·网络空间安全·　　文章编号：1000-3428(2023)11-0160-09　　文献标志码：A　　中图分类号：TP393

引入区块链的SDN路由一致性检测

刘宇宸，唐　菀，杨喜敏，张　艳

（中南民族大学 计算机科学学院，武汉 430074）

摘　要：为使软件定义网络(SDN)能满足复杂多样的应用层网络需求，SDN控制层采用多控制器结构，然而新制定的路由策略与已有路由策略间存在路由一致性问题，可能会导致数据层流表项存储冗余和网络流量的转发环路。提出一种基于区块链的SDN路由策略一致性检测方案RCDB-SDN，利用区块链不可篡改特性存储SDN流表项特征属性等网络信息，采用基于投票的实用拜占庭容错共识机制在控制层实现对流表项集的一致性验证，并降低路由策略一致性问题给网络带来的不良影响。通过验证输出端流表项的一致性，比较新制定的路由策略与已有策略的转发效果，检测造成存储冗余的重叠路径。根据有向图的环路检测算法及转发路径关键节点上的流表项，检测引起网络流量转发环路的环路路径。基于Multichain平台针对导致路径重叠和路径环路的流表项进行仿真实验，结果表明RCDB-SDN方案的检测精确率高于WedgeTail方案，达到95%以上，并且能在一定程度上减少控制层与数据层间的消息传递次数。

关键词：软件定义网络；区块链；路由一致性；共识机制；流表项

开放科学（资源服务）标志码（OSID）：

中文引用格式：刘宇宸，唐菀，杨喜敏，等. 引入区块链的SDN路由一致性检测[J]. 计算机工程，2023，49(11)：160-168.

英文引用格式：LIU Y C，TANG W，YANG X M，et al. Routing consistency detection with blockchain for SDN[J]. Computer Engineering，2023，49(11)：160-168.

Routing Consistency Detection with Blockchain for SDN

LIU Yuchen，TANG Wan，YANG Ximin，ZHANG Yan

（College of Computer Science，South-Central Minzu University，Wuhan 430074，China）

【Abstract】A multi-controller structure is adopted for the Software-Defined Network（SDN）control layer to meet complex and diverse application layer network requirements. However，there is still the problem of routing consistency between the latest and existing routing policies，which may lead to storage redundancy of flow entries in the data layer and flow forwarding loops.To address this issue，Routing strategy Consistency Detection based on Blockchain for SDN（RCDB-SDN）is proposed，whereby network information，such as feature attributes of flow entries stored in SDN switches，can also be obtained benefiting from the tamper-proof characteristics of the blockchain. By leveraging blockchain technology，RCDB-SDN can reduce the adverse impact of routing policy inconsistency on networks. The RCDB-SDN scheme verifies the consistency of flow entry sets at the control layer through a Practical Byzantine Fault Tolerant（PBFT）consensus mechanism based on voting.To detect whether path overlaps lead to storage redundancy，the proposed RCDB-SDN scheme compares the forwarding effectiveness of the newly formulated and existing routing policies by verifying the consistency of new and existing output flow entries. A circuit detection algorithm is applied with direction graphs and flow entry detection on key nodes of the forwarding path，to determine whether a path loop causes a flow forwarding loop in the current network. Experiments are carried out on flow entries leading to path overlaps and loops on the multichain platform.The results demonstrate that the detection accuracy of the RCDB-SDN scheme is higher than that of the WedgeTail scheme and can reach more than 95%，reducing the messaging times between control and data layers to a certain extent.

【Key words】Software-Defined Network（SDN）；blockchain；routing consistency；consensus mechanism；flow entry

DOI：10. 19678/j. issn. 1000-3428. 0065661

基金项目：湖北省自然科学基金（2020CFB629）；中南民族大学中央高校基本科研业务费专项资金（CZY22016）。

作者简介：刘宇宸（1997—），男，硕士研究生，主研方向为软件定义网络、区块链；唐　菀，教授；杨喜敏（通信作者），副教授；张　艳，硕士。

收稿日期：2022-09-02　　**修回日期：**2022-12-02　　**E-mail：**2020110278@mail.scuec.edu.cn

计算机工程 www.ecice06.com

0　概述

当前网络环境日益复杂，软件定义网络（Software-Defined Network，SDN）架构中的传统单一控制器结构已不能满足复杂多样的应用层需求[1-2]。控制层作为SDN架构中网络管理和调度的智能中心，新下发的路由策略与数据层已有的路由策略之间的一致性问题显得尤为重要。针对路由策略的一致性问题，在控制层的研究多数通过统计和分析进行检测[3]，无须对交换机或数据包进行额外处理，可降低网络部署复杂度。

在验证控制层路由策略一致性问题的研究方案中，多数方案利用算法建模进行验证[4]并直接分析控制层。区块链技术与SDN的结合[5]对于解决路由策略的一致性问题带来了新的思路。区块链去中心化的特性使其能在SDN平台得到应用，实现智能化网络资源管理并提升网络安全性和可扩展性[6]，同时通过共识机制确保路由策略的一致性[7-9]。但是，现有引入区块链技术的研究方案多数仅针对多控制器的协同问题，控制层的路由一致性问题还有待进一步解决[10]。

在多控制器结构下，控制器之间的协同处理[11-12]以及控制层的下发路由策略会对数据层造成影响。本文提出基于区块链的SDN路由策略一致性检测（Routing strategy Consistency Detection based on Blockchain for SDN，RCDB-SDN）方案，利用区块链存储流表项信息，结合共识机制对控制层新制定的流表项集进行一致性验证，并在控制器将流表项下发交换机前，检测出可能会对网络造成不良影响的流表项。

1　相关研究

在控制层的一致性研究中，ZHOU等[13]提出NEAt，通过拦截SDN应用的更新将对应策略制成有向图，对违反管理员高级策略的更新及时进行修复；ABHASHKUMAR等[14]设计一种多层图控制平面模型，通过自定义属性的验证算法直接对控制层进行分析以验证网络策略。

