软件定义网络中基于密码标识的报文转发验证机制

秦 晰 唐国栋* 常朝稳 王瑞云

(信息工程大学 郑州 450001)

摘 要：针对软件定义网络(SDN)中缺乏安全高效的数据来源验证机制问题，该文提出基于密码标识的报文转发验证机制。首先，建立基于密码标识的报文转发验证模型，将密码标识作为IP报文进出网络的通行证。其次，设计SDN批量匿名认证协议，将SDN控制器的验证功能下放给SDN交换机，由SDN交换机进行用户身份验证和密码标识验证，快速过滤伪造、篡改等非法报文，提高SDN控制器统一认证与管理效率，同时可为用户提供条件隐私保护。提出基于密码标识的任意节点报文抽样验证方案，任何攻击者无法通过推断采样来绕过报文检测，确保报文的真实性的同时降低其处理延迟。最后，进行安全性分析和性能评估。结果表明该机制能快速检测报文伪造和篡改及抵抗ID分析攻击，但同时引入了大约9.6%的转发延迟和低于10%的通信开销。

关键词：软件定义网络；密码标识；数据来源验证；条件隐私性

中图分类号：TP393 **文献标识码**：A **文章编号**：1009-5896(2018)09-2042-08

DOI: 10.11999/JEIT171226

Packet Forwarding Authentication Mechanism Based on Cipher Identification in Software-defined Network

QIN Xi TANG Guodong CHANG Chaowen WANG Ruiyun

(*Information Engineering University*, *Zhengzhou* 450001, *China*)

Abstract: To deal with the lack of a secure and efficient data source authentication mechanism in Software-Defined Network (SDN), a packet forwarding authentication mechanism based on cipher identification is proposed. Firstly, a packet forwarding authentication model based on cipher identification is established, where the cipher identification is identified as a passport of IP packets entering and leaving the network. Secondly, the SDN batch anonymous authentication protocol is designed to decentralize the authentication function of the SDN controller to the SDN switch. The SDN switch performs user authentication and cipher identification verification, and quickly filters forgery, falsification, and other illegal packets to improve the unified authentication and management efficiency of the SDN controller, while providing users with the conditions of privacy protection. Thirdly, a scheme for sampling and verifying packets based on cipher identification in any node is proposed, where any attacker can not bypass the packet detection by inferring the sample, to ensure the authenticity of the packet while reducing its processing delay. Finally, safety analysis and performance evaluation are conducted. The results show that this mechanism can quickly detect packet falsification and tampering and resist ID analysis attacks, but at the same time it introduces about 9.6% forwarding delay and less than 10% communication overhead.

Key words: Software-Defined Network (SDN); Cipher identification; Data source authentication; Conditional privacy

1 引言

软件定义网络[1](Software-Defined Network, SDN)通过把传统封闭的网络体系解耦为数据平面、控制平面和应用平面，并为网络提供可编程的接口，从而革命性地改变了现有的网络架构[2,3]，使得网络能够像软件一样灵活、便捷，同时提高网络的创新能力。然而SDN的灵活机制导致对数据层攻击的防御变得非常复杂[4–6]，易遭受因报文伪造、篡改所引发的一系列攻击，同时此类攻击为恶意攻击者隐匿真实身份、逃避制裁提供温床，并由

收稿日期：2017-12-26；改回日期：2018-06-01；网络出版：2018-07-12
*通信作者： 唐国栋 tgdhooping@163.com
基金项目：国家自然科学基金(61572517)
Foundation Item: The National Natural Science Foundation of China (61572517)

此引发许多安全、管理和计费问题[7]，例如DoS/DDoS攻击、僵尸网络(Botnet)、垃圾流量(SPAM)等。

数据来源验证是指对IP报文(以下简称为报文)的来源进行验证，在报文未被篡改的情况下，确保该报文是由其声称的用户发送，并且该用户不能否认其行为。目前SDN网络中的已有一些解决方案。如Yao等人[8]提出VAVE安全框架，在控制器中嵌入源地址验证模块，通过计算路由路径并向路径上交换机动态下发相应流表项对报文进行过滤，实现敏捷灵活的源地址验证操作，但SDN控制器存在DDoS攻击风险；孙鹏[9]将源IP地址与底层不可变标识如MAC地址、端口号绑定，在交换机上形成(MAC地址，端口号，源IP地址)三元组流表的过滤规则，以达到源地址验证目的，但其没有提出自动快速更新三元组流表的方案。Liu等人[10]提出SDN-SAVI解决方案，在控制器中开发SAVI模块，通过侦听AAM包动态生成过滤规则，由SDN交换机验证数据来源，为防止攻击者伪造AAM包攻击控制器，限制AAM包上传速率。然而这些方案[8–10]中都是基于路径过滤机制，攻击者难以追踪。而现有基于密码的验证方案[11–13]通过签名或消息认证码来确保报文的真实性和用户的不可否认性，但签名带来较大的通信开销和计算开销，消息认证码只能由特定验证者进行验证，灵活性差。

为确保用户身份与网络行为一一对应，本文借鉴身份标识映射思想，将密码标识引入SDN网络，提出SDN中基于密码标识的报文转发验证机制。本文与一体化标识网络[14]、LISP[15]等身份标识映射方案的区别在于：后者强调的是身份与位置分离，主要解决IP语义过载问题，而本文设计的密码标识并不用于寻址，主要是为了确保数据源的真实性。

