基于密码标识的 SDN 安全控制转发方法

秦晰[1]，唐国栋[1]，常朝稳[1,2]
（1. 信息工程大学三院，河南 郑州 450001；2. 郑州信大先进技术研究院，河南 郑州 450001）

摘 要：针对软件定义网络（SDN, software defined networking）中匹配域范围有限和缺乏有效的数据来源验证机制问题，提出基于密码标识的 SDN 安全控制转发方法。首先，根据用户身份、文件属性或业务内容等特征信息生成密码标识，为数据流打上密码标识并用基于密码标识的私钥签名。其次，在其进出网络时验证签名，确保数据的真实性，同时将密码标识设计为转发设备能识别的匹配项，基于密码标识定义网络转发行为，形成基于人、物、业务流等细粒度网络控管能力。最后，通过实验分析验证该方法的有效性。

关键词：软件定义网络；密码标识；安全控制转发；流表匹配
中图分类号：TP393
文献标识码：A
doi: 10.11959/j.issn.1000-436x.2018022

SDN security control and forwarding method based on cipher identification

QIN Xi[1], TANG Guodong[1], CHANG Chaowen[1,2]
1. The Third Institute, Information Engineering University, Zhengzhou 450001, China
2. Zhengzhou Xinda Advanced Technology Research Institute, Zhengzhou 450001, China

Abstract: Aimed at the limited matching fields and the lack of effective data source authentication mechanism in the software defined networking (SDN), a SDN security control forwarding method based on cipher identification was proposed. First, the cipher identification was generated according to the user identity, file attributes or business content and other characteristics, and the data stream was marked by the cipher identification and signed with the private key based on the cipher identification. Then, when the data stream entered and left the network, the forwarding device verified its signature to ensure the authenticity of the data. At the same time, the cipher identification was designed as a matching item recognized by the forwarding device, and the network forwarding behavior was defined based on the cipher identification, so a fine-grained network control capability could be formed based on people, things, and business flow. Finally, the validity of the method is verified by experimental analysis.

Key words: software defined networking, cipher identification, security control and forwarding, flow table matching

1 引言

软件定义网络[1]是由美国斯坦福大学提出的一种逻辑控制和数据转发分离的新型网络架构[2]，被称为未来网络的重要发展方向。其集中管理和开放可编程等特性有效简化网络管理工作，可为用户提供个性的定制化服务，但降低了对 SDN 的攻击门槛，给其带来一系列安全威胁与挑战[3]。目前，针对 SDN 中存在的安全问题已有一些解决方案[4~7]，但转发设备流表匹配时缺乏有效数据来源验证机制，不能有效监测数据分组伪造等攻击行为且攻击者可对其行为否认，此外，现有的

收稿日期：2017-05-24；**修回日期**：2017-12-13
通信作者：唐国栋，tgdhooping@163.com
基金项目：国家自然科学基金资助项目（No. 61572517）
Foundation Item: The National Natural Science Foundation of China (No. 61572517)

OpenFlow 协议只能根据网络前 4 层特征信息控制数据转发行为，控制粒度有限，难以满足网络业务精确控制的需求。

结合 SDN 的特点，研究网络空间密码标识理论与技术，提出一种基于密码标识的 SDN 安全控制转发方法，在数据分组进出网络时对其来源进行验证，确保用户的不可否认性和数据分组的真实性，基于密码标识控制数据转发，从应用层、控制层和数据层全方位进行网络流的安全控制，形成基于人、物、业务流等细粒度网络控管能力，为实现 SDN 数据流的安全控制转发提供一种有效方法。

2 相关工作

流表匹配时，现有 2 种解决方案验证数据的来源，防止数据分组伪造。一种解决思路是在控制器开发安全模块，由控制器直接进行实时监控和检测。Yao 等[8]提出 VAVE 安全框架，在控制器中嵌入源地址验证模块，由控制器过滤伪造地址，实现敏捷灵活的源地址验证操作；Casado 等[9]提出 Ethane 架构，通过中央控制器向基于流的以太网交换机下发策略，统一管理流的准入，并由控制器完成对主机入网和用户入网的认证；Shin 等[10]提出一种面向 SDN 控制器的可组合安全模块开发框架 FRESCO，在 SDN 控制器中加入一个安全模块，允许网络管理人员创建新的模块化库，整合和扩展安全功能，使用 SDN 控制器、硬件控制和管理流量，快速实现部署多个通用网络安全功能，可替代防火墙和 IDS 等检测工具。然后在控制器开发安全模块，由控制器直接进行实时监控和检测会增加控制器负担，增大控制器遭受 DDoS 攻击的概率。另一种解决思路是依托 SDN 架构，将 SDN 交换机作为数据分组拦截或重定向平台，根据网络安全态势将网络流量重定向到安全设备中进行检测和监控。Ballard 等[11]提出 OpenSAFE，研究在大规模网络中通过 SDN 交换机线速重定向网络流量，将流路由到监测设备进行安全检查；Wundsam 等[12]提出的 OFRewind 也实现了类似功能，并支持多种粒度，而不仅是对整个 OpenFlow 进行记录；Shin 等[13]提出了一种云环境下的 SDN 流量监控方法 CloudWatcher，将网络流量自动导入相应的安全设备，以实现必要的网络分组检查。然而利用 SDN 将流量重定向到安全设备实现数据来源验证复杂，需要综合考虑安全设备的位置、不同安全设备的协作水平和 SDN 流量控制的粒度等多方面因素。其中主要是 SDN 流量控制粒度，但目前 SDN 支持的匹配字段仅限于网络前 4 层中一些常用的协议，控制粒度有限[14]。当安全设备检测出攻击者的分组特征，由于攻击者伪造的分组与合法分组的头部前 4 层一样，SDN 不能区分攻击者与合法者的分组，若将符合攻击者分组特征的分组全部丢弃或交由安全设备筛选都会影响合法者分组的正常传输。因此，目前缺乏一种实用数据来源验证机制且 SDN 控制粒度有限。

为解决上述问题，将密码标识引入 SDN，提出一种基于密码标识的 SDN 安全控制转发方法，利用密码标识的 3 个属性确保数据流在 SDN 中安全控制转发。其主要有 3 个方面贡献。1) 根据用户身份、文件属性或业务内容等特征信息生成密码标识，基于密码标识定义网络行为，形成基于人、物、业务流等细粒度网络控管能力。2) 使用 SDN 交换机验证数据来源，确保上传给 SDN 控制器的分组都是真实的，减少控制器遭受 DDoS 攻击的概率。3) 在网络的入口与出口验证基于密码标识的签名，确保目的设备收到的都是真实且未篡改的分组。