在多控制器场景下，基于拜占庭容错（Byzantine Fault Tolerance，BFT）机制，MA等[15]提出一种多控制器SDN网络架构，数据层交换机由多个控制器共同管理，并在控制层和数据层之间添加一个代理，以保证流表项的正确下发。SHAGHAGHI等[16]提出WedgeTail，选取哈希算法，通过比较网络中数据包的实际转发路径与控制层的预期转发路径来检测异常的数据包转发问题，但这可能会对网络的实际部署造成严重影响。LEI等[17]构建2VMeri框架，使用Bloom过滤器和二维向量标签，验证控制层策略和数据层规则的一致性。

区块链具有去中心化、持久性等特征，能够实现资源共享，通过共识机制、链式结构等技术，可以保证数据共享的安全性和可靠性。学者们对SDN与区块链技术的融合进行了大量研究并取得了一系列研究成果。MONDAL等[18]提出BIND方案，基于效用博弈论，借助备用路径解决流表项冲突问题，在多租户控制器之间引入区块链技术，使得每个控制器都能公平地替换流表项，确保控制器间的合作并避免垄断。FAN等[10]设计并构建区块链协调控制器（Blockchain-Coordinating Controller，BCC）来确保SDN控制器间的协调。CHATTARAJ等[19]结合基于属性的加密和基于证书的访问控制协议，引入实用拜占庭容错（Practical BFT，PBFT）算法，提出一种支持区块链的细粒度访问控制机制，提高了SDN的鲁棒性。LI等[20]设计多控制器规则执行验证（BlockREV）机制，采用区块链技术为转发行为提供不变性和隐私保护，保证跨域转发的正确性。

在将区块链技术应用于SDN控制层的研究中，GUO等[21]提出一种基于区块链的SDN安全框架，采用LLDP协议周期性地获取网络链路信息并保证多控制器之间拓扑信息的一致性，另一种基于区块链的SDN体系结构B-SDN[22]结合水平和垂直架构重新构建SDN网络的控制层。RAHMAN等[23]提出一种分层架构并部署SDN-IoT框架，通过识别和隔离恶意交换机来确保安全的簇头选择和网络通信，并保持控制器集群内的一致性。

学者们针对传统SDN中一致性问题的研究多数在数据层或控制层进行改进，较少涉及多控制器场景，也不适用于规模较大的多控制器场景。本文从解决方案、研究特点和主要技术等方面出发，归纳传统SDN与结合区块链技术[12]的SDN在一致性问题上的研究现状，如表1所示。虽然引入区块链技术能更好地考虑控制器之间的协同通信、跨域转发的正确性以及多控制器之间网络拓扑和网络状态等信息的一致性，但对于控制层路由策略与网络已有路由策略之间的一致性问题仍需进一步探讨。因此，本文提出RCDB-SDN方案，通过引入区块链技术来改进基于控制层的路由策略的一致性检测。

计算机工程 www.ecice06.com

表1 SDN一致性问题研究比较

Table 1 Comparison of research on consistency problems in SDN

分类	解决方案	思路与特点	所用技术
传统SDN	NEAt[13]	拦截SDN应用的更新,将策略制定成有向图,及时修复违反高级策略的更新	图算法
	Tiramisu[14]	基于ARC进行改进,使用多层图的控制层模型	图算法
	多控制器异常检测[15]	基于BFT改进SDN多控制器异常检测方法,保证流表的正确下发	BFT
	WedgeTail[16]	比较网络中数据包的实际转发路径与控制层的预期转发路径	哈希算法、数据标签
	2VMeri[17]	使用Bloom过滤器和二维向量标签,验证控制层和数据层的一致性	Bloom过滤器、二维向量标签
引入区块链的SDN	SD-WAN[10]	设计并构建区块链协调控制器,确保多控制器之间的协调	重构BCC、智能合约
	BIND[18]	借助备用路径,基于效用博弈确保控制器之间的合作,引入区块链确保流表项的更新	备用路径、效用博弈
	PBAC-SDN[19]	是一种支持区块链的细粒度访问控制机制,引入PBFT共识方法	访问控制、共识机制
	BlockREV[20]	是一种安全的多控制器规则执行验证机制,基于转发路径的验证算法	聚合签名、路径验证
	BCSDN[21]	提出基于区块链的SDN安全框架,物理上分布式、逻辑上集中式,采用LLDP协议获取网络链路信息	LLDP
	B-SDN[22]	基于区块链技术,混合水平和垂直架构重新构建SDN的控制层	控制层重构
	SDN-IoT[23]	构建分层架构部署区块链,通过识别和隔离恶意交换机来确保簇头选择和网络通信	簇头选择

2 基于区块链的一致性检测

RCDB-SDN方案在SDN架构中引入区块链系统:控制层采用水平分布式架构,控制器之间构建区块链网络;数据层的交换机被划分在不同的区域,每个区域分属于不同的控制器管理。SDN交换机中的流表项是网络设备进行数据转发的依据,指导匹配和转发数据包的操作。在OpenFlow 1.3版本中,流表项由MatchField、Priority、Counter、Instruction、Timeout、Cookie和Flag等字段组成。RCDB-SDN方案架构如图1所示。

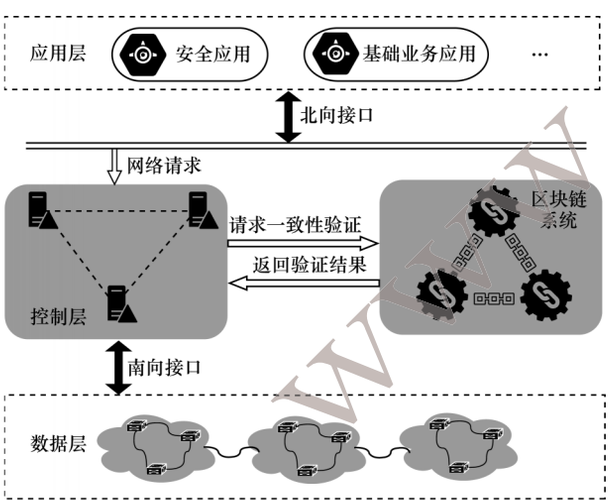


图1 RCDB-SDN方案架构

Fig.1 Architecture of RCDB-SDN scheme

在网络运行期间,应用层通过北向接口向控制层发送网络请求,控制层根据接收到的网络请求制定路由策略并生成流表项集,数据层进行网络流量的转发和处理。区块链系统负责存储流表项信息以及对流表项集进行一致性验证。区块链各节点在控制层新生成的流表项集被下发之前对其进行共识验证,检测该流表项集在数据层所对应的转发路径,以判断其是否会导致已有网络出现路径重叠或路径环路。