本文的主要贡献是：(1)提出基于密码标识的报文转发验证模型，将密码标识与用户身份绑定，确保每个报文都有责任人；(2)设计SDN批量匿名认证协议，通过SDN交换机辅助验证，提高SDN控制器认证与管理效率，确保用户条件隐私性；(3)引入随机检测模型，以较小的开销代价实现高效的转发验证。

2　机制描述

本文提出SDN中基于密码标识的报文转发验证模型，如图1所示，该模型由密码标识管理中心，用户U_i，带密码标识组件的源设备H_i和目的设备H_n, SDN交换机S_1, S_2, …, S_n和SDN控制器C组成。

密码标识管理中心(Cipher Identification Management Center, CIMC)主要负责管理网络使用授权，包括用户信息管理和用户密钥管理，如生成真实身份标识，合成用户部分密钥，设置上网限期等。

用户U_i负责管理和维护自身的网络使用授权信息，如真实身份标识，用户密钥，上网期限等。当其需要使用SDN网络时，向密码标识组件提供真实身份标识和用户密钥。

密码标识组件，负责用户接入认证和密码标识管理，如发起用户接入认证，协商共享密钥，生成密码标识，密码标识封装和解封装等。

SDN交换机在原有的SDN交换机的基础上，嵌入数据来源验证模块，通过流表匹配，选择合适的报文进行数据来源验证。

SDN控制器C负责用户统一认证与管理，如用户的有效性验证、密钥协商和选择合适的SDN交换机进行抽样验证等。

模型的安全性是基于以下假设：

(1)SDN网络为单SDN控制器网络，SDN数据平面到控制平面之间采用带外的组网方式；

(2)SDN控制器C是可信的，不会泄露用户的真实身份；

(3)使用TLS协议提供南向通道双向身份认证和密钥协商；

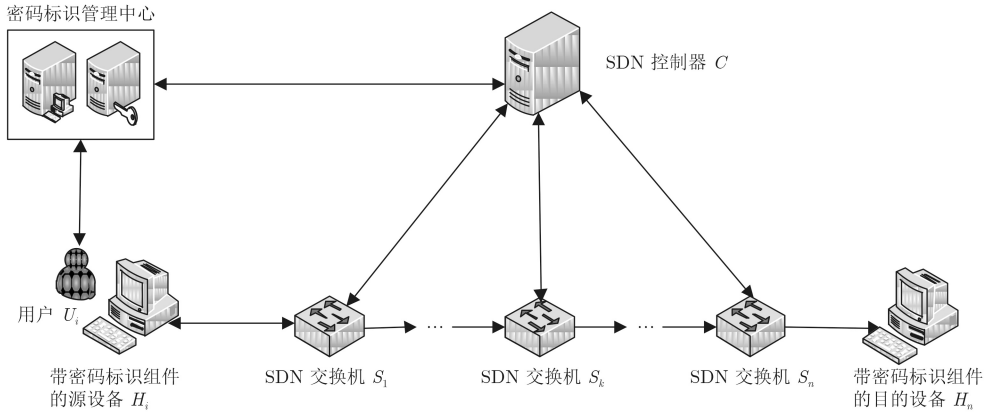

图 1 基于密码标识的报文转发验证模型

(4)SDN控制器C预置公私钥对(b,B)，其中$B=bP$, P是q阶循环加法群G的生成元。

2.1 生成身份基

定义1 身份基(Identity Base, IB)指基于无证书公钥密码体制，密码标识管理中心与用户U_i根据用户身份信息生成的四元组，即

$$\mathrm{IB}[i]=\{\mathrm{RID}_i,\mathrm{Lifetime}_i,\mathrm{pk}_i,\mathrm{sk}_i\} \tag{1}$$

其中，RID_i表示用户U_i的真实身份标识，$\mathrm{Lifetime}_i$表示用户U_i的上网期限，pk_i表示用户公钥，sk_i表示用户私钥。

SDN并不是对所有用户开放，需要用户向密码标识管理中心注册，申请网络使用授权，其中身份基是用户获得网络使用授权的凭证。

密码标识管理中心系统初始化是用户获得身份基的前提。密码标识管理中心选择一个安全参数$l\in Z^*$，满足$q>2^l$, G是q阶的循环加法群，P是G的生成元；选择随机数$s\in Z_q^*$作为系统主私钥，计算$P_{\mathrm{pub}}=sP$，作为系统公钥；分别定义5个散列函数：$H_0:\{0,1\}^*\to\{0,1\}^{64}$, $H_1:\{0,1\}^{64}\times G\to Z_q^*$, $H_2:\{0,1\}^{64}\times G\times G\to Z_q^*$, $H_3:\{0,1\}^{64}\times\{0,1\}^{64}\times G\to Z_q^*$, $H_4:\{0,1\}^{64}\times\{0,1\}^{64}\times G\times\{0,1\}^*\to Z_q^*$，公开系统参数$\mathrm{params}=\{l,q,G,P,P_{\mathrm{pub}},H_0,H_1,H_2,H_3,H_4\}$，秘密保存系统主密钥$s$。

身份基是由用户向密码标识管理中心注册之后由用户生成，具体过程如图2所示。

(1)$U_i\to\mathrm{CIMC}:\mathrm{Registration\ Request}$

新用户U_i通过安全信道向密码标识管理中心发送包括用户个人信息的注册请求，如用户身份证，邮箱，手机号等。

(2)$\mathrm{CIMC}\to U_i:\{d_i,\mathrm{RID}_i,\mathrm{Lifetime}_i,R_i\}$

密码标识管理中心CIMC审核用户U_i的身份，并为通过审核的用户U_i生成真实身份标识RID_i和用户部分密钥(d_i,R_i)，设置上网期限$\mathrm{Lifetime}_i$，然后通过安全信道将$\{d_i,\mathrm{RID}_i,\mathrm{Lifetime}_i,R_i\}$发送给用户$U_i$。具体如下：

