信，HSM对初始资源记录进行签名、创建和保存密钥，提高了密钥的安全性，将签名工作与软件服务器解耦，使得软件服务器可以专注于通信和管理等工作，大大缓解对中央处理器的依赖。

[0047] 密钥管理模块在对区文件和密钥进行管理时需要与HSM加密机进行通信，通过pkcs#11接口在HSM中创建密钥，并通过调用相应的pkcs#11的签名接口将资源记录传给HSM进行签名，然后将签名后到资源记录进行一定规律的拼装再通过IXFR机制下发给第二节点(slave)。

[0048] 密钥管理模块默认只开启主服务器上的服务，辅服务器上的服务并不开启。通过定时同步程序保证辅服务器上的服务和主服务器上的密钥管理模块的配置文件和其他管理文件的高度一致，一旦主服务器上的对应文件有变动，则实时同步到辅服务器的相应文件。

[0049] 通过监控程序实时监控主服务器上的第一节点、opendnssec服务、第二节点的服务可用性，如果上述服务器中的三个服务均不可用，如端口不可达，dig返回异常结果，则自动启动辅服务器中的opendnssec服务，由于两台服务器中的opendnssc服务中的数据完全相同，即区信息相同，对应的密钥相同则保证了dnssec服务的连续行。

[0050] 步骤S4、所述第二节点将所述加密签名后的资源记录发送至各个权威DNS服务器中，递归服务器对加密签名后的资源记录进行查询和验证。

[0051] 步骤S5、所述主服务器和所述辅服务器中的数据信息保持一致，当所述主服务器中的服务不可用时，则启动辅服务器中的服务。

[0052] 具体地，辅助服务器上的opendnssec服务实时收到辅助服务器中的第一节点的资源记录数据，调用hsm接口进行签名，最后再发送给辅助服务器上的第二节点。主辅服务器中的第二节点同时作为下一级第二节点的第一节点，但是默认下一级别的第二节点首先去请求主服务器中的第二节点，只有当主服务器不可用时，才会尝试去辅服务器中的第二节点获取区数据，平时辅助服务器上的第二节点不会收到请求，这样就不会造成区数据的不同导致下发出现问题。

[0053] 由于序列值的原因，平时辅助服务器上的第二节点接收不到opendnssec的下发数据，因为它没有开启，所以它的序列值小于主服务器中的第二节点，理论上下一级别的第二节点只会去请求比它的序列值更大的第一节点的数据。当辅助服务器的opendnssec开启后，它对区数据的签名和下发规则完全和主服务器中的opendnssc相同，包括序列值的变化规律，所以当第一节点下发record纪录到主服务器宕机时刻的时候，两边的opendnssc下发的数据的序列值达到了相同的值，从此以后如果第一节点继续下发数据给opendnssec，那么序列值将会超过以前曾经达到的最大序列值，从这一个序列值以后，第二节点的下一级别的第二节点将会对比自己的序列值小于当前所请求的辅服务器中第二节点的序列值，所以会继续请求新的资源记录数据，进而DNS数据下发的连续性便得到了保证。

[0054] 本实施例提供的DNSSEC签名方法中，通过采用硬件加密签名模块与pkcs#11接口来保证数据加密过程中的机密性、密钥的不可导出性，有效的防止了密钥的泄露，解决了生

产环境中DNSSEC硬件冗余部署的问题，通过动态监控和主辅服务器的智能切换来保证DNSSEC数据的连续性和完整性。

[0055] 图2为本发明实施例二提供的DNSSEC签名系统的结构示意图，如图2所示，该DNSSEC签名系统包括：主服务器201、辅服务器202、硬件加密签名模块203、定时同步单元204和实时监控单元205。其中，主服务器201包括：第一节点2011、密钥管理模块2012和第二节点2013；辅服务器202包括：第一节点2021、密钥管理模块2022和第二节点2023。

[0056] 具体地，用户从区域文件数据库中获取初始资源记录，并将初始资源记录发送至主服务器201中的第一节点2011；主服务器中201的第一节点2011接收并下发初始资源记录至密钥管理模块2012；密钥管理模块2012通过第一接口与硬件加密签名模块203进行通信，在硬件加密签名模块203中对初始资源记录进行加密签名，并将加密签名后的资源记录发送至第二节点2013，其中，密钥管理模块2012默认开启主服务器201的服务；第二节点2013将加密签名后的资源记录发送至各个权威DNS服务器中，递归服务器对加密签名后的资源记录进行查询和验证；主服务器201和辅服务器202中的数据信息保持一致，当主服务器201中的服务不可用时，则启动辅服务器202中的服务。