3 基于密码标识的 SDN 安全控制转发方法

3.1 基本原理

针对匹配域范围有限、不能满足网络业务精确控制的需求和转发设备流表匹配时缺乏有效的数据来源验证机制等问题，为确保数据的真实性，满足网络业务精确控制需求，提出基于密码标识的 SDN 安全控制转发方法，利用密码标识的 3 个属性来保证数据流的安全控制转发。密码标识的 3 个属性分别指身份属性、标签属性和密码属性。身份属性指密码标识与重要对象的身份绑定，可通过密码标识验证其身份，利用该属性，根据用户、设备、文件等重要对象的特征信息设计密码标识；标签属性指可根据密码标识进行数据转发，利用该属性，将密码标识作为转发设备能识别的匹配项，基于密码标识定义网络转发行为；密码属性指可通过密码标识鉴别数据真实性，利用该属性，在数据分组进出网络时验证密码标识，确保用户的不可否认性和数据的真实性。3 种属性相辅相成，共同构建基于密码标识控制网络的安全防护体系。

3.2 体系结构

如图 1 所示，该体系结构由密码标识和密钥管

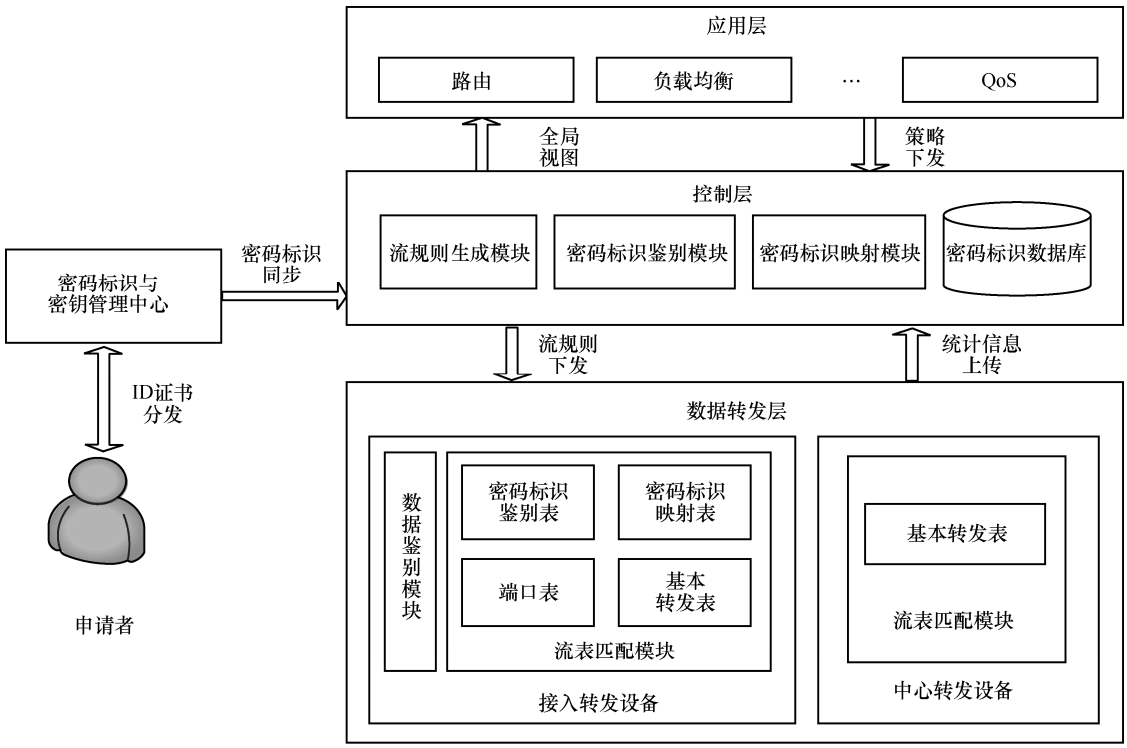


图 1　体系结构

理中心、应用层、控制层和数据转发层 4 个部分组成。在密码标识和密钥管理中心的支持下，上层应用可根据密码标识制订控制策略，控制层中的控制器将控制策略编译为流规则并下发给数据转发层中的转发设备，转发设备根据收到的流规则进行匹配和转发数据流，从应用层、控制层和数据层全方位进行网络流的安全控制，从而实现粒度更细的安全控制转发。

3.2.1　密码标识和密钥管理中心

负责密码标识和密钥的管理工作，主要是审核申请者身份、管理密码标识、根据密码标识生成公私钥对和制作并分发 ID 证书。同时，将新生成、刚更新、刚注销的密码标识同步到控制器的密码标识数据库中。其中，ID 证书包括密码标识、私钥、有效期和安全域等信息。

3.2.2　基于密码标识的控制层

控制层中的控制器是整个网络逻辑控制的核心，通过收集整个网络的信息资源形成全网拓扑，同时通过南向通道实现对转发设备的管控和配置。控制器的主要功能模块有密码标识鉴别模块、密码标识映射模块、流规则生成模块、密码标识数据库等。重点研究密码标识鉴别模块和密码标识映射模块。

密码标识鉴别模块主要负责鉴别密码标识的有效性。通过与密码标识数据库交互，建立密码标识黑名单，并通过查询未匹配的密码标识是否处于黑名单中判断其有效性，防止失效的密码标识进出网络。

密码标识映射模块通过随机散列算法建立密码标识映射表，并在数据分组进出网络时通过查询密码标识映射表对密码标识进行映射与逆映射。密码标识映射与逆映射的相互转换，实现密码标识的透明传输，防止其成为网络攻击的靶子。

密码标识数据库负责存储全网密码标识信息。

流规则生成模块主要负责控制策略编译成流规则并下发给底层的转发设备。

3.2.3　基于密码标识的数据转发层

数据转发层主要由转发设备组成，可分为接入转发设备和中心转发设备，其中，接入转发设备指位于骨干网与接入网之间的转发设备，中心转发设备指位于骨干网中的转发设备。

接入转发设备主要由数据鉴别模块和流表匹配模块 2 个部分组成。数据鉴别模块通过验证密码标识的签名鉴别数据真实性，防止非法的数据分组

进出网络；流表匹配模块通过流表匹配的方式验证密码标识有效性，完成密码标识映射与逆映射的相互转换，将合法的数据流转发到指定位置。

中心转发设备只有流表匹配模块，且该模块直接匹配和转发收到数据流。

以用户 U 访问服务器 B_1 为例，分析在该方法下的网络通信过程，如图 2 所示。其中，用户 U 默认为已收到 ID 证书。

1) 对用户 U 的数据分组打上密码标识并用其私钥签名，然后转发给接入转发设备 S_1。

2) 接入转发设备 S_1 收到用户 U 的数据分组后，通过数据鉴别模块验证数据分组真实性，通过流表匹配模块鉴别密码标识有效性，进行密码标识映射，最后，匹配与转发该数据分组，其中，密码标识在骨干网中将以映射值的形式传递。

3) 中心转发设备收到数据分组后，直接进行匹配与转发。

4) 接入转发设备 S_n 收到数据分组后，通过流表匹配模块进行密码标识逆映射，将密码标识映射值还原成初始值，通过数据鉴别模块验证密码标识的真实性，最后，匹配与转发该数据分组到目的终端。