2.1 区块链与SDN的融合

在RCDB-SDN中,区块链技术与SDN的结合主要体现在以下两环节:

1)区块链存储流表项信息,确保流表项数据的可信度和完整性。控制层解析要下发的流表项集,将得到的流表项属性信息发送到区块链系统请求一致性验证,只有通过验证的流表项信息才会被存储在区块链。

2)区块链节点对需要下发的流表项集采用共识验证机制进行一致性验证。区块链每个节点都遵循基于投票的PBFT共识机制[24]对一致性验证请求进行决策,并将整个区块链系统的最终决策返回控制层,只有在区块链系统中达成共识的流表项集才能下发。

在进行路由策略冲突检测时,以MatchField、Instruction、Priority三字段作为路由策略的主要特征和参考因素。在OpenFlow 1.3版本中,完整的MatchField字段涵盖了开放系统互联(Open System Interconnection,OSI)模型中L1(物理层)至L4(传输层)网络的特征。但由于考虑全部MatchField字段过于复杂,且SDN应用主要处于OSI模型的L3(网络层)至L4网络,选取MatchField字段中的L3和L4特征作为研究特征。

一条流表项r和一个流表项集R分别表示为$r=<s,t,p_i,p_o,i_s,i_d,p_r,a>$和$R=\{r_1,r_2,\cdots,r_n\}$,其中,s、t、$p_i$、$p_o$、$i_s$、$i_d$、$p_r$、a分别表示交换机ID、流表ID、入端

口、出端口、源地址、目的地址、优先级和动作，n表示流表项集R中的流表项总数。

2.2　流表项集上链

控制层根据制定的路由策略生成一组流表项集，只有通过区块链系统的共识验证之后才能被下发到数据层并写入区块链。流表项集上链流程如图2所示，具体步骤如下：

步骤1　控制层根据网络请求制定新的路由策略。

步骤2　根据新路由策略生成流表项集合。

步骤3　格式化流表项集的相关属性信息成一条交易，并打包发送给区块链系统。

步骤4　区块链系统采用基于投票的共识机制对交易进行共识验证。

步骤5　将验证结果返回给控制层。

步骤6　只有验证通过的流表项集才能被下发到数据层并写入区块，否则取消整个流表项集的下发。

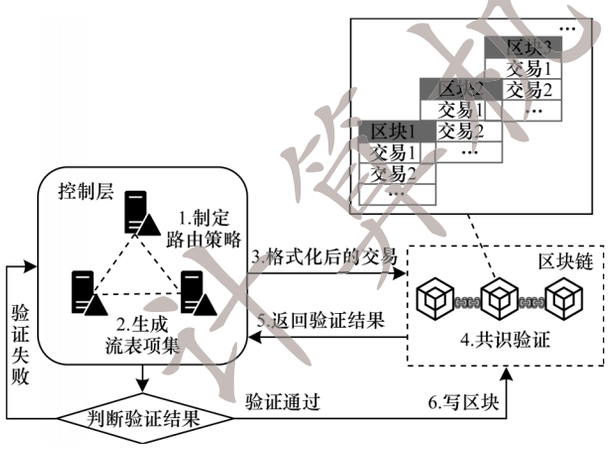


图2　流表项集上链过程

Fig.2　Up-chaining process of the set of flow entries

表2和表3给出了RCDB-SDN区块结构和交易结构。区块结构由区块头和区块体组成，区块头包含对区块进行描述的属性，区块体是存储的交易，交易所包含的元素对应流表项集的特征属性，它们都是在控制层对所要下发的流表项集进行解析时获得。

表2　区块结构

Table 2　Block structure

区块元素	描述
hash	当前区块的哈希值
previous block hash	前一个区块的哈希值
miner	广播区块的节点ID
size	区块大小
height	区块高度
Merkle root	Merkle树根
time	区块生成时间
Tx	交易（格式化的流表项集）

表3　交易结构

Table 3　Transaction structure

交易元素	描述
switch-id	交换机ID
table-id	流表ID
in-port	输入端口
out-port	输出端口
src-ip	源IP地址
dst-ip	目的IP地址
action	动作
priority	优先级

2.3　问题描述

控制层根据应用层的请求所制定的路由策略对应数据层的流表项，一组具有相同源IP和目的IP的流表项可以表示一条转发路径。新的转发路径添加到现有网络的转发路径后，可能会带来路径重叠和路径环路问题。

1）路径重叠：当新的转发路径与网络中已有的转发路径重叠，且两条路径对应的流表项具有相同的转发效果时，会造成数据层交换机中的流表项存储冗余。

2）路径环路：当新的转发路径加入现有网络后，与已有的转发路径构成转发路径环路，并且在导致成环的关键节点上，数据包匹配新制定的流表项，引起网络中数据包的转发环路。

此外，传统的检测方案通过比较实际转发路径与控制层预设转发路径来检测路径重叠和路径环路问题，需要将流表项下发到数据层后再进行验证，增加了控制层与数据层之间的交互，从而给网络带来额外的处理能耗。

3　基于PBFT的一致性检测

3.1　区块链共识验证

基于PBFT共识机制，RCDB-SDN的区块链节点对需要下发的流表项集进行一致性验证。将网络中的所有控制器节点分为请求节点Q和验证节点V，请求节点为收到应用层网络请求并制定新的路由策略及下发的节点；验证节点是对请求节点所要下发的路由策略进行一致性验证的所有剩余节点。从验证节点中随机选取一个节点作为主节点M，对所要下发的流表项集进行一致性验证和投票的流程如图3所示。

请求节点解析流表项集得到其中每条流表项的特征属性（包括源地址、目的地址、优先级、交换机ID、流表ID等）对应表3中的交易元素，将所有流表项的特征属性格式转化成一条交易Tx。主节点将Tx打包广播给所有区块链节点，每个节点检索存储的数据进行一致性验证。在对区块链数据进行检索时，为降低遍历所有数据的耗时，将区块链所有存储的区块按节点数量进行平均划分。每个节点只在划分到的区块中进行检索，所有节点并行地检索区块链数据，可以加快遍历整个区块链并减少时延。