[0057] 优选地，该DNSSEC签名系统还包括：定时同步模块204，用于当主服务器201中的密钥管理模块2012的文件发生变化时，通过定时同步模块204将变化实时同步至辅服务器202中的密钥管理模块2022中，以使主服务器201中的密钥管理模块2012与辅服务器202中的密钥管理模块2022中的数据信息相同。

[0058] 进一步地，该DNSSEC签名系统还包括：实时监控模块205，用于实时监控主服务器201中的第一节点2011、密钥管理模块2012和第二节点2013，当主服务器201中的服务不可用时，则启动辅服务器202中的服务包括：当主服务器201中的第一节点2011、密钥管理模块2012和第二节点2013的服务不可用时，辅服务器202的密钥管理模块2022实时收到辅服务器202的第一节点2021的初始资源记录，通过第一接口与硬件加密签名模块202进行通信，在硬件加密签名模块202中对初始资源记录进行加密签名，并将加密签名后的资源记录发送至第二节点2023。

[0059] 本实施例提供的DNSSEC签名系统中，通过采用硬件加密签名模块与pkcs#11接口来保证数据加密过程中的机密性、密钥的不可导出性，有效的防止了密钥的泄露。通过部署两套系统解决单点问题，从而解决了生产环境中DNSSEC硬件冗余部署的问题，通过动态监控和主辅服务器的智能切换来保证DNSSEC数据的连续性和完整性。

[0060] 图3为DNSSEC签名系统的应用示意图，如图3所示，该DNSSEC签名系统中，通过部署两套系统来解决单点的问题。通过两个consumer保证两个master中的record纪录保持最新并且一致。首先保证两个master使用的原始区的区文件内容和serial值完全相同，然后两边的consumer服务通过epp库中新增的record纪录按顺序更新对应的master节点的数据，由于master采用bind的nsupdate机制，保证了两边的更新数据量和serial的增加的规律是一致的。如果任何一个master服务不可用，对应的consumer将无法更新，直到master节点恢复正常，但由于consumer的事务保证机制，如果更新record失败，则会回滚，继续尝试更新，所以不存在丢失区数据的情况。

[0061] Opendnssc默认只开启主服务器上的服务，辅服务器上的服务并不开启，但通过定时同步程序保证辅服务器上的opendnssec服务和主服务器上的opendnssec的配置文件和

其他管理文件的高度一致，一旦主服务器上的对应文件有变动，则实时同步到辅服务器的相应文件。通过监控程序实时监控主服务器上的master节点、opendnssec服务、slave节点的服务可用性，如果上述服务器中的三个服务均不可用，如端口不可达，dig返回异常结果，则自动启动辅服务器中的opendnssec服务，由于两台服务器中的opendnssc服务中的数据完全相同，即区信息相同，对应的key相同则保证了dnssec服务的连续行。

[0062] 辅助服务器上的opendnssec服务实时收到辅助服务器中的master节点的record数据，调用HSM设备提供的pkcs#11接口进行签名，最后再发送给辅助服务器上的slave阶段。主辅服务器中的slave节点同时作为下一级slave节点的master节点，但是默认下一级别的slave节点首先去请求主服务器中的slave节点，只有当主服务器不可用时，才会尝试去辅服务器中的slave节点获取区数据，平时辅助服务器上的salve节点不会收到请求，这样就不会造成区数据的不同导致下发出现问题。由于serial值的原因，平时辅助服务器上的slave节点接收不到opendnssec的下发数据，因为它没有开启，所以它的serial值小于主服务器中的slave节点，理论上下一级别的slave节点只会去请求比它的serial值更大的master节点的数据。

[0063] 当辅助服务器的opendnssec开启后，它对区数据的签名和下发规则完全和主服务器中的opendnssc相同，包括serial值的变化规律，所以当master节点下发record纪录到主服务器宕机时刻的时候，两边的opendnssc下发的数据的serial值达到了相同的值，从此以后如果master继续下发数据给opendnssec，那么serial值将会超过以前曾经达到的最大serial值，从这一个serial值以后，slave节点的下一级别的slave节点将会对比自己的serial值小于当前所请求的辅服务器中slave节点的serial值，所以会继续请求新的record数据，进而dns数据下发的连续性便得到了保证。

[0064] 本实施例提供的DNSSEC签名系统中，采用主服务器和服务器，保证DNS数据从签名到下发的完整性和可靠性。通过采用硬件加密签名模块与pkcs#11接口来保证数据加密过程中的机密性、密钥的不可导出性，有效的防止了密钥的泄露。本发明的技术方案解决了生产环境中DNSSEC硬件冗余部署的问题，通过动态监控和主辅服务器的智能切换来保证DNSSEC数据的连续性和完整性。

[0065] 可以理解的是，以上实施方式仅仅是为了说明本发明的原理而采用的示例性实施方式，然而本发明并不局限于此。对于本领域内的普通技术人员而言，在不脱离本发明的精神和实质的情况下，可以做出各种变型和改进，这些变型和改进也视为本发明的保护范围。