3.3 实现方案

由于组合公钥密码体制（CPK, combined public key cryptosystem）具有密钥产生规模化、计算速度快、认证效率高、认证流程相对简单等特点，采用 CPK v8.0[15]设计密码标识和密钥管理中心，为申请者分配密码标识，根据密码标识生成相应的公私钥对；当数据分组进出网络时，设计数据鉴别模块验证基于密码标识的签名，确保终端用户的不可否认性和数据分组的真实性；将密码标识设计为转发设备能识别的匹配项，并结合 SDN 流表匹配特点，重新设计流表匹配模块，通过流表匹配的方式鉴别密码标识的有效性，在数据分组进入网络时将密码标识转换成其映射值，在数据分组离开网络时将密码标识还原成初始值，实现密码标识透明传输，如果流表匹配失败，交由控制器处理。

3.3.1 密码标识和密钥管理

密码标识和密钥管理中心负责管理密码标识，结合 CPK v8.0，根据密码标识生成相应的公私钥

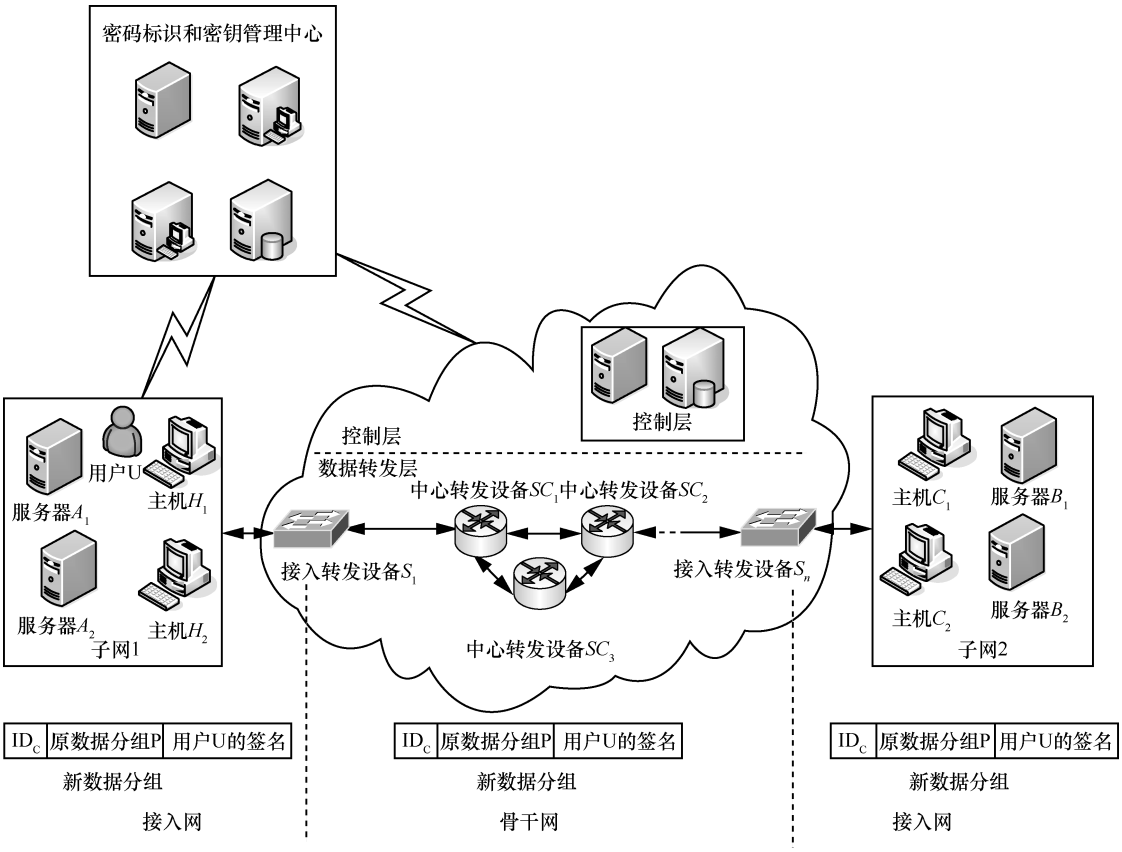


图 2 基于密码标识的 SDN 通信流程

对，生成与分发 ID 证书。

1) 管理密码标识

密码标识的管理是指密码标识生成、更新和注销全周期的管理。其中，密码标识是根据用户的身份、文件的属性或业务的内容等特征信息生成，包括编号、申请人姓名、特征信息、安全域、有效期等内容；密码标识的更新是指更新密码标识中除了特征信息以外的其他内容，如角色、安全域、有效期等；密码标识的注销是指将密码标识中所有内容注销。同时，将新生成、刚更新、刚注销密码标识信息同步到控制器的密码标识数据库中。

2) 生成组合密钥

基于椭圆曲线上离散对数难题的数学原理构建公私钥矩阵，采用散列函数与密码变换将密码标识映射为矩阵的行坐标与列坐标序列，选取并组合矩阵中元素，生成数量巨大的公私钥对。具体步骤如下。

步骤 1　构建组合矩阵。在给定椭圆曲线参数 (a,b,G,n,p) 的基础上，由密码标识和密码管理中心构建组合矩阵，可分为私钥矩阵和公钥矩阵，矩阵大小为 32×32。私钥矩阵由互不相同的小于 n 的随机数构成，矩阵中的元素标记为 $r_{i,j}$，私钥矩阵记为 ***SSK***，由密码标识和密钥管理中心保有，用于私钥的生成，是秘密变量。

$$\boldsymbol{SSK}=\begin{bmatrix} r_{1,1} & r_{1,2} & \cdots & r_{1,32} \\ r_{2,1} & r_{2,2} & \cdots & r_{2,32} \\ \vdots & \vdots & \ddots & \vdots \\ r_{32,1} & r_{32,2} & \cdots & r_{32,32} \end{bmatrix} \tag{1}$$

公钥矩阵由私钥矩阵派生，即 $r_{i,j}G=(x_{i,j},y_{i,j})=R_{i,j}$，公钥矩阵记为 ***PSK***，是公开变量，公钥矩阵分发到每一个实体，用于公钥的计算。

$$\boldsymbol{PSK}=\begin{bmatrix} R_{1,1} & R_{1,2} & \cdots & R_{1,32} \\ R_{2,1} & R_{2,2} & \cdots & R_{2,32} \\ \vdots & \vdots & \ddots & \vdots \\ R_{32,1} & R_{32,2} & \cdots & R_{32,32} \end{bmatrix} \tag{2}$$

步骤 2　密码标识到矩阵坐标的映射。该映射是由 *YS* 序列指示的，*YS* 序列是用户 U 的密码标识 ID_{U} 在映射密钥 *HKey* 下经散列变换的输出，$YS=Hash_{Hkey}(ID_{\mathrm{U}})=w_0,w_1,w_2,\cdots,w_{35}$，将 $w_0\cdots w_{35}$ 分为 4 组，分别以 $w_{00}\cdots w_{08}$、$w_{10}\cdots w_{18}$、$w_{20}\cdots w_{28}$、$w_{30}\cdots w_{38}$ 标记。其中 $w_{00},w_{10},w_{20},w_{30}$ 的字长为 6 bit，分别指示置换序号（3 bit）和置换起点（3 bit）。$w_{i,j}(i=0\cdots3,j=1\cdots8)$ 指示组合矩阵 ***A*** 的行坐标，$w_{i,j}$ 的字长为 5 bit。组合矩阵 ***A*** 的 32 列分 4 组，分别经过置换变换。置换表的大小是 8×8，属秘密，其中置换表的列为置换序号，行为置换起点。