(a)审核新用户U_i的身份信息，若真实，进行步骤(2)，否则拒绝其注册；

(b)根据用户U_i唯一身份信息(用户邮箱，手机号，身份证或组织域名等)生成一个长度固定的真实身份标识RID_i，即$\mathrm{RID}_i=H_0(U_i's\ \mathrm{feature})$；并为用户$U_i$设置上网期限$\mathrm{Lifetime}_i$；

(c)选择随机数$r_i\in Z_q^*$，计算$R_i=r_iP,\alpha_i=H_1(\mathrm{PID}_i,R_i)$和$d_i=\alpha_i s+r_i \bmod q$。

(3)$U_i:\mathrm{IB}[i]=\{\mathrm{RID}_i,\mathrm{Lifetime}_i,\mathrm{pk}_i,\mathrm{sk}_i\}$

用户U_i首先通过验证等式$d_iP=H_1(\mathrm{PID}_i,R_i)\cdot P_{\mathrm{pub}}+R_i$是否成立，完成对密码标识管理中心生成的用户部分密钥(d_i,R_i)正确性验证；然后随机选择$x_i\in Z_q^*$作为秘密值，计算$X_i=x_iP$；最后生成用户身份基，即$\mathrm{IB}[i]=\{\mathrm{RID}_i,\mathrm{Lifetime}_i,\mathrm{pk}_i,\mathrm{sk}_i\}$。其中$\mathrm{sk}_i=(d_i,x_i)$, $\mathrm{pk}_i=(R_i,X_i)$。

2.2 SDN批量匿名认证

由于SDN控制器为SDN的核心，为防止大量用户同时接入网络，导致SDN控制器出现单点失效问题，基于许芷岩等人[16]提出的无证书聚合签名方案，设计SDN批量匿名认证协议，将SDN控制器的用户身份验证功能下放给SDN交换机，由SDN接入交换机采用批量验证的方式过滤非法用户；SDN控制器只验证用户的有效性，然后与有效用户通过Diffie-Hellman算法协商共享密钥；另外，使用用户假名代替用户真实身份标识，除SDN控制器外任何人不能通过ID分析攻击获取用户信息，保护用户隐私。具体如图3所示。

