文章编号:1671-4598(2018)02-0142-04 DOI:10.16526/j.cnki.11—4762/tp.2018.02.035 中图分类号:TP393 文献标识码:A

基于 LabWindows 的云计算环境安全框架研究

唐卫国[1], 廖大强[2]
(1. 广东工程职业技术学院 信息工程学院, 广州 510520; 2. 广东南华工商职业学院 信息工程与商务管理学院, 广州 510507)

摘要: 为保证云计算环境下网络数据传输过程中数据的保密性、完整性以及流畅性, 需要对云计算环境安全框架进行研究, 目前的云计算环境安全框架系统设计方法主要是利用恩尼格码加密技术和分割二进制码技术实现当前云计算环境下网络数据的安全传输与通信; 存在网络节点能量开销较大, 且数据安全性判断平均准确率较低的问题; 为提高云计算环境下网络数据的安全性判断准确率, 避免网络节点的能量浪费, 提出一种基于 LabWindows 的云计算环境安全框架系统设计方法, 首先运用 LabWindows 对云计算环境下的数据进行采集, 然后利用证据信任度求取算法对云计算环境下的网络数据安全性进行判断; 其次将异常漂移检测器与恶意节点 ID 号过滤器有机结合, 剔除云计算环境中的恶意攻击数据; 再利用数字证书对云计算环境下的客户端与服务器进行身份认证; 最后利用 LabWindows 平台创建云计算环境安全框架模型; 实验结果证明, 利用该方法能够节省云计算环境下网络节点的能量开销, 对网络数据安全性判断准确率较高。

关键词: 基于 LabWindows; 云计算环境; 安全框架

Labwindows—based Cloud Computing Environment Security Framework Research

Tang Weiguo[1], Liao Daqiang[2]
(1. Guangdong Engineering Polytechnic College, Guangzhou 510520, China;
2. Guangdong Nanhua Vocational College, Guangzhou 510507, China)

Abstract: In order to ensure that cloud computing environment in the process of the network data transmission data confidentiality, integrity and fluency, need security framework for research on cloud computing environment, the current cloud computing environment security framework system design method is mainly use the Enigma code encryption technology and segmentation binary code technology to realize the current cloud computing environment the security of the network data transmission and communication. The problem is that the network node has a high energy cost and the average accuracy of the data security is low. In order to enhance the security of network data in cloud computing environment judgment accuracy, avoid network node energy waste, presents a cloud computing environment based on LabWindows security framework system design method, first using LabWindows to cloud computing environment data acquisition, and then use evidence credibility calculating algorithm in cloud computing environment of the network data security for judgment; The second is to combine the anomalous drift detector with the malicious node—Id filter, which removes the malicious attack data from the cloud computing environment; Using digital certificates to authenticate clients and servers in the cloud computing environment; Finally, use the LabWindows platform to create a cloud computing environment security framework model. The experimental results show that the method can save the energy expenditure of network nodes in