步骤 3　组合密钥的计算。组合私钥的计算在密码标识和密钥管理中心中进行，设第 i 组经置换后的列坐标用 $t_{i,j}$ 表示 $(i=0,\cdots,3,j=1,\cdots,8)$。密码标识的组合私钥 *csk* 为

$$csk=\sum_{i=0}^{3}\sum_{j=1}^{8}r_{|w_{i,j},t_{i,j}|}\bmod n \tag{3}$$

密码标识的组合公钥 *CPK* 由各网络实体自行计算为

$$CPK=\sum_{i=0}^{3}\sum_{j=1}^{8}R_{|w_{i,j},t_{i,j}|}\bmod n \tag{4}$$

3) ID 证书的生成与分发

密码标识和密钥管理中心将密码标识、私钥、公钥查询函数、有效期、配置信息等内容制成 ID 证书，通过安全信道或媒介发送给申请者。

3.3.2　数据真实性鉴别

数据鉴别模块通过验证数据分组中的签名，检验数据分组的真实性和完整性，防止伪造或遭篡改的数据分组进出网络，从网络攻击的源头入手，限制网络安全风险范围。具体的处理流程如图 3 所示。

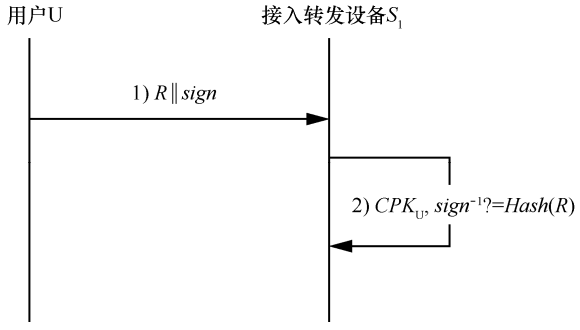


图 3　数据鉴别模块的处理流程

1) $\mathrm{U}\rightarrow S_1:R\|sign$，用户 U 发送数据分组给接入转发设备 S_1；其中，$R=\{ID_{\mathrm{U}},r,P\}$，$sign=E_{csk_{\mathrm{U}}}[Hash(R)]$，$ID_{\mathrm{U}}$ 为用户 U 的密码标识，P 为初始数据分组，r 为随机数，*sign* 为用户 U 用其私钥 csk_{U} 对 R 签名。

2) $S_1:CPK_{\mathrm{U}},sign^{-1}?=Hash(R)$。接入转发设备 S_1 验证用户 U 的身份，验证过程如下：S_1 首先验

证随机数 r 的新鲜性，使用公钥查询函数 φ 查询用户 U 的公钥,即 $CPK_{\mathrm{U}}=\varphi(ID_{\mathrm{U}})$，然后对用户 U 的签名进行验证，即 $sign^{-1}=E_{CPK_{\mathrm{U}}}[sign]$，若 $sign^{-1}=Hash(R)$，表明数据分组真实且未被篡改，否则，验证失败，丢弃该数据分组。

3.3.3 基于密码标识的流表匹配

将密码标识设计为流表匹配模块能识别的匹配项，增加一个转换动作用于密码标识的映射与逆映射，并基于多级流表设计了多级流表流水线处理流程，可通过流表匹配的方式鉴别密码标识的有效性，完成密码标识的映射与逆映射的相互转换，将合法的数据流转发到指定位置。

1) 流规则的基本结构

结合 OpenFlow v1.3 协议，采用 TLV 格式，将匹配域中实验字段 OFPXMC_EXPERIMENTER 扩展为密码标识 ID；修改 OpenFlow 协议中 Flow-Mod 消息体，使匹配域包含密码标识 ID 的流规则可被接入转发设备和中心转发设备识别并无排斥的插入在相应流表中。然后自定义新动作——转换，作用是将密码标识转换为映射值，或将密码标识映射值转换为原始值；修改 OpenFlow 协议中 Flow-Mod 消息体，使接入转发设备能够解析该动作并写入动作库。因此，本文使用南向协议是兼容 OpenFlow1.3 协议，支持现有的 OpenFlow1.3 协议的控制器可以与接入转发设备和中心转发设备正常通信，但该控制器不能下发匹配域包含密码标识 ID 的流规则。通过将密码标识 ID 自定义新的匹配项，添加一个转换动作，形成新的流规则结构，具体如图 4 所示。

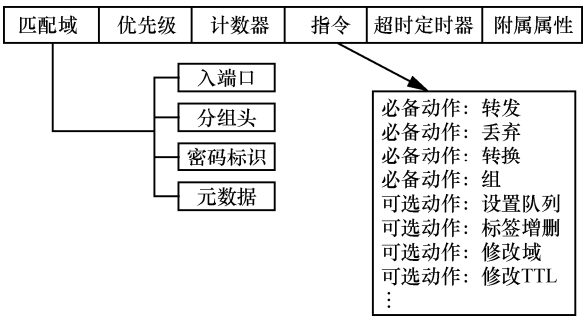
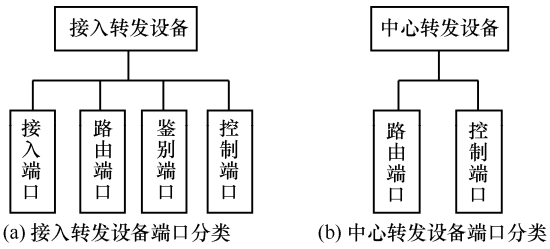


图 4 流规则结构

2) 端口分类

接入转发设备是数据流进出网络的门户，当数据流到达接入转发设备时，共有 3 种流向：1) 从源终端接收后直接转发到目的终端；2) 从源终端接收后再转发到网络中；3) 从网络中接收后再转发到目的终端。不同流向的数据流其流表匹配方式存在差异，如从源终端接收的数据流无须进行密码标识映射直接转发到目的终端。为识别不同数据流的流向，对端口分类，如图 5 所示。



(a) 接入转发设备端口分类 (b) 中心转发设备端口分类

图 5 转发设备的端口分类

接入转发设备的端口主要分为接入端口、路由端口、鉴别端口和控制端口，其中，接入端口指与终端相连的端口，路由端口指与转发设备相连的端口，鉴别端口指与数据鉴别模块相连的端口，控制端口指与控制器相连的端口。而中心转发设备的端口主要分为路由端口和控制端口。因此，数据流的不同流向可通过端口来描述，共有 3 种类型：① 从接入端口进从接入端口出；② 从接入端口进从路由端口出；③ 从路由端口进从接入端口出。类型①对应从源终端接收后直接转发到目的终端；类型②对应从源终端接收后再转发到网络中；类型③对应从网络中接收后再转发到目的终端。