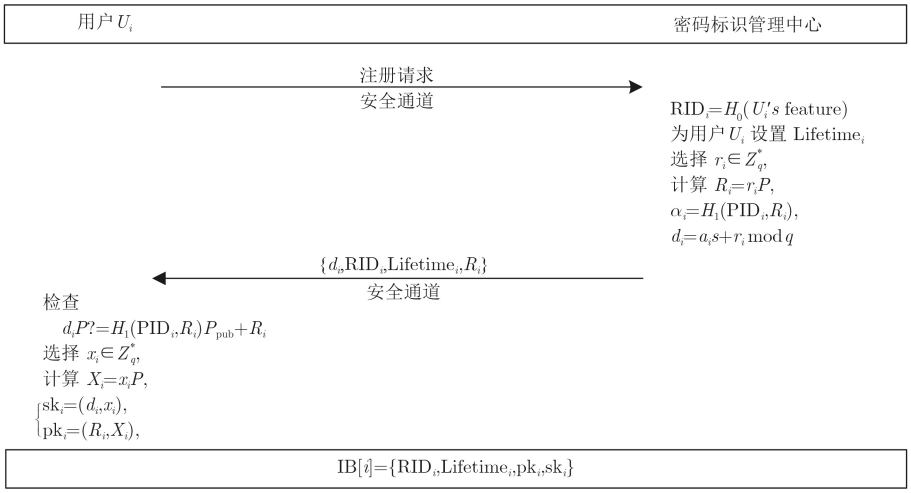

图 2 生成身份基

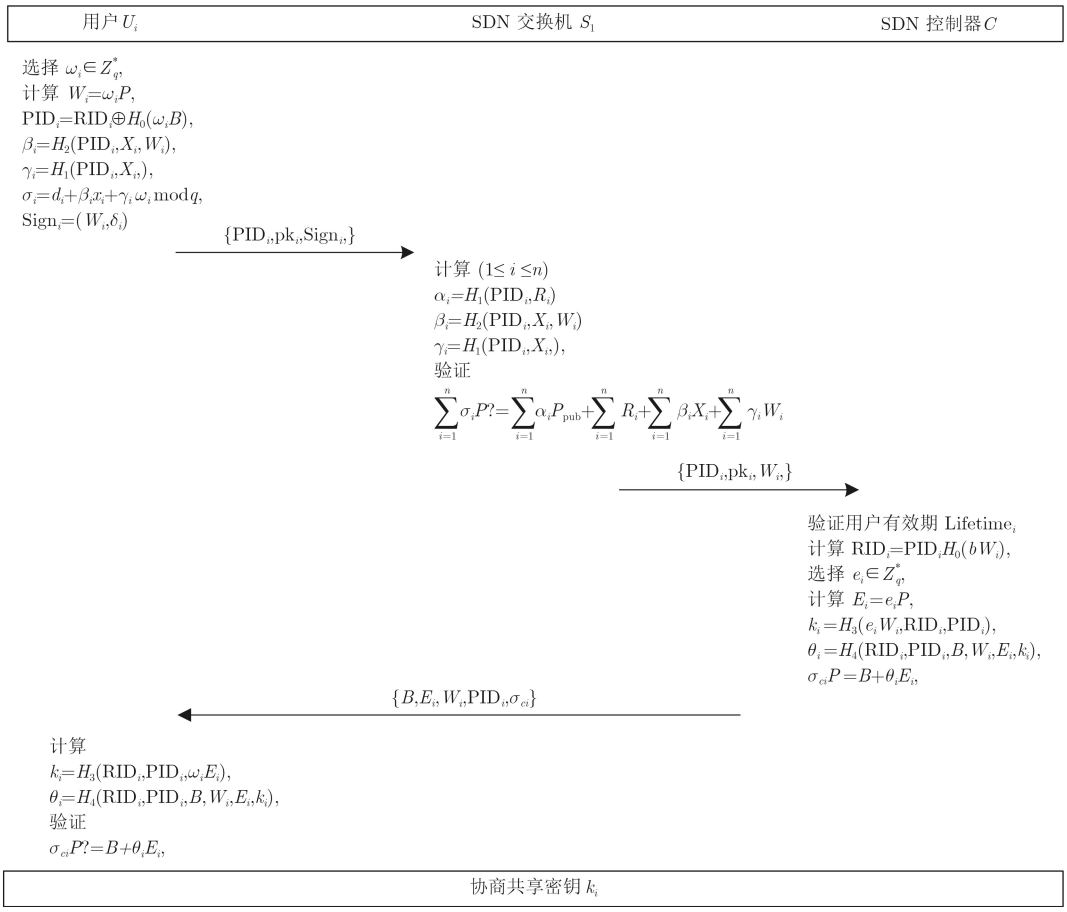

图 3 SDN批量匿名认证

(1) $U_i \to S_1: \{\mathrm{PID}_i, \mathrm{pk}_i, \mathrm{Sign}_i\}$：用户$U_i$选择随机数$\omega_i \in Z_q^*$，计算$W_i=\omega_i P$和$\mathrm{PID}_i=\mathrm{RID}_i \oplus H_0(\omega_i B)$；然后计算$\gamma_i=H_1(\mathrm{PID}_i, X_i)$和$\beta_i=H_2(\mathrm{PID}_i, X_i, W_i)$；再计算$\sigma_i=d_i+\beta_i x_i+\gamma_i \omega_i \bmod q$和$\mathrm{Sign}_i=(W_i, \sigma_i)$；最后将用户认证报文$\{\mathrm{PID}_i, \mathrm{pk}_i, \mathrm{Sign}_i\}$发送给SDN交换机$S_1$。

(2) $S_1 \to C: \{\mathrm{PID}_i, W_i\}$：SDN交换机$S_1$批量验证用户身份的真实性。SDN交换机$S_1$在时间$t$收到$n$个用户的认证报文$\{(\mathrm{PID}_i, \mathrm{pk}_i, \mathrm{Sign}_i) | 1 \le i \le n\}$，分别计算$\alpha_i=H_1(\mathrm{PID}_i, R_i)$，$\beta_i=H_2(\mathrm{PID}_i, X_i, W_i)$和$\gamma_i=H_1(\mathrm{PID}_i, X_i)$，并依据式(2)批量验证收到的签名是否有效。

$$\sum_{i=1}^{n}\sigma_i P=\sum_{i=1}^{n}\alpha_i P_{\mathrm{pub}}+\sum_{i=1}^{n} R_i+\sum_{i=1}^{n}\beta_i X_i+\sum_{i=1}^{n}\gamma_i W_i \tag{2}$$

文中采用b-SPECS[17]方案处理失效的批认证以及从中提取出有效的签名而不是丢弃整个批认证，然后将通过验证用户的$\{\mathrm{PID}_i, W_i\}$发送给SDN控制器C。

(3) $C \to U_i: \{E_i, \mathrm{PID}_i, \sigma_{ci}\}$：SDN控制器$C$计算用户$U_i$的真实身份$\mathrm{RID}_i=\mathrm{PID}_i \oplus H_0(bW_i)$，向密码标识管理中心查询$\mathrm{RID}_i$的有效期$\mathrm{Lifetime}_i$，验证用户$U_i$有效性，若失效拒绝其接入请求。否则，随机选择$e_i \in Z_q^*$，计算$E_i=e_i P, k_i=H_3(\mathrm{RID}_i, \mathrm{PID}_i, e_i W_i)$，$\theta_i=H_4(\mathrm{RID}_i, \mathrm{PID}_i, E_i, k_i)$，$\sigma_{ci}=b+\theta_i e_i$；再将$\{E_i, \mathrm{PID}_i, \sigma_{ci}\}$发送给用户$U_i$。

(4) U_i验证$\{E_i, \mathrm{PID}_i, \sigma_{ci}\}$：用户$U_i$计算$k_i=H_3(\mathrm{RID}_i, \mathrm{PID}_i, \omega_i E_i)$和$\theta_i=H_4(\mathrm{RID}_i, \mathrm{PID}_i, E_i, k_i)$；然后依据式(3)验证收到的签名是否有效。

$$\sigma_{ci} P=B+\theta_i E_i \tag{3}$$

若式(3)成立，表明用户U_i与SDN控制之间通过双向认证和协商共享密钥k_i；否则拒绝用户接入网络。

3　任意节点报文抽样验证

定义2　密码标识(Cipher Identification, CI)指采用密码技术，将用户身份属性与密码属性结合而形成的一种新的网络标识。即

$$\mathrm{CI}[i]=\{\mathrm{PID}_i, \mathrm{MAC}_{k_i}(\mathrm{PID}_i, m_i)\} \tag{4}$$