计算机工程 www.ecice.com

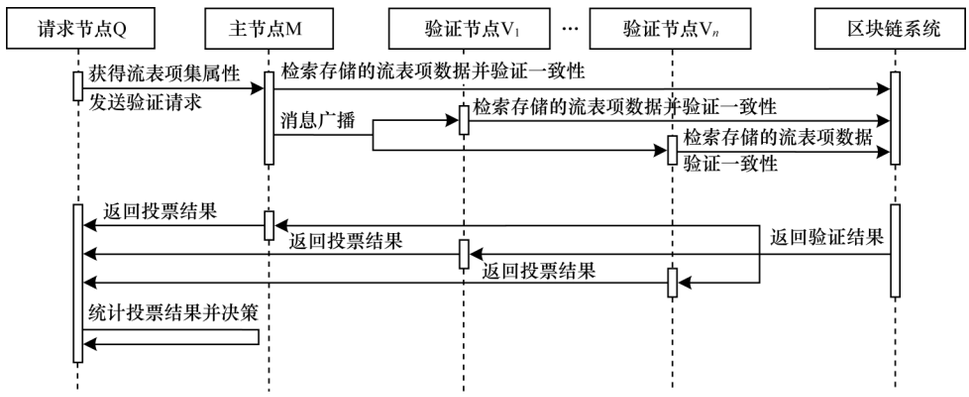


图3 基于投票的流表项共识验证

Fig.3 Consensus verification of flow entries based on voting

根据一致性验证的结果,各验证节点将投票信息反馈给请求节点。若验证失败,则返回false,为反对票;否则返回true,为同意票。按照少数服从多数的原则,同意票数不少于半数时,判定该交易有效,请求节点此次获得向区块链中写区块的权利;否则该交易无效,请求节点此次无权写区块。请求节点根据投票结果来决策是否下发流表项集。若下发,则在下发的同时将流表项集格式化后,打包并写入区块链。

3.2 一致性检测

在区块链系统中,每个节点根据自己检索的数据对交易进行一致性验证,再按照各自的验证结果投票,汇总投票结果之后返回控制层进行决策。在一致性检测中,RCDB-SDN方案分为针对路径重叠和路径环路两部分。

对于路径重叠的检测,即在检测到完全重叠的转发路径时,验证流表项特征属性的相关性,判断是否会造成流表存储冗余[25]。对于路径环路的检测,采用环路检测算法检测构建的有向图是否存在环路,并在关键节点上验证流表项特征属性的相关性。若路径环路存在,则判断其是否会造成网络转发环路。

在构建转发路径时,节点Node = <s, p_i, p_o, nextNode>,其中,s、p_i、p_o、nextNode分别表示交换机ID、入端口、出端口、当前节点的下一跳节点。一条转发路径P的表示形式为$P=\{Node_1, Node_2, \cdots, Node_n\}$。

3.2.1 路径重叠检测

由于两条转发路径完全重叠,在路径上各节点中的流表项具有相同的转发效果,因此验证两条转发路径的转发效果是否一致,只须验证两条路径上输出端节点中的流表项。

控制层对制定的流表项集R进行解析得到特征属性,结合区块链系统的共识机制对其进行一致性验证,确保R的下发不会造成流表项的存储冗余。路径重叠检测的流程如图4所示,具体步骤如下:

步骤1 构建转发路径。控制层根据上层应用下发的网络请求制定路由策略,生成流表项集R并进行解析,将获得的特征属性格式化成交易Tx,打包发送到区块链系统。在区块链中查找与R途经相同交换机的流表项集R',获取并结合对应流表项集的特征属性,构建两条转发路径P和P'。

步骤2 一致性检测。检测P和P'是否相同。若两者相同,则存在路径重叠,此时返回路径输出端节点NodeT。只有当P和P'满足式(1)时,才存在这样一个输出端节点NodeT,其中num表示路径中所包含的节点数量。

$$\text{NodeT}=P'.\text{Node},\ (P.\text{num}>1)\wedge(P'.\text{num}>1)\wedge(P\cap P'=P\cup P')\wedge(P'.\text{Node.nextNode}=\varnothing) \tag{1}$$

步骤3 流表项检测。若NodeT存在,则在两条转发路径上的NodeT节点所对应的交换机中存在流表项r和r'(r为新制定的流表项,r'为交换机已有的流表项),通过函数$f(r,r')$验证两者是否会引起存储冗余。当r和r'满足式(2)时,函数返回值为true,表明会引起流表项存储冗余(用PO表示)。

$$\text{PO}=f(r,r'),\ (r.i_s\subseteq r'.i_s)\vee(r.i_d\subseteq r'.i_d)\vee(r.i_s\supset r'.i_s)\vee(r.i_d\supset r'.i_d) \tag{2}$$

步骤4 若验证结果表明不会引起流表项存储冗余,则下发R;反之取消R的下发。

在上述检测流程中,基于解析得到的流表项特征属性,通过区块链系统的检索,在存储的区块中找到与其相对应的流表项属性并构建转发路径。转发路径的构建以及输出端节点上的流表项验证是路径重叠检测的关键。

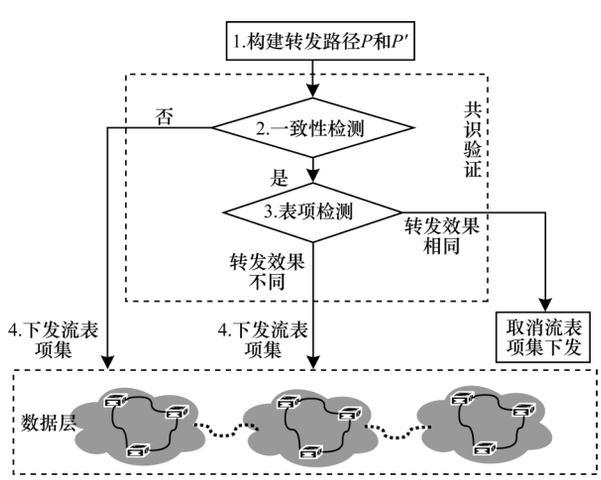


图4 路径重叠检测

Fig.4 Detection of path overlap

计算机工程 www.ecice.com

3.2.2　路径环路检测

控制层对生成的流表项集R进行解析得到特征属性，借助有向图的构建和环路检测，结合区块链系统的共识机制完成一致性验证，确保R的下发不会造成网络中数据包转发环路。路径环路检测的流程如图5所示，具体步骤如下：