转发设备在与控制器开始建立连接时，通过 OFPT_MULTIPART_REPLY 向控制器发送端口分类信息，如哪些端口属于接入端口，哪些端口属于路由端口，哪些端口属于鉴别端口等，方便控制器识别不同数据流向，正确下发流规则。当端口分类信息发生变化，转发设备通过 OFPT_PORT_MOD 主动向控制器报告端口分类变更情况。

3) 多级流表流水线处理

由于不同流向的数据流处理方式存在差异，基于多级流表提出多级流表流水线处理流程，根据入端口的类型为不同流向的数据流选择合适的处理方式，通过流表匹配的方式鉴别密码标识的有效性，通过流表匹配的方式实现密码标识的透明传输，若流表匹配失败，交由控制器处理。

如图 6 所示，将接入转发设备的多级流表分为端口表、密码标识鉴别表、密码标识映射表和基本转发表 4 类。端口表根据入端口的类型决定数据流的处理方式，其中，入端口类型包括接入端口、鉴别端口、路由端口 3 种类型；密码标识鉴别流表用于鉴别密码

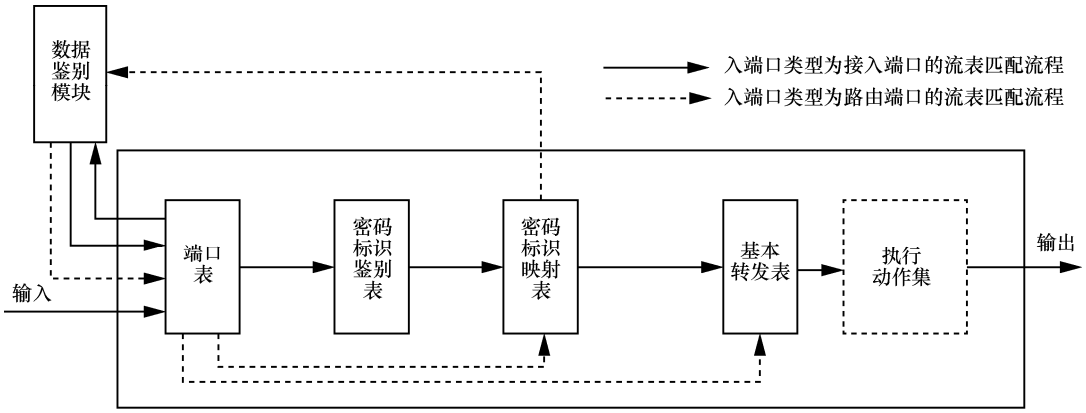


图 6　多级流表流水线处理流程

标识的有效性，其匹配项为失效的密码标识，若匹配成功表明该密码标识已失效；密码标识映射流表用于密码标识的映射和逆映射；基本转发流表用于匹配转发收到的数据流。具体流程如图 7 所示。

流表匹配模块收到数据流后，首先匹配端口表，根据入端口类型决定数据流的处理方式。若入端口类型为接入端口，其流表匹配处理过程如下。

① 将元数据设置为 01，再将数据流转发到数据鉴别模块进行密码标识真实性鉴别。

② 数据鉴别模块将通过鉴别的数据流返回给流表匹配模块。

③ 再次匹配端口表，若匹配项为鉴别端口且元数据为 01，将该数据流转发到密码标识鉴别表。

④ 匹配密码标识鉴别表。若匹配成功，丢弃该类型的数据流，表明其携带的密码标识已失效，否则，转发到密码标识映射流表。

⑤ 匹配密码标识映射表。若匹配成功，按指令对该数据流进行相应的处理，若指令为直接转发到基本转发表，表明该数据流的流向是从接入端口进从接入端口出，若指令为将密码标识转化为映射值，再转发到基本转发流表，表明该数据流的流向是从接入端口进从路由端口出；若匹配失败，将该数据流的首包封装到 Packet-In 再交由到控制器处理。

⑥ 匹配基本转发表，按匹配成功的指令进行相应的处理。

⑦ 控制器收到未匹配的数据分组后，会根据处理结果会下发相应的流规则指示接入转发设备如何对其进行处理。

若入端口类型为路由端口，表明该数据流的流向是从路由端口进从接入端口出，其数据分组处理过程如下。

① 将元数据设置为 10，再将数据流转发到密码标识映射表。

② 匹配密码标识映射表，根据匹配结果进行相应的密码标识逆映射，再将数据流转发到数据鉴别模块进行密码标识真实性鉴别。

③ 数据鉴别模块将通过鉴别的数据流返回给流表匹配模块。

④ 再次匹配端口表，根据匹配项为入端口类型为鉴别端口且元数据为 10，将该数据流转发到基本转发表。

⑤ 匹配基本转发表，按匹配成功的指令对该数据流进行相应的处理。

中心转发设备的流表匹配模块与一般的 SDN 交换机的匹配方式相似，直接进行匹配转发即可，这里不再赘述。

3.3.4　控制器流规则生成

在流表匹配过程中，控制器负责处理未匹配成功的数据流，通过密码标识鉴别模块鉴别标识的有效性，通过密码标识映射模块将密码标识进行转换，通过流规则生成模块为其生成相应的流规则，并下发到相关的转发设备中。

1) 密码标识鉴别模块

为防止失效的密码标识进入网络，在控制器中开发密码标识鉴别模块，通过与密码标识数据库进行交互，将失效的密码标识放入黑名单，监听密码标识数据库更新，并随时更新黑名单内容。通过检验密码标识是否处于黑名单来判断其有效性，若处于黑名单中，通知流规则生成模块下发相应的流规则拒绝所有带有该密码标识的数据流进入网络，否则交由密码标识映射模块做进一步处理。