其中，PID_i表示用户U_i的假名，k_i是用户U_i与SDN控制器的共享密钥，m_i为IP负载。

密码标识是报文进出SDN网络的通行证，源设备的密码标识组件在报文的扩展首部封装密码标识，然后将其发送到SDN。而报文在SDN中是通过流表匹配的方式进行转发，如果流表匹配失败，将未匹配成功的报文上传到SDN控制器，由SDN控制器为其选定转发路径，生成合适的流表项。

当组表类型为select时，SDN交换机基于自身的选择算法选择性地执行组表项的一个动作桶，如基于用户指定的元组进行哈希或者简单的轮循。为确保报文的真实性的同时降低报文转发的平均延迟，利用组表的select类型特性，提出任意节点报文抽样验证流表项生成算法，如表1所示。该算法综合考虑密码标识有效性鉴别结果、上层应用策略和全网视图等多种因素，为用户U_i的报文选择合适的转发路径$S_1 \to \cdots \to S_k \to \cdots \to S_n$；引入随机检测模型，在报文转发路径任意选择SDN交换机S_k下发报文抽样验证流表项，指示该SDN交换机抽样验证报文携带的密码标识，而向其他SDN交换机下发正常转发流表项。其中抽样验证流表项动作为转向select类型的组表项，该组表项的动作桶分为两种：(1)将报文转发到数据来源验证模块；(2)报文正常转发。

另外，该算法引入检测因子h来控制报文的采样和检测比例，h值表示将两类动作桶的权重比。当$h=1$时，报文正常转发与转发到数据来源验证模块权重比为1:1，即当前报文采样比例约等于50%。当设定检测因子h后，SDN控制器将h和1分别作为报文正常处理类型动作桶和转发到报文源验证模块类型动作桶的权重，从而控制报文抽样验证的概率。

表 1 任意节点报文抽样验证流表项生成算法

算法1 任意节点报文抽样验证流表项生成算法

输入：未匹配报文P_i；检测因子h

输出：流表项；组表项；共享密钥k_i

(1) $\mathrm{PID}_i \leftarrow \mathrm{getPID}(P_i)$;

(2) SwitchID $\leftarrow$ getSwitchID (P_i);

(3) $\mathrm{SrcIP}_i \leftarrow \mathrm{getSrcIP}(P_i)$;

(4) $\mathrm{RID}_i \leftarrow \mathrm{PID}_i \oplus H_0(bW_i)$;

(5) get $\mathrm{Lifetime}_i, k_i$ by querying L_c according to RID_i;

(6) $\alpha = \mathrm{ValidityCheck}(\mathrm{Lifetime}_i)$;

(7) if $\alpha == 0$ /*RID_i失效*/

(8) setFlowEntry (SwitchID; SrcIP_i; drop);

(9) else /*RID_i有效*/

(10) select an optimized Path_i for unmatched packet P_i;

(11) $L_i \leftarrow \mathrm{getLength}(\mathrm{Path}_i)$;

(12) randomly select $x \in Z_q^*$;

(13) $k \leftarrow x \bmod L_i$;

(14) for $j=1; j \le L_i; j++$

(15) SwitchID$\leftarrow$ getSwitchID (Path (j));

(16) if $j \ne k$

(17) setFlowEntry(SwitchID; C_i; Forward);/*C_i为匹配域*/

(18) else

(19) SwitchID$\leftarrow$ getSwitchID (Path (k));

(20) setFlowEntry(SwitchID; C_i; Group);/*C_i为匹配域*/

(21) setGroupTable(SwitchID; select; h; Forward,Verify-MAC);

(22) send k_i to SwitchID by TLS;

(23) end if

(24)end if

4 分析与评估

4.1 正确性证明

当SDN交换机S_1收到n个用户的认证报文$\{(\mathrm{PID}_i, \mathrm{pk}_i, \mathrm{Sign}_i) \mid 1 \le i \le n\}$，签名验证式(2)可展开为

$$\begin{aligned}\sum_{i=1}^{n}\sigma_i P &= \sum_{i=1}^{n}\left(d_i+\beta_i x_i+\gamma_i\omega_i\right)P \\ &= \sum_{i=1}^{n}\left(\alpha_i s+r_i\right)P+\sum_{i=1}^{n}\left(\beta_i x_i\right)P+\sum_{i=1}^{n}\left(\gamma_i\omega_i\right)P \\ &= \sum_{i=1}^{n}\alpha_i P_{\mathrm{pub}}+\sum_{i=1}^{n}R_i+\sum_{i=1}^{n}\beta_i X_i+\sum_{i=1}^{n}\gamma_i W_i\end{aligned} \tag{5}$$

即式(2)的左边等于右边。

当用户收到SDN控制器C发送的认证报文$\{E_i, \mathrm{PID}_i, \sigma_{ci}\}$，签名验证式(3)可展开为

$$\begin{aligned}\sigma_{ci}P &= \left(b+\theta_i e_i\right)p \\ &= B+\theta_i E_i\end{aligned} \tag{6}$$

即式(3)的左边等于右边。

SDN控制器C生成的共享密钥k_i与用户U_i生成的共享密钥k_i的不同之处在于$e_i W$和$\omega_i E_i$。展开可得$e_i W = e_i\omega_i P = \omega_i E_i$，即可证二者生成的共享密钥是一致的。