步骤1　构建有向图。控制层根据上层应用下发的网络请求制定路由策略，生成流表项集R并进行解析，将获得的特征属性格式化成交易Tx，打包发送到区块链系统。在区块链中查找和R途径相同交换机的流表项集R'，获取对应的流表项集的特征属性，结合R和R'的特征属性，构建有向图G。

步骤2　有向图G环路检测。有向图G=<V,E>，基于深度优先搜索来检测图G是否存在一个环路（用P_{loop}表示）。一条边e表示为<Node.s, Node.nextNode>，节点集合$V=\{s_1,s_2,\cdots,s_k\}$，需要满足条件$\forall s\in V,\exists(P.\text{Node}.s=s)\vee(P'.\text{Node}.s=s)$，边集合$E=\{e_1,e_2,\cdots,e_m\}$，需要满足条件$\forall e\in E,\exists(<P.\text{Node}.s,P.\text{Node.nextNode}>=e)\vee(<P'.\text{Node}.s,P'.\text{Node.nextNode}>=e)$，其中，$k$和$m$分别表示$V$和$E$中节点和边的数量。

步骤3　确定环路关键节点KeyNode。若有向图G存在环路，则表明两组流表项集同时存在会导致路径环路。因此，需要找出环路关键节点，在该节点的转发操作会直接决定是否产生网络转发环路。

$$\text{KeyNode}=\text{Node},\left(P'.\text{Node}.s=P_{\text{loop}}.\text{Node}.s\right)\wedge\left(P'.\text{Node.nextNode}\neq P_{\text{loop}}.\text{Node.nextNode}\right)\quad(3)$$

步骤4　流表项字段相关性检测。检测节点KeyNode所对应的交换机上流表项r和r'，验证两者是否具有相关性，即r和r'的源IP地址与目的IP地址分别是否存在包含与被包含的情况。

步骤5　匹配顺序检测。当多条流表项具有相同的优先级与不同的匹配域粒度时，会按照流表项添加的先后顺序匹配。因此，若r和r'具有相关性，则进一步检测两者同时存在时，数据包匹配的优先次序。通过函数$v(r,r')$验证r和r'，当两者满足式(4)时，函数返回值为true，表明会导致网络转发环路（用PL表示）。

$$\text{PL}=v(r,r'),\left(r.p_{\text{r}}>r'.p_{\text{r}}\right)\wedge\left(\left(r.i_{\text{s}}\subseteq r'.i_{\text{s}}\right)\vee\left(r.i_{\text{d}}\subseteq r'.i_{\text{d}}\right)\vee\left(r.i_{\text{s}}\supset r'.i_{\text{s}}\right)\vee\left(r.i_{\text{d}}\supset r'.i_{\text{d}}\right)\right)\quad(4)$$

步骤6　若验证结果表明不会产生路径环路，也不会引起网络环路，则下发R；反之取消R的下发。

在上述检测流程中：有向图G的环路检测是路径环路检测的关键所在，目的在于初步检测是否有导致路径环路存在的可能；流表项字段与匹配顺序检测则是验证路径环路的重要步骤。

总之，一致性检测分为路径重叠和路径环路两阶段。前者通过构建转发路径进行比较，需要的存储开销与网络中存在的重叠路径数量有关；后者通过构建有向图进行验证，考虑与新制定的流表项集存在相关性的流表项集，存储开销较前者更大。

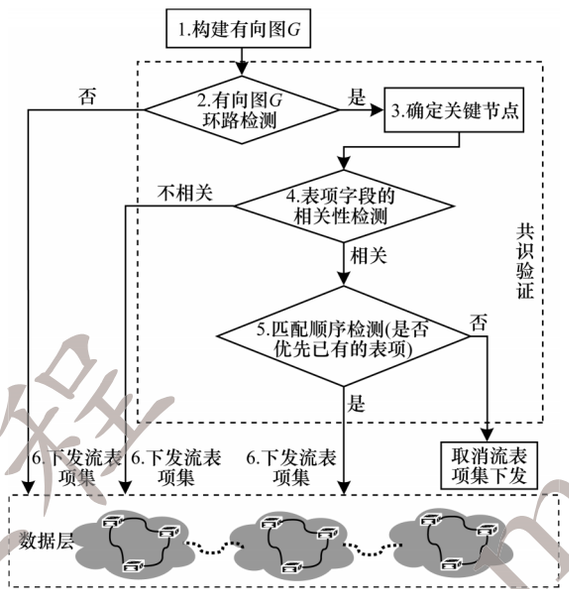


图5　路径环路检测

Fig.5　Detection of path loop

4　实验与评估

4.1　实验平台与设置

考虑到快速构建区块链网络的需求，选取Multichain[26]作为实验的区块链平台。在初始化区块链时，确保在没有新的交易产生时，区块链平台不会自动添加区块，以减少区块链平台在无区块写入时存储空间的使用以及无效区块的生成。实验选用Ubuntu作为系统平台、Mininet作为网络模拟器及Opendaylight作为SDN控制器。

基于Multichain平台和Mininet模拟器构建RCDB-SDN方案模型，使用20个交换机（s1~s20），并依次划分为5个域（D1~D5），由5个控制器（c1~c5）分管。在网络运行期间，每当有新的流表项集生成时，在对应的控制器中将其格式化为一条交易并打包之后，广播给其他控制器节点，向每个控制器节点发起验证请求，其余控制器节点按照RCDB-SDN方案进行检测，并将结果反馈给初始发起请求的节点。