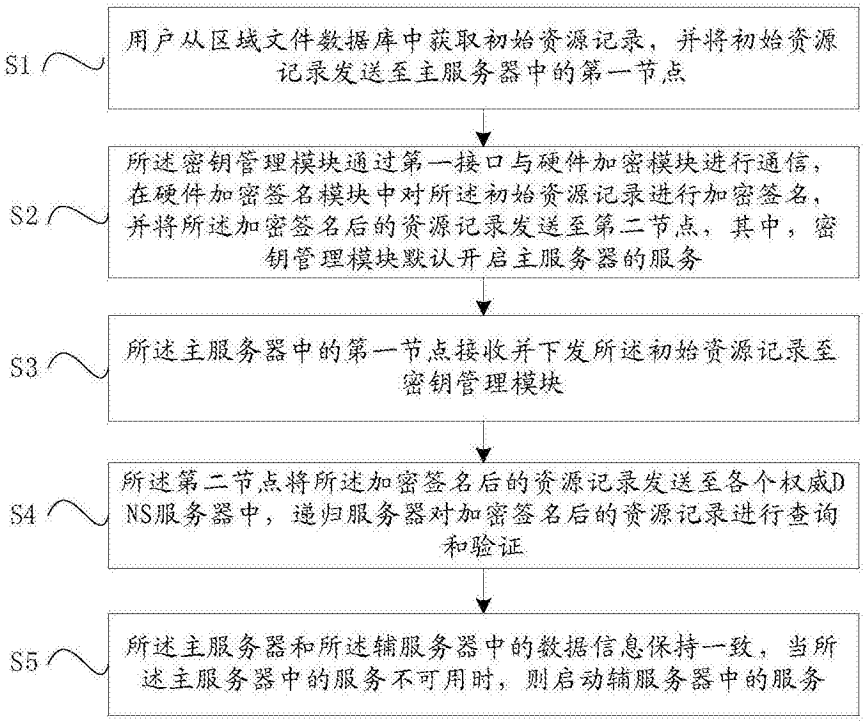

S1
用户从区域文件数据库中获取初始资源记录，并将初始资源记录发送至主服务器中的第一节点
S2
所述密钥管理模块通过第一接口与硬件加密模块进行通信，在硬件加密签名模块中对所述初始资源记录进行加密签名，并将所述加密签名后的资源记录发送至第二节点，其中，密钥管理模块默认开启主服务器的服务
S3
所述主服务器中的第一节点接收并下发所述初始资源记录至密钥管理模块
S4
所述第二节点将所述加密签名后的资源记录发送至各个权威DNS服务器中，递归服务器对加密签名后的资源记录进行查询和验证
S5
所述主服务器和所述辅服务器中的数据信息保持一致，当所述主服务器中的服务不可用时，则启动辅服务器中的服务

图1

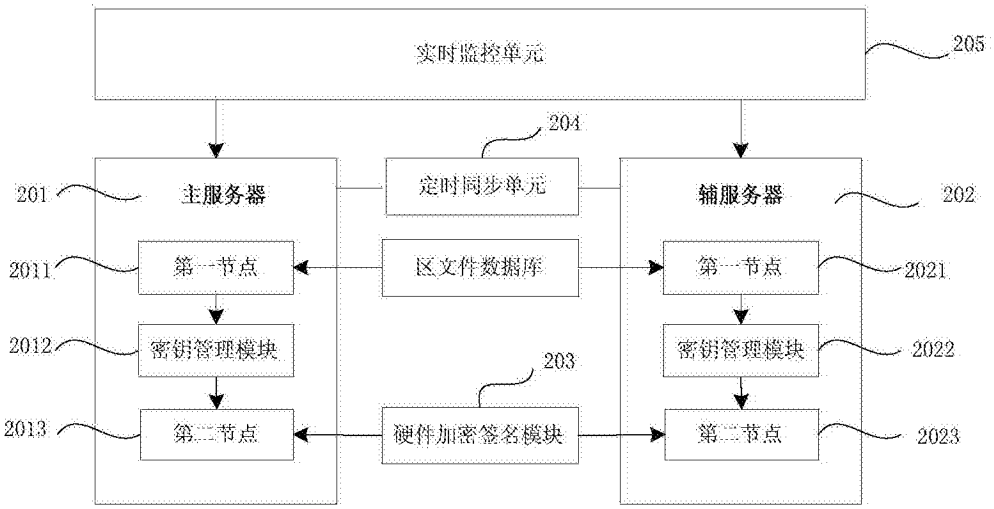

实时监控单元
205
204
201
主服务器
定时同步单元
辅服务器
202
2011
第一节点
区文件数据库
第一节点
2021
2012
密钥管理模块
密钥管理模块
2022
203
2013
第二节点
硬件加密签名模块
第二节点
2023