4.2 安全性分析

SDN批量匿名认证协议中，基于许芷岩等人[16]提出的无证书聚合签名方案生成用户与SDN控制器的签名，其安全性归约于椭圆曲线上离散对数问题(Elliptic Curves Discrete Logarithm Problem, ECDLP)，在随机预言模型下证明其满足不可伪造性。下面将从共享密钥的安全性、用户身份的匿名性和可追踪性3个方面对SDN中基于密码标识的报

文转发验证机制安全性进行分析。

(1)共享密钥的安全性：共享密钥$k_i = H_3(\mathrm{RID}_i, \mathrm{PID}_i, e_i\omega_i P)$，其中$\mathrm{RID}_i = \mathrm{PID}_i \oplus H_0(b\omega_i P)$；攻击者若要伪造共享密钥$k_i$，则需要通过求解ECDLP问题得到$e_i, \omega_i, b$，由CDH(Computational Diffie-Hellman)假设可知，该问题是困难的，因此其满足不可伪造性。由于共享密钥k_i中ω_i和e_i分别由用户U_i与SDN控制器随机选取，只有通过双向认证才能获得相同的共享密钥k_i，实现共享密钥的联合控制。由于共享密钥k_i中包含双方随机数，用户每次接入网络时，双方都会选取新的随机数，因此每次协商的共享密钥k_i不同，满足前向安全性。

(2)匿名性：用户U_i使用假名替代真实身份，即$\mathrm{PID}_i = \mathrm{RID}_i \oplus H_0(b\omega_i P)$，由于ECDLP问题，即使捕获假名$\mathrm{PID}_i$，在无法获得随机值$\omega_i$或SDN控制器私钥$b$时，攻击者也无法获得$U_i$的真实身份。这也保证只有SDN控制器才能通过计算$\mathrm{RID}_i = \mathrm{PID}_i \oplus H_0(bW_i)$，获得用户$U_i$的真实身份，其他任何实体都不能获取，实现匿名的用户认证。当用户U_i重新接入SDN时，假名PID_i也随之更新，可防止用户被非法追踪或分析。

(3)可追踪性：用户U_i使用假名PID_i隐藏自己的真实身份RID_i，并不意味其违法行为不能溯源。一旦发现用户的违法行为，SDN交换机在SDN控制器的协助下，利用报文中携带的密码标识追踪其真实身份。

4.3 性能评估

使用华为RH2288作为实验运行服务器，其配置为Intel Xeon E5-2 600 CPU, 128 GB内存，在该服务器上创建3个操作系统为64位Ubuntu的虚拟机(VM)：VM1安装Mininet用于模拟网络环境；VM2上安装OpenDaylight控制器；VM3运行密码标识管理中心。本文假设所有用户都已经完成用户注册，拥有自己的身份基。网络拓扑采用Fattree拓扑结构，交换机与主机数目如表2所示。

表 2　交换机与主机数目表

网络符号	说明
网络拓扑结构	Fattree
核心交换机数目	64
聚集交换机数目	128
边界交换机数目	128
主机数目	512

(1)认证开销：为便于评估SDN批量匿名认证过程的开销，假设T_{em}表示群上的点乘运算；T_{ea}表示群上的点加运算；而其他运算(如one-way哈希运算等)的计算开销远小于前两者所给运算的计算开销，忽略不计。$|G|$表示群G中元素的长度；$|Z_q^*|$表示Z_q^*中元素的长度；$|\mathrm{ID}|$表示用户身份标识长度。从计算开销、通信开销等方面对比文献[18,19]方案，结果如表3所示。

分析可得，本方案在计算开销上优于文献[18]和文献[19], SDN控制器(服务器)的计算开销改善的幅度较大，原因在于SDN控制器将验证功能下放给SDN交换机，SDN控制器只需验证真实用户的有效性和协商共享密钥。SDN交换机采用批量验证，其计算开销小于逐包验证的开销。而通信开销略有增加，原因在于，本方案为三方交互协议，为减少SDN交换机的存储开销，用户认证报文携带自己的公钥。在用户认证成功后，用户在每个IP报文嵌入密码标识，增加的通信开销为$(|\mathrm{ID}|+|Z_q^*|)$。

(2)网络吞吐量：本文使用自定义发包脚本，分别设定检测因子h为9, 7, 4, 3和1，其对应的报文验证触发概率为10%, 12.5%, 20%, 25%和50%，测量在不同的检测因子h下的网络吞吐量，并与未使用报文转发验证机制的网络吞吐量进行对比。实验结果如图4所示。

以未使用报文转发验证机制的网络吞吐量为基准，在h=9，吞吐量下降了5.6%左右，随着h值的减少，吞吐量随之下降，其中h=1，吞吐量下降最多，降低了约31.5%左右。因此网络吞吐量的影响与检测因子h成反比关系，检测因子h越大，网络吞吐量受到的影响越小。

(3)检测准确率：本文使用自定义发包脚本，分别以0.5和0.5的概率进行随机注入伪造的数据包和随机篡改合法数据包等操作，各个攻击分别持续60 s，各做100次，实验结果取平均值，测试在不同检测因子下报文转发验证机制的检测准确率。其

表 3　认证开销

方案	参与方数量	通信开销	用户计算开销	SDN控制器(服务器)计算开销	SDN交换机计算开销
文献[18]	2	$3\|G\|+4\|\mathrm{ID}\|+2\|Z_q^*\|$	$7T_{\mathrm{em}}+2T_{\mathrm{ea}}$	$5T_{\mathrm{em}}+2T_{\mathrm{ea}}$	$(3n+1)\ T_{\mathrm{em}}+(4n-1)\ T_{\mathrm{ea}}$
文献[19]	2	$2\|G\|+4\|\mathrm{ID}\|+4\|Z_q^*\|$	$7T_{\mathrm{em}}+T_{\mathrm{ea}}$	$7T_{\mathrm{em}}+T_{\mathrm{ea}}$	–
本文方案	3	$5\|G\|+3\|\mathrm{ID}\|+2\|Z_q^*\|$	$5T_{\mathrm{em}}+T_{\mathrm{ea}}$	$2T_{\mathrm{em}}$	–