仿真实验搭建的网络采用图6中的数据中心网络Fat-Tree[27]拓扑结构，并在控制层通过编写脚本文件生成会造成路径重叠和路径环路的流表项集。流表项集的下发次数为200和400（对每一次流表项集的下发都进行检测），每类实验分别有10组，每组实验分别在不同的域内以及域间模拟会造成影响的流表项集。取10组实验的平均值，评估当网络中实际存在的流表项数量变化时，RCDB-SDN方案对路径重叠和路径环路的检测情况。在每组实验所下发的流表项集中，实际会造成路径重叠或者路径环路的流表项集与实际不会造成影响的流表项集比例为1∶1。

www.ecice06.com

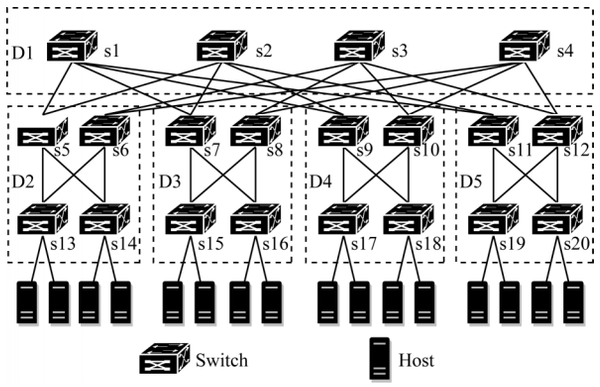


图6 仿真实验平台的Fat-Tree网络拓扑结构

Fig.6 Fat-Tree network topology of simulation platform

在网络中流表项集所对应的转发路径引发冲突的情形通常不会集中出现。因此,在模拟真实场景时,每次实验中会生成路径重叠和路径环路的流表项集下发的时间和周期不固定。

4.2 评价指标

选取精确率、误检率、查全率、漏检率和消息传递次数等5项指标对RCDB-SDN进行评估。精确率指在检测到的所有冲突结果中,真实冲突所占的比率。误检率指在实际不冲突的结果中,错误检测成冲突的结果所占的比率;查全率指检测出的真实冲突结果占全部真实冲突的比率;漏检率指未检测出的真实冲突占全部真实冲突的比率;消息传递次数用来统计控制层与数据层之间的消息传递。

在传统的没有引入区块链技术的检测方案WedgeTail[16]中,通过比较数据包的实际路径与控制层的预设路径之间的差异来检测异常。将RCDB-SDN方案的路径重叠和路径环路两部分检测与WedgeTail进行比较实验。

4.3 结果分析

4.3.1 路径重叠检测

路径重叠检测对比结果如图7所示。由图7可以看出,在分别下发200次和400次流表项集合的两类实验下,当现有网络中的流表项总数在一定范围内增长时,RCDB-SDN结合区块链技术对路径重叠检测的精确率和误检率整体上优于WedgeTail[16]。主要原因为RCDB-SDN通过检索区块链存储的所有流表项信息进行验证,但由于分区检索的缘故,一条转发路径对应的流表项可能被划分到不同的节点进行验证,导致检测结果与实际结果不一致。在不同检测次数下,区块链存储的流表项信息与网络中实际生效的流表项之间存在的差异会对检测的精确率产生影响。此外,对于RCDB-SDN而言,检测精确率和误检率受检测次数增加的影响不明显,反而随着网络中流表项数量的增加影响较明显。随着流表项总数的增加,在实际网络中流表信息的删除和更新会改变流表项数量,但区块链系统中存储的数据不会减少,因此区块链存储的流表项信息会与实际网络中有效的流表项之间出现差异,导致RCDB-SDN的精确率有所下降,误检率有所上升,但整体上RCDB-SDN的精确率依然高于WedgeTail,误检率低于WedgeTail。

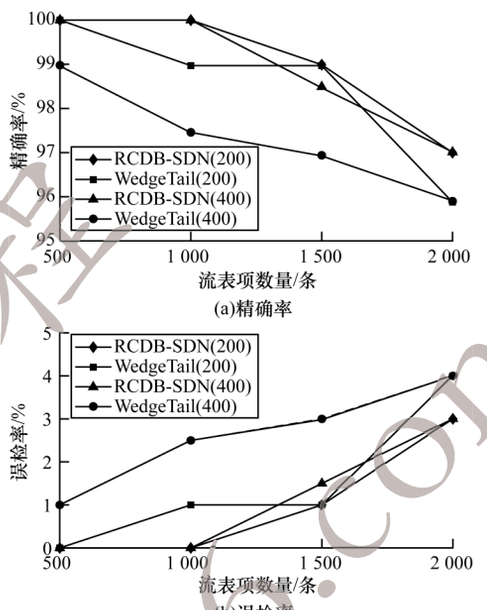


图7 路径重叠检测对比

Fig.7 Comparison of path overlap detection

路径重叠检测的查全率和漏检率如表4所示。由表4可以看出,检测次数对RCDB-SDN和WedgeTail两种方案的查全率和漏检率影响不大,在分别下发200次和400次流表项集合的两类实验下的实验结果大致相近,但是前者的查全率高于后者,且随着流表项数量增多而愈发显著。同时,通过对比消息传递次数(如图8所示)可以看出:WedgeTail在检测到路径重叠之后,需要反馈信息给控制器,然后由控制器再次下发指令消息删除对应的流表项;RCDB-SDN在流表项下发之前进行检测,可以避免这一步骤,使控制层与数据层之间的消息传递次数更少。

表4 路径重叠检测的查全率和漏检率

Table 4 Recall and missed detection rate of path overlap detection

流表项数量/条	查全率/%				漏检率/%			
	RCDB-SDN		WedgeTail		RCDB-SDN		WedgeTail	
	200	400	200	400	200	400	200	400
500	98.0	98.5	97.0	97.0	2.0	1.5	3.0	3.0
1 000	98.0	98.0	96.0	96.0	2.0	2.0	4.0	4.0
1 500	98.0	98.0	96.0	95.0	2.0	2.0	4.0	5.0
2 000	97.0	97.5	93.0	93.5	3.0	2.5	7.0	6.5