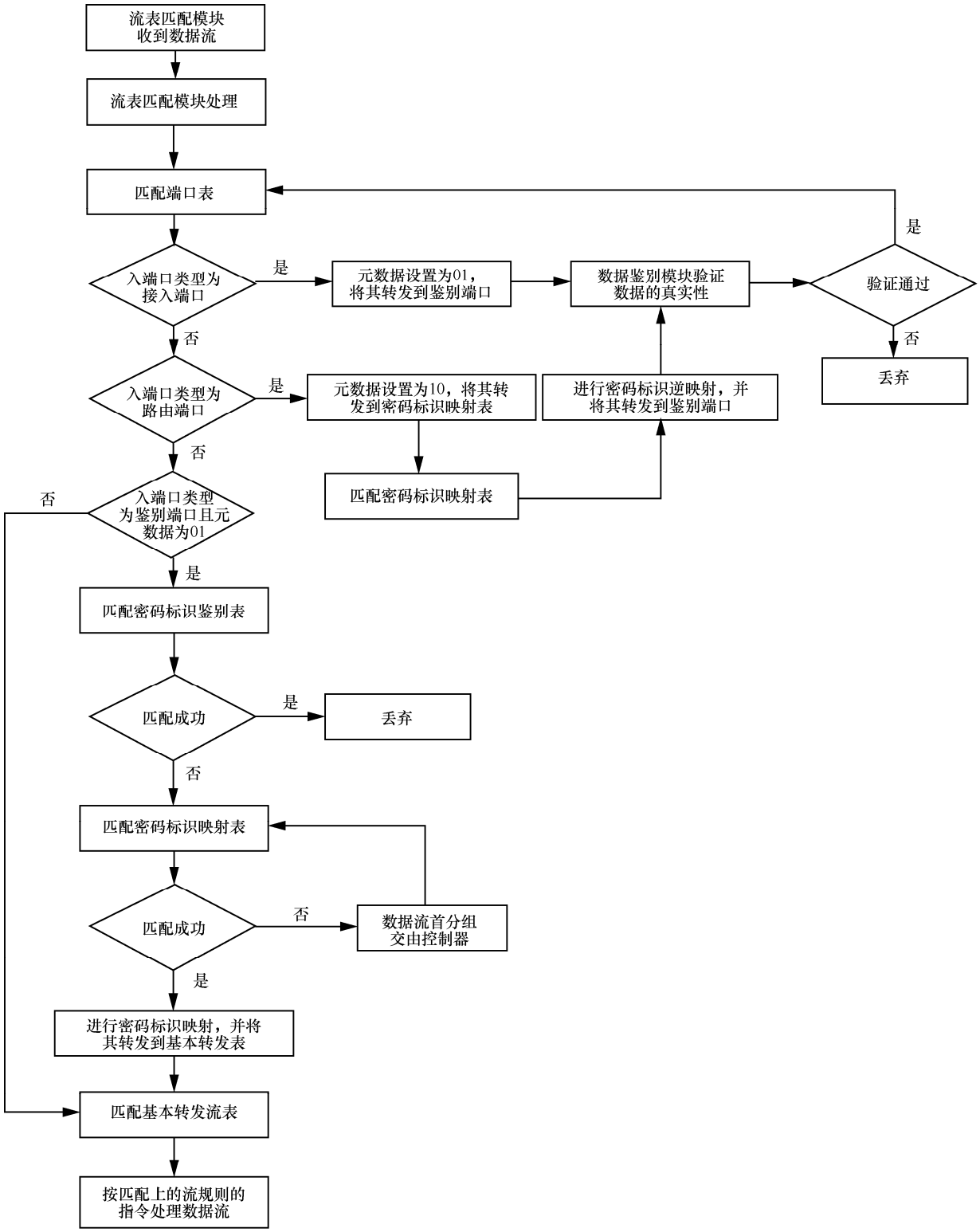


图 7　流表匹配的处理流程

2) 密码标识映射模块

为实现密码标识的透明传输，防止其成为网络攻击的靶子，在控制器中开发密码标识映射模块，通过随机散列算法建立密码标识映射表，为密码标识查找其映射值，若查找失败，该模块为其生成映射值，同时存储该映射关系，方便再次处理相同的密码标识。

3) 流规则生成模块

流规则生成模块主要将控制策略转化为转发设

备能识别的流规则并下发给相应的转发设备，其下发的流规则分为预置流规则和实时流规则。

端口表中的流规则为预置流规则，当控制器收集完端口分类信息后，该模块根据入端口类型主动下发流规则到各接入转发设备的端口表中，决定数据流处理方式。

密码标识鉴别表中的流规则为实时流规则，该模块根据密码标识鉴别模块提供的密码标识失效策略下发流规则到指定接入转发设备的密码标识鉴别表中。

密码标识映射表中的流规则为实时流规则，该模块根据密码标识映射模块提供的密码标识映射与逆映射策略和数据流的流向下发相应的流规则到指定接入转发设备的密码标识映射表中。针对不同的数据流向，设计映射选择算法决定下发何种类型映射流规则。具体步骤如算法 1 所示。

算法 1　映射选择算法

输入　接入转发设备 S，由接入转发设备 S 上传的未匹配分组 P

输出　映射流规则 R

1) if $P.in\_port \in access\ port$ && $P.out\_port \in access\ port$

2)　生成动作为直接转发到基本转发表的流规则 R

3) if $P.in\_port \in access\ port$ && $P.out\_port \in route\ port$

4)　生成动作为密码标识映射并转发到基本转发表的流规则 R

5) else

6)　生成动作为密码标识逆映射并转发到数据鉴别模块的流规则 R

7)下发流规则 R 到接入转发设备 S

基本转发表中的流规则为实时流规则，该模块调用全网视图（拓扑视图和资源视图）和结合应用层下发的相应控制策略最优化选取源地址到目的地址的路径，并下发流规则到指定转发设备的基本转发表中。

4　仿真实验与分析

4.1　实验环境

实验分别使用 6 台配置为 i7-7700 CPU，16 GB 内存，8 网卡的联想 A8800t 搭载 OpenDaylight 控制器和 Open vSwitch（简称 OVS），8 台扬天 M4000e 作为终端主机。实验拓扑如图 8 所示，OVS e1~e2 充当接入转发设备，OVS a1~a3 充当中心转发设备，h1~h8 充当终端主机。

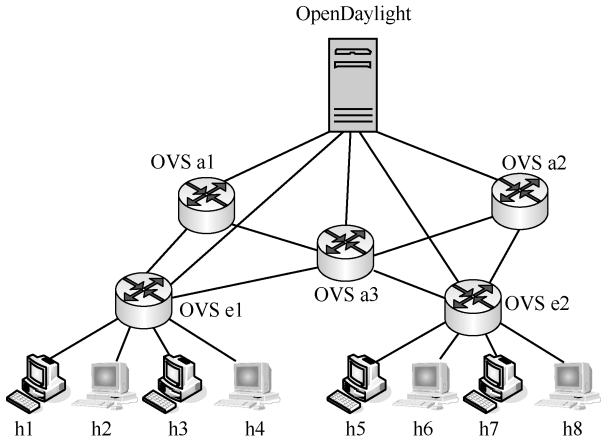


图 8　实验拓扑

4.2　有效性验证

为验证所提方法的有效性，设计了 3 个实验。实验 1 用于验证该方法能否鉴别密码标识的真实性和有效性以及密码标识映射转换情况，实验 2 用来验证该方法能否基于密码标识定义网络转发行为，实验 3 用来验证映射选择算法的有效性。

4.2.1　不同数据分组访问网络

在主机 h1 上模拟携带有效的密码标识及签名的数据流，在主机 h2 上模拟携带失效的密码标识及签名的数据流，在主机 h3 上模拟不携带密码标识及签名的数据流，在主机 h4 上模拟携带有效的密码标识但被篡改的数据流，4 台主机上的数据分组发送速率都为 50 个/秒，持续向 h8 发送数据分组，并规定转发路径为 $h1 \to h4 \to e1 \to a1 \to a3 \to a2 \to e2 \to h8$，使用 sFlow 监测 e1 和 a1 数据分组的到达情况，重复 10 次，每次持续时间为 10 s，把 10 次实验数据作平均，测试结果如图 9 所示。