图2

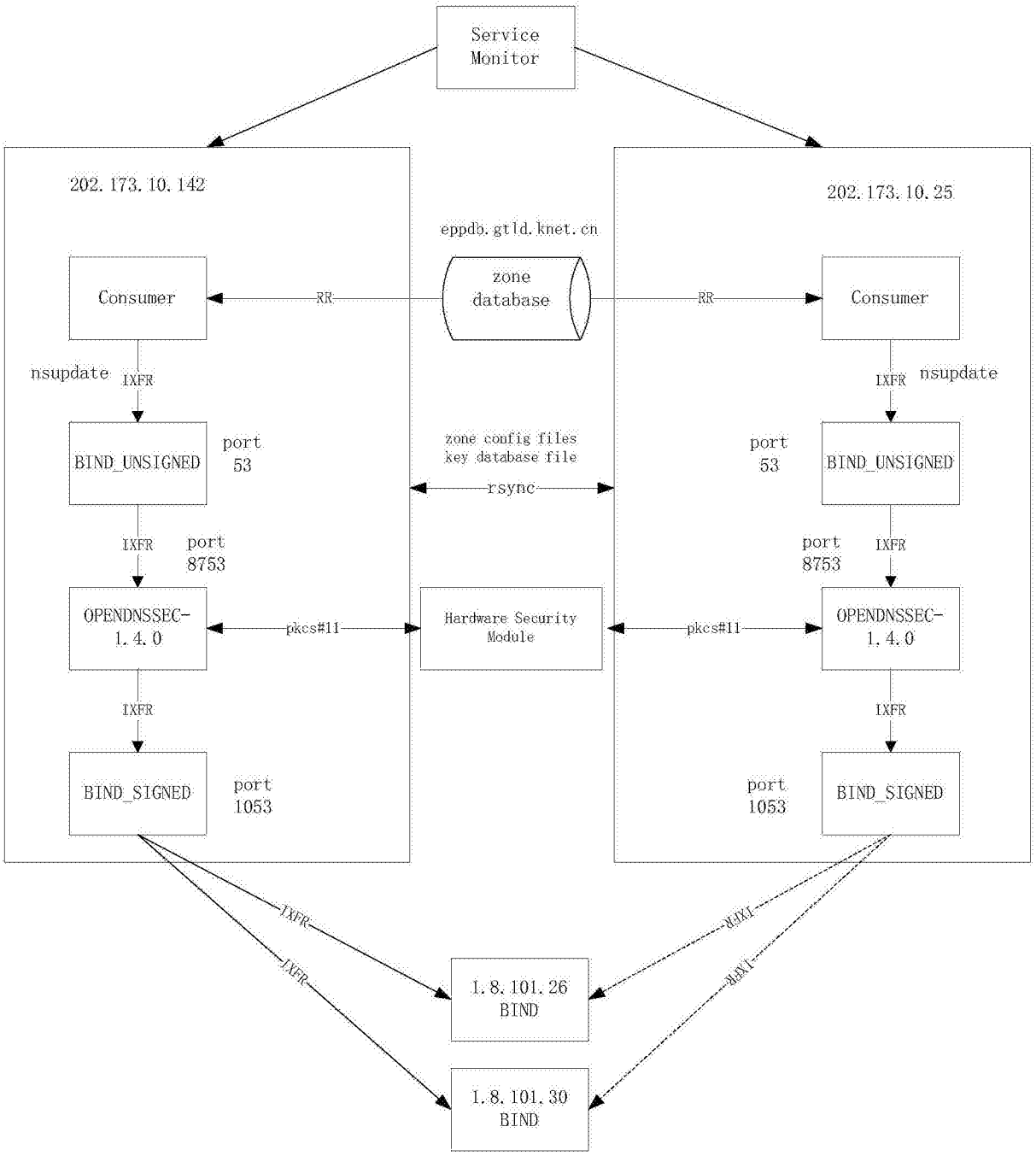

Service Monitor
202.173.10.142
202.173.10.25
eppdb.gtld.knet.cn
Consumer
RR
zone database
RR
Consumer
nsupdate
IXFR
IXFR
nsupdate
BIND_UNSIGNED
port 53
zone config files
key database file
rsync
port 53
BIND_UNSIGNED
IXFR
port 8753
port 8753
IXFR
OPENDNSSEC-1.4.0
pkcs#11
Hardware Security Module
pkcs#11
OPENDNSSEC-1.4.0
IXFR
IXFR
BIND_SIGNED
port 1053
port 1053
BIND_SIGNED
IXFR
IXFR
IXFR
IXFR
1.8.101.26 BIND
1.8.101.30 BIND

图3