www.ecice0.com 计算机工程

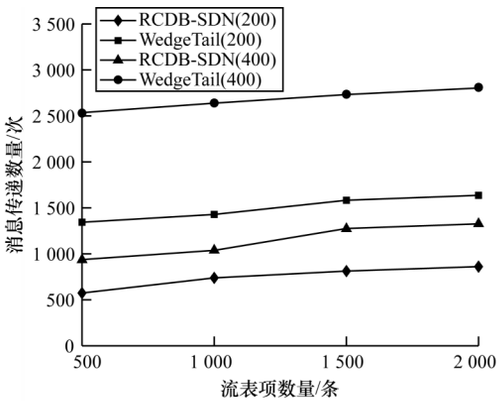


图8　路径重叠检测的消息传递次数

Fig.8　Messaging times during path overlap detection

4.3.2　路径环路检测

路径环路检测对比结果如图9所示。由图9可以看出，当网络中的流表项总数在一定范围内增长时，在分别下发200次和400次流表项集合的两类实验下，RCDB-SDN对于路径环路检测的精确率和误检率整体上优于WedgeTail[16]。主要原因为RCDB-SDN对区块链存储的数据分区之后进行检索，在提高检索速度的同时，不同的节点可能只对一条转发路径所对应的流表项集中的一部分流表项进行验证，验证不完全导致检测结果与实际情况出现偏差。随着时间推移，当检测次数增加之后，检测结果与实际情况不一致的可能性会有所增加。此外，对于RCDB-SDN而言，路径环路检测次数的增加对精确率和误检率有一定影响，但网络中流表项总量对精确率和误检率的影响更大。随着流表项总数的增加，在RCDB-SDN中，区块链存储的流表项信息会持续增加，但是实际网络中的流表项由于删除和更新等操作，与区块链存储的数据会逐步出现差异，因此RCDB-SDN的精确率有所下降而误检率有所上升，但整体上其精确率依然高于WedgeTail，误检率低于WedgeTail。

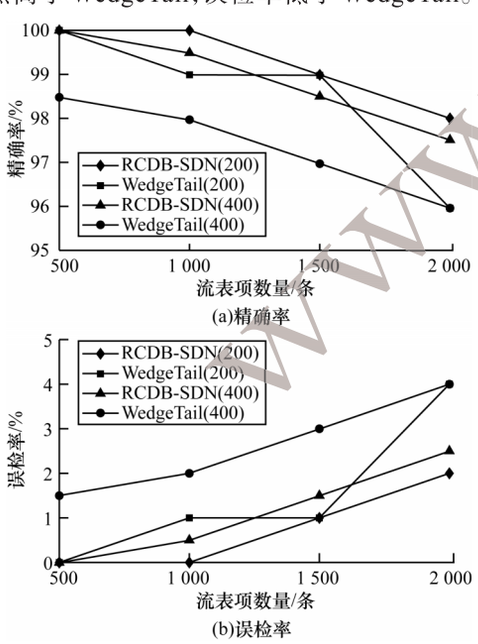


图9　路径环路检测对比

Fig.9　Comparison of path loop detection

路径环路检测的查全率和漏检率如表5所示。由表5可以看出，在查全率和漏检率上，RCDB-SDN和WedgeTail两种方案受检测次数的影响较小，在分别下发200次和400次流表项集合的两类实验下的实验结果大致相近，但是前者的查全率高于后者。

表5　路径环路检测的查全率和漏检率

Table 5　Recall and missed detection rate of path loop detection

流表项数量/条	查全率/%				漏检率/%			
	RCDB-SDN		WedgeTail		RCDB-SDN		WedgeTail	
	200	400	200	400	200	400	200	400
500	99.0	99.0	98.0	97.5	1.0	1.0	2.0	2.5
1 000	99.0	98.5	98.0	96.5	1.0	1.5	2.0	3.5
1 500	98.0	98.5	97.0	96.0	2.0	1.5	3.0	4.0
2 000	98.0	98.0	95.0	95.0	2.0	2.0	5.0	5.0

路径环路检测的消息传递次数如图10所示。由图10可以看出，相较于WedgeTail在检测到路径环路后反馈信息给控制器，并下发指令删除对应的流表项，RCDB-SDN在流表项下发前就进行路径环路检测，可以在出现路径环路时，有效减少控制层与数据层之间的消息传递次数。

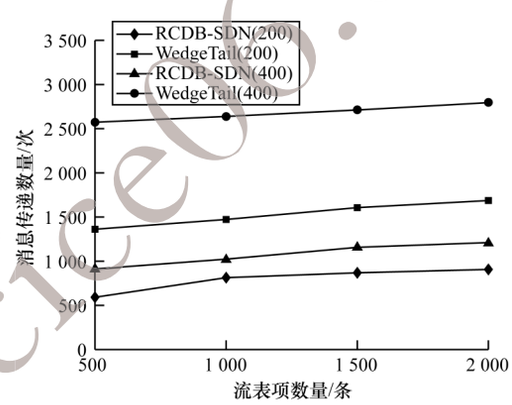


图10　路径环路检测的消息传递次数

Fig.10　Messaging times during path loop detection

综合两部分检测的实验结果来看，由于设计的RCDB-SDN方案在检测中对区块链进行了划分，因此由不同的节点各自负责区块链存储的一部分数据。当实际会引起冲突（路径重叠或路径环路）的流表项集恰好被划分到不同的节点进行检测时，则被检测为不会引起冲突的可能性较大。

另外，由于真实网络中的流表不断更新，被删除的流表项却依然存储在区块链中，在借助区块链对实际上不会引起冲突的流表项集进行一致性验证时，也可能被错误地检测为会引起网络路由信息冲突，导致检测结果的误差。

5　结束语

SDN所具有的转控分离的特点使其可以灵活高效地处理网络流量，但当SDN采用多控制器结构时，控制层根据应用层网络请求制定路由策略，生成的流

www.ecice06.com

表项可能会带来流表项存储冗余和网络流量转发环路等问题。本文提出的RCDB-SDN方案结合区块链可追溯、不可篡改的特性，引入共识机制检测路由策略的一致性，并通过仿真实验验证了RCDB-SDN方案对路径重叠和路径环路检测的可行性与有效性。后续将进一步优化检测方案，当区块链系统存储的流表项信息与实际网络存储的有效流表项信息之间的差异越来越大时，通过改进区块链系统的检索方式，尽可能地提高检测结果与实际网络之间的一致性。

参考文献

[1] YRJÖLÄ S. How could blockchain transform 6G towards open ecosystemic business models?[C]//Proceedings of IEEE International Conference on Communications Workshops. Washington D. C. , USA: IEEE Press, 2020: 1-6.

[2] AUJLA G S, GARG S, KAUR K, et al. Software defined Internet of everything[M]. Berlin, Germany: Springer, 2022.

[3] ZHANG P, ZHANG F Z, XU S M, et al. Network-wide forwarding anomaly detection and localization in software defined networks [J]. IEEE/ACM Transactions on Networking, 2021, 29(1): 332-345.