从图 9 可知，OVS e1 数据分组到达数目约为 OVS a1 的 4 倍，同时通过查看 e1、e2 和 a1 中流规则的情况发现：1) e1 中增加了 2 条流规则，一是将 h2 的数据分组丢弃，另一个是将 h1 的数据分组的密码标识进行转换；2) a1 中无密码标识相关的流规则；3) e2 中增加了一条流规则，内容为将 e1 中转换的密码标识还原成初始值，然后，使用 wireshark 在 OVS a1 抓取分组得出绝大多数 IP 分组来源于 h1，原因在于接入转发设备能够识别密码标识是否失效，通过流表匹配将失效的密码标识丢弃，将有

效的密码标识进行转换并在数据分组到达目的地址前将转换的密码标识还原成初始值，同时接入转发设备还能拒绝未携带密码标识或遭到篡改的数据分组进入网络。

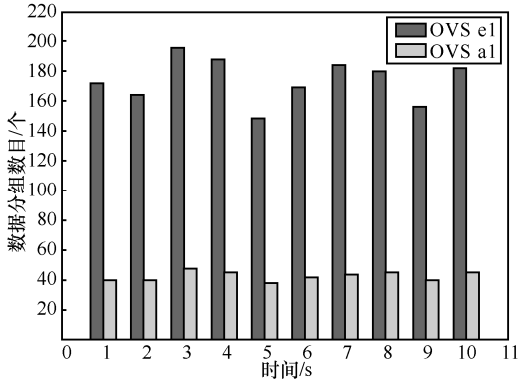


图 9 接入转发设备 e1 的数据分组到达统计

4.2.2 基于密码标识的控制转发

在主机 h1 上模拟携带不同密码标识及签名的数据流，分别是用户 A、用户 B 和用户 C 的有效的密码标识，不同类型的数据分组发送速率都为 50 个/秒，并持续向 h8 发送数据分组，并规定转发路径为 $h1 \rightarrow e1 \rightarrow a1 \rightarrow a3 \rightarrow a2 \rightarrow e2 \rightarrow h8$。使用控制器对 a3 下发 3 条流规则。1) 将携带用户 A 的密码标识的数据分组丢弃；2) 将携带用户 B 的密码标识的数据分组转发到 a2；3) 将携带用户 C 的密码标识的数据分组转发到 e2。使用 sFlow 监测 a3 端口流量情况。重复 10 次，每次持续时间为 10 s，把 10 次实验数据作平均，测试结果如图 10 所示。

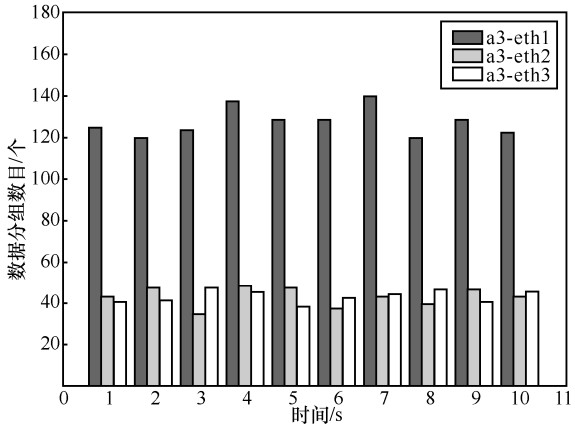


图 10 中心转发设备 a3 的端口流量统计

从图 10 可知，a3-eth2 和 a3-eth3 端口流量大致相同，a3-eth1 端口流量约为 a3-eth2 和 a1-eth3 的 3 倍。然后，通过查看端口连接情况，得知：1) a3-eth1 与 a1 相连；2) a3-eth2 与 a2 相连；3) a3-eth3 与 e2 相连。再通过 wireshark 在 a2 和 e2 上进行分组抓取，得知：1) a2 收到数据分组携带用户 B 的密码标识；2) e2 收到数据分组携带用户 C 的密码标识。原因在于，密码标识与用户的身份绑定，控制器可基于密码标识为不同的用户制定不同的转发策略。

4.2.3 映射选择算法有效性验证

为验证接入转发是否能根据数据流的流向选择不同的处理方式，通过 h1 ping h2 模拟流向为从接入端口进、从接入端口出的数据流，通过 h1 ping h8 模拟流向为从接入端口进、从路由端口出和从路由端口进、从接入端口出的数据流。

分别查看 e1 和 e2 的流规则，得到：1) 当 h1 ping h2 时，e1 中映射流规则为跳转到下级流表，数据流进出 e1 前后密码标识无变化；2) 当 h1 ping h8 时，e1 中的映射流规则是对密码标识进行转换再跳转到下级流表；通过 wireshark 进行分组抓取，得到数据流经过 e1 时密码标识从 ID_U 变成 ID_u，经过 e2 时密码标识从 ID_u 变成 ID_U，原因在于控制器通过映射选择算法识别了数据流的流向，并根据流向下发相应的映射流规则。

4.3 性能分析

通过实验分析转发设备的处理时延与控制器的 CPU 利用率，计算增加的相关模块对转发设备和控制器的影响。

4.3.1 转发设备的处理时延

在主机 h1 和 h2 上分别使用 hping3 向网络持续注入合法的数据分组，数据分组发送速率分别为 50 Mbit/s、100 Mbit/s、150 Mbit/s、200 Mbit/s、250 Mbit/s、300 Mbit/s、350 Mbit/s、400 Mbit/s、450 Mbit/s、500 Mbit/s，数据分组的源地址、目的地址、源端口、目的端口均不重复（通过 hping3 命令参数设置）。在不同场景下，分别测试接入转发设备、中心转发设备和正常的 OVS 在不同数据分组发送速率的处理时延，重复 10 次，每次实验取最高结果，再把 10 次实验数据取平均，实验结果如图 11 所示。其中，各转发设备都已预置了相关流规则可直接匹配转发。

从图 11 可知，中心转发设备与一般的 OVS 处理时延基本一致，而接入转发设备的处理时延比前两者稍大，三者的处理时延都随流量的增加而增大，且随着流量的增加，接入转发设备的处理时延增速持续上升。原因在于在不考虑控制处理

未匹配数据流的时延，后两者的处理时延只包含数据流直接匹配转发的时延，因此，它们的处理时延基本一致，而接入转发设备的时延 $T_{\text{Access}}=T_{\text{verify}}+T_{\text{validity}}+T_{\text{map}}+T_{\text{match}}$，$T_{\text{verify}}$ 表示数据鉴别模块验证的时延，T_{validity} 表示密码标识有效性鉴别的时延，T_{map} 表示密码标识映射的时延，T_{match} 表示数据流直接匹配转发的时延，四者都随数据流量的增加而增大。在相同条件下，接入转发设备比后两者都多 $(T_{\text{verify}}+T_{\text{validity}}+T_{\text{map}})$，故随数据流量的增加，时延差距逐渐加大。但是在数据分组数目可控的情况下接入转发设备的时延是在可接受范围内的。