注：“–”表示不存在该项，n为单位时间SDN交换机收到用户数目

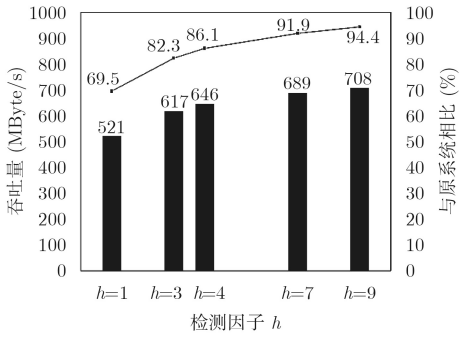

图 4 不同的检测因子h下的网络吞吐量

中检测因子h分别设为9, 7和4。如果报文转发验证机制未能检测非法数据包，则记录为漏报。同时在正常情况下向SDN注入合法的数据包，每次持续60 s，如果报文转发验证机制将一些报文丢弃则记录为误报。实验结果如图5所示。

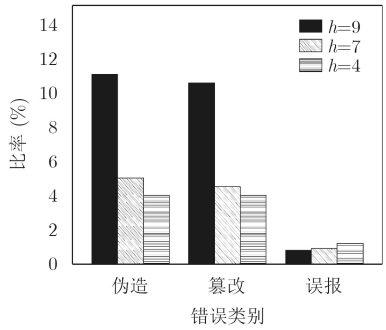

图 5 检测准确率

从图5知，在不同的检测因子h下，伪造和篡改报文的漏报率差不多相等，这是由于该机制通过验证报文携带的密码标识识别非法报文，伪造和篡改的报文都会使密码标识验证失败。同时，在不同的检测因子h下，都会产生误报但相对较低，分别约为0.8%，0.9%和1.2%，原因在于SDN控制器通过TLS信道将共享密钥发送给指定的SDN交换机具有一定的延迟，指定的SDN交换机在验证流量过大时将无共享密钥验证的报文丢弃。此外，检测因子h的值越大，其伪造和篡改报文的漏报率越高，同时误报率越低，这也就意味着较高的采样比例可以获得较高的安全性能。同时综合网络吞吐量的实验结果，可得出$h=7$时，可以获得较好的检测准确率，同时不需要付出较高的吞吐开销。

(4)转发延迟：本文使用自定义发包脚本，分别在使用及未使用报文转发验证机制的SDN中发送10万个数据包，在两个网络中所有数据包使用相同的转发路径；设置检测因子h为7；使用Wireshark分别从网络入口和出口抓取数据包，计算数据包的转发延迟，描绘如图6所示的转发延迟的累积分布函数(Cumulative Distribution Function, CDF)图像。

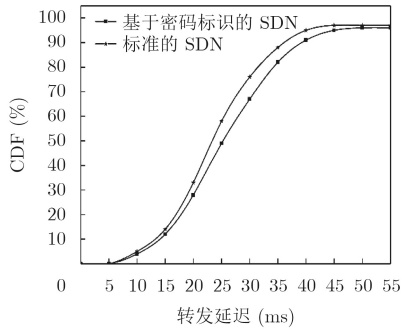

图 6 转发延迟CDF

从图6可知，在相同的网络拓扑情况下，未使用报文转发验证机制系统中数据包的转发延迟都集中在20～40 ms，所有数据包的平均转发延迟为30.7 ms；基于密码标识的SDN中数据包的转发延迟集中在30～40 ms，数据包的平均转发延迟为33.65 ms，增加了约9.6%的转发延迟，主要原因是为确保SDN网络中报文的真实性，SDN控制器在报文的转发路径中指定SDN交换机抽样验证报文中携带的密码标识。

5 结束语

针对软件定义网络中缺乏安全高效的数据来源验证机制问题，本文提出基于密码标识的报文转发验证机制。建立基于密码标识的报文转发验证模型，基于批量匿名验证和抽样验证技术，提出了SDN批量匿名认证协议和基于密码标识的任意节点抽样验证方案，允许多用户同时接入，提高了网络的可用性，同时为用户提供条件隐私保护；最后，在基于OpenDaylight和Mininet的实验环境中对所提机制进行实现和验证。结果表明该机制能快速检测报文伪造和篡改及抵抗ID分析攻击，但同时引入大约9.6%的转发延迟和低于10%的通信开销。在未来的工作中，我们将研究该机制的扩展性，在多控制器的网络中实现数据来源可验证。

参 考 文 献

[1] MCKEOWN N. Software-defined networking[C]. IEEE International Conference on Computer Communications, Rio de Janeiro, Brazil, 2009: 30–32.

[2] NUNES B, MENDONCA M, NGUYEN X, *et al*. A survey of software-defined networking: Past, present, and future of programmable networks[J]. *IEEE Communications Surveys & Tutorials*, 2014, 16(3): 1617–1634. doi: 10.1109/SURV.2014.012214.00180.

[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. doi: 10.13328/j.cnki.jos.005020.
WANG Mengmeng, LIU Jianwei, CHEN Jie, *et al*. Software defined networking: Security model, threats and mechanism[J]. *Journal of Software*, 2016, 27(4): 969–992. doi: 10.13328/j.cnki.jos.005020.