[4] GEMBER-JACOBSON A, VISWANATHAN R, AKELLA A, et al. Fast control plane analysis using an abstract representation[C]//Proceedings of 2016 ACM SIGCOMM Conference. New York, USA: ACM Press, 2016: 300-313.

[5] KHORSANDROO S, SÁNCHEZ A G, TOSUN A S, et al. Hybrid SDN evolution: a comprehensive survey of the state-of-the-art[J]. Computer Networks, 2021, 192: 107981.

[6] NGUYEN T, TRAN N, LOVEN L, et al. Privacy-aware blockchain innovation for 6G: challenges and opportunities [C]//Proceedings of the 2nd 6G Wireless Summit. Washington D. C. , USA: IEEE Press, 2020: 1-5.

[7] 关建峰，牛晓彤，高先明，等. SDN多控制器共识机制研究综述[J]. 数据与计算发展前沿，2021，3(1)：15-33.
GUAN J F, NIU X T, GAO X M, et al. Review on consensus mechanism of SDN multi-controller[J]. Frontiers of Data & Computing, 2021, 3(1): 15-33. (in Chinese)

[8] LATIF S A, WEN F B X, IWENDI C, et al. AI-empowered, blockchain and SDN integrated security architecture for IoT network of cyber physical systems [J]. Computer Communications, 2022, 181: 274-283.

[9] WARNAT-HERRESTHAL S, SCHULTZE H. Swarm Learning for decentralized and confidential clinical machine learning[J]. Nature, 2021, 594(7862): 265-270.

[10] FAN W J, CHANG S Y, KUMAR S, et al. Blockchain-based secure coordination for distributed SDN control plane [C]//Proceedings of the 7th International Conference on Network Softwarization. Washington D. C. , USA: IEEE Press, 2021: 253-257.

[11] 唐菀，张艳，杨喜敏，等. 引入区块链的SDN-IoT网络安全：架构、方案与挑战[J]. 小型微型计算机系统，2022，43(10)：2179-2199.
TANG W, ZHANG Y, YANG X M, et al. Network security of SDN-IoT with blockchain: architecture, scheme and challenge[J]. Journal of Chinese Computer Systems, 2022, 43(10): 2179-2199. (in Chinese)

[12] 张亮，刘百祥，张如意，等. 区块链技术综述[J]. 计算机工程，2019，45(5)：1-12.
ZHANG L, LIU B X, ZHANG R Y, et al. Overview of blockchain technology[J]. Computer Engineering, 2019, 45(5): 1-12. (in Chinese)

[13] ZHOU W X, CROFT J, LIU B Z, et al. Automatically correcting networks with NEAt[C]//Proceedings of the 15th USENIX Conference on Networked Systems Design and Implementation. New York, USA: ACM Press, 2018: 595-608.

[14] ABHASHKUMAR A, GEMBER-JACOBSON A, AKELLA A. Tiramisu: fast multilayer network verification [C]// Proceedings of the 17th USENIX Conference on Networked Systems Design and Implementation. New York, USA: ACM Press, 2020: 201-220.

[15] MA Q Q, DONG L G, JIANG X, et al. Research on anomaly detection method for SDN multi-controller[C]//Proceedings of International Conference on Information Science, Parallel and Distributed Systems. Washington D. C. , USA: IEEE Press, 2022: 136-139.

[16] SHAGHAGHI A, ALI KAAFAR M, JHA S. WedgeTail: an intrusion prevention system for the data plane of software defined networks[C]//Proceedings of 2017 ACM on Asia Conference on Computer and Communications Security. New York, USA: ACM Press, 2017: 849-861.

[17] LEI K, LI K K, HUANG J L, et al. Measuring the control-data plane consistency in software defined networking [C]// Proceedings of IEEE International Conference on Communications. Washington D. C. , USA: IEEE Press, 2018: 1-7.

[18] MONDAL A, MISRA S. BIND: blockchain-based flow-table partitioning in distributed multi-tenant software-defined networks[C]//Proceedings of IEEE Conference on Computer Communications Workshops. Washington D. C. , USA: IEEE Press, 2020: 219-224.

[19] CHATTARAJ D, BERA B, DAS A K, et al. Designing fine-grained access control for software-defined networks using private blockchain[J]. IEEE Internet of Things Journal, 2022, 9(2): 1542-1559.

[20] LI P, GUO S T, WU J H, et al. BlockREV: blockchain-enabled multi-controller rule enforcement verification in SDN[EB/OL]. [2022-08-20]. https://doi. org/10. 1155/2022/7294638.

[21] GUO X, WANG C, CAO L C, et al. A novel security mechanism for software defined network based on Blockchain [J]. Computer Science and Information Systems, 2022, 19(2): 523-545.

[22] TONG W, TIAN W S, DONG X W, et al. B-SDN: a novel blockchain-based software defined network architecture [C]//Proceedings of International Conference on Networking and Network Applications. Washington D. C. , USA: IEEE Press, 2021: 206-212.

[23] RAHMAN A, ISLAM M J, MONTIERI A, et al. SmartBlock-SDN: an optimized blockchain-SDN framework for resource management in IoT[J]. IEEE Access, 2021, 9: 28361-28376.

[24] 谭敏生，杨杰，丁琳，等. 区块链共识机制综述[J]. 计算机工程，2020，46(12)：1-11.
TAN M S, YANG J, DING L, et al. Review of consensus mechanism of blockchain[J]. Computer Engineering, 2020, 46(12): 1-11. (in Chinese)

[25] 陈志鹏，徐明伟，杨芫. SDN交换机转发规则TCAM存储优化综述[J]. 计算机学报，2021，44(7)：1341-1362.
CHEN Z P, XU M W, YANG Y. A survey on TCAM storage optimization for SDN switch forwarding rules[J]. Chinese Journal of Computers, 2021, 44(7): 1341-1362. (in Chinese)

[26] Coin Sciences Company. Multichain[EB/OL]. [2022-08-20]. http://www. multichain. com.

[27] HEMACHANDRA K G R P, JAYASENA K P N, RANKOTHGE W, et al. Investigating the performance in SDN based data centers under different network topologies [C]//Proceedings of the 2nd International Conference on Advanced Research in Computing. Washington D. C. , USA: IEEE Press, 2022: 361-366.

编辑 陆燕菲

计算机工程 www.ecice.com