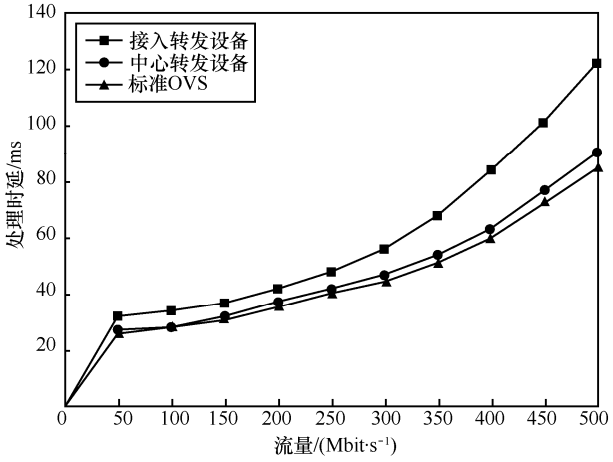


图 11　转发设备的处理时延

4.3.2　控制器的 CPU 利用率

测试多种情况下原版 OpenDaylight 控制器和二次开发的 OpenDaylight 控制器在 CPU 利用率上的差异，在主机 h1 上使用 hping3 向网络持续注入合法的数据分组，数据分组的源地址、目的地址、源端口、目的端口均不重复（通过 hping3 命令参数设置）。每种情形进行了 10 次重复实验，每次实验取最高结果，再把 10 次实验数据取平均，测试结果如图 12 所示。

由图 12 可知，在不同情形下实验使用的 OpenDaylight 控制器的 CPU 占用率比原版 OpenDaylight 控制器略高，但两者差异不是很大，在可接受的范围内。

5　结束语

针对匹配域范围有限、不能满足网络业务精确控制的需求和转发设备流表匹配时缺乏有效的数据来源验证方法等问题，融合软件定义网络和网络空间密码标识技术，利用密码标识的 3 个属性，设计基于密码标识的 SDN 安全控制转发方法，在数据流进出网络时对其来源进行验证，限制网络安全风险范围，根据密码标识定义网络转发行为，能够对网络进行灵活的动态规划和管理，形成基于人、物、业务流等细粒度网络管控能力。未来的工作将研究基于密码标识的控制策略的快速编译与执行问题，进一步验证所提方法的可扩展性。

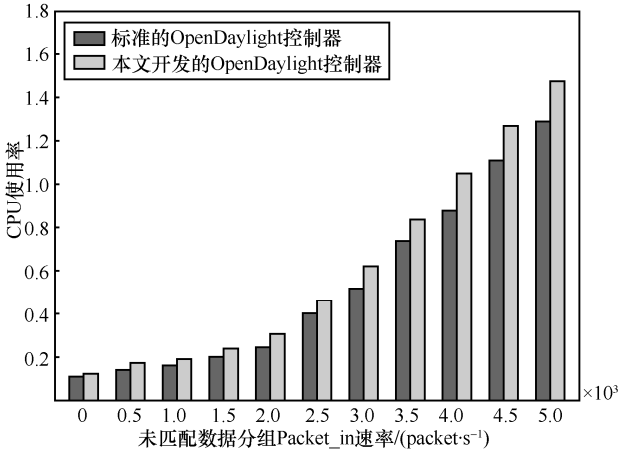


图 12　控制器的 CPU 占用率

参考文献：

[1] MCKEOWN N. Software-defined networking[C]//IEEE International Conference on Computer Communications. 2009: 30-32.

[2] 左青云, 陈鸣, 赵广松, 等.基于 OpenFlow 的 SDN 技术研究[J].软件学报,2013(5):1078-1097.
ZUO Q Y, CHEN M, ZHAO G S, et al. Research on OpenFlow-based SDN technologies[J]. Journal of Software, 2013(5):1078-1097.

[3] 王蒙蒙, 刘建伟, 陈杰, 等. 软件定义网络:安全模型、机制及研究进展[J].软件学报,2016,27(4):969-992.
WANG M M, LIU J W, CHEN J, et al. Software defined networking: security model, threats and mechanism[J]. Journal of Software, 2016, 27(4): 969-992.

[4] LIU H H, WU X, ZHANG M, et al. zUpdate: updating data center networks with zero loss[J]. Computer Communication Review, 2013, 43(4):411-422.

[5] LI D, SHANG Y, CHEN C. Software defined green data center network with exclusive routing[C]//INFOCOM. 2014:1743-1751.

[6] DHAWAN M, PODDAR R, MAHAJAN K, et al. SPHINX: detecting security attacks in software-defined networks[C]//Network and Distributed System Security Symposium. 2015:1-15.

[7] 王首一, 李琦, 张云. 轻量级的软件定义网络数据分组转发验证[J].

计算机学报,2017,40(7):9-26.
WANG S Y, LI Q, ZHANG Y. Lightweight packet forwarding verification in SDN[J]. Journal of Computers. 2017,40(7):9-26.

[8] YAO G, BI J, XIAO P. Source address validation solution with OpenFlow/NOX architecture[C]//IEEE International Conference on Network Protocols. 2011:7-12.

[9] CASADO M, FREEDMAN M J, PETTIT J, et al. Ethane: taking control of the enterprise[C]//ACM SIGCOMM Conference on Applications. 2007:1-12.

[10] SHIN S, PORRAS P, YEGNESWARAN V, et al. FRESCO: modular composable security services for software-defined networks[C]//Network & Distributed Security Symposium, 2013.

[11] BALLARD J R, RAE I, AKELLA A. Extensible and scalable network monitoring using OpenSAFE[C]//Internet Network Management Conference on Research on Enterprise Networking. 2010:8.

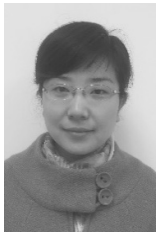
[12] WUNDSAM A, LEVIN D, SEETHARAMAN S, et al. OFRewind: enabling record and replay troubleshooting for networks[C]//Usenix Conference on Usenix Technical Conference. 2011:29.

[13] SHIN S, GU G. CloudWatcher: network security monitoring using OpenFlow in dynamic cloud networks [C]//IEEE International Conference on Network Protocols. 2012:1-6.

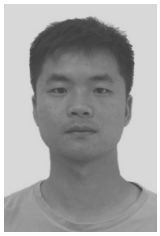
[14] 毕军.SDN 体系结构与未来网络体系结构创新环境[J]. 电信科学, 2013, 29(8):6-15.
BI J. SDN architecture and future network innovation environment[J]. Telecommunications Science, 2013, 29(8):6-15.

[15] 南湘浩.CPK 组合公钥体制(v8.0)[J].金融电子化,2013(3):39-41.
NAN X H. CPK combined public key cryptosystem(v8.0)[J]. Financial Electronics, 2013(3):39-41.

[作者简介]



秦晰（1978-），女，河南焦作人，博士，信息工程大学副教授、硕士生导师，主要研究方向为 SDN 安全、可信计算。



唐国栋（1992-），男，湖南永州人，信息工程大学硕士生，主要研究方向为 SDN 安全。

常朝稳（1966-），男，河南滑县人，博士，信息工程大学教授、博士生导师，主要研究方向为移动信息安全、物联网安全。