[4] LIU Hongqiang, WU Xin, ZHANG Ming, *et al*. zUpdate: Updating data center networks with zero loss[J]. *Computer Communication Review*, 2013, 43(4): 411–422. doi: 10.1145/2486001.2486005.

[5] LI Dan, SHANG Yunfei, and CHEN Congjie. Software defined green data center network with exclusive routing[C]. IEEE International Conference on Computer Communications, Toronto, Canada, 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, San Diego, USA, 2015: 1–15.

[7] 李杰, 吴建平, 徐恪, 等. Hidasav: 一种层次化的域间真实源地址验证方法[J]. 计算机学报, 2012, 35(1): 85–100. doi: 10.3724/SP.J.1016.2012.00085.
LI Jie, WU Jianping, XU Ke, *et al*. An hierarchical inter-domain authenticated source address validation solution[J]. *Chinese Journal of Computers*, 2012, 35(1): 85–100. doi: 10.3724/SP.J.1016.2012.00085.

[8] YAO Guang, BI Jun, and XIAO Peiyao. Source address validation solution with OpenFlow/NOX architecture[C]. IEEE International Conference on Network Protocols, Vancouver, Canada, 2011: 7–12.

[9] 孙鹏. 面向SDN的源地址验证方法研究[J]. 电光与控制, 2016, 23(3): 49–53. doi: 10.3969/j.issn.1671-637X.2016.03.012.
SUN Peng. Source address validation methods based on SDN[J]. *Electronics Optics & Control*, 2016, 23(3): 49–53. doi: 10.3969/j.issn.1671-637X.2016.03.012.

[10] LIU Bingyang, BI Jun, and ZHOU Yu. Source address validation in software defined networks[C]. ACM Conference on SIGCOMM, Florianópolis, Brazil, 2016: 595–596.

[11] KIM H, BASESCU C, JIA L, *et al*. Lightweight source authentication and path validation[C]. ACM Conference on SIGCOMM, Chicago, USA, 2014: 271–282.

[12] TAKAYUKI S, CHRISTOS P, TAEHO L, *et al*. SDNsec: Forwarding accountability for the SDN data plane[C]. International Conference on Computer Communication and Networks, Hawaii, USA, 2016: 1–10.

[13] 陈越, 贾洪勇, 谭鹏许, 等. 基于流认证的IPv6接入子网主机源地址验证[J]. 通信学报, 2013, 34(1): 171–178. doi: 10.3969/j.issn.1000-436x.2013.01.019.
CHEN Yue, JIA Hongyong, TAN Pengxu, *et al*. Host's source address verification based on stream authentication in the IPv6 access subnet[J]. *Journal of Communications*, 2013, 34(1): 171–178. doi: 10.3969/j.issn.1000-436x.2013.01.019.

[14] 董平, 秦雅娟, 张宏科. 支持普适服务的一体化网络研究[J]. 电子学报, 2007, 35(4): 599–606.
DONG Ping, QIN Yajuan, and ZHANG Hongke. Research on universal network supporting pervasive services[J]. *Acta Electronica Sinica*, 2007, 35(4): 599–606.

[15] FARINACCI D, MEYER D, ZWIEBEL J, *et al*. The locator/id separation protocol (LISP) for multicast environments[S]. Internet Draft, draft-farinacci-lisp-15.txt, 2011.

[16] 许芷岩, 吴黎兵, 李莉, 等. 无线漫游认证中可证安全的无证书聚合签名方案[J]. 通信学报, 2017, 38(7): 123–130. doi: 10.11959/j.issn.1000-436x.2017152.
XU Zhiyan, WU Libing, LI Li, *et al*. Provably secure certificateless aggregate signature scheme in wireless roaming authentication[J]. *Journal of Communications*, 2017, 38(7): 123–130. doi: 10.11959/j.issn.1000-436x.2017152.

[17] HORNG S, TZENG S, PAN Y, *et al*. b-SPECS+: batch verification for secure pseudonymous authentication in VANET[J]. *IEEE Transactions on Information Forensics & Security*, 2013, 8(11): 1860–1875. doi: 10.1109/TIFS.2013.2277471.

[18] 谢永, 吴黎兵, 张宇波, 等. 面向车联网的多服务器架构的匿名双向认证与密钥协商协议[J]. 计算机研究与发展, 2016, 53(10): 2323–2333. doi: 10.7544/issn1000-1239.2016.20160428.
XIE Yong, WU Libing, ZHANG Yubo, *et al*. Anonymous mutual authentication and key agreement protocol in multi-server architecture for VANETs[J]. *Journal of Computer Research and Development*, 2016, 53(10): 2323–2333. doi: 10.7544/issn1000-1239.2016.20160428.

[19] 周彦伟, 杨波, 张文政. 一种改进的无证书两方认证密钥协商协议[J]. 计算机学报, 2017, 40(5): 1181–1191. doi: 10.11897/SP.J.1016.2017.01181.
ZHOU Yanwei, YANG Bo, and ZHANG Wenzheng. An improved two-party authenticated certificateless key agreement protocol[J]. *Chinese Journal of Computers*, 2017, 40(5): 1181–1191. doi: 10.11897/SP.J.1016.2017.01181.

秦　晰：女，1978年生，副教授，硕士生导师，研究方向为SDN安全、可信计算.
唐国栋：男，1992年生，硕士生，研究方向为SDN安全.
常朝稳：男，1965年生，教授，博士生导师，研究方向为网络安全、态势感知.
王瑞云：女，1992年生，硕士生，研究方向为协议形式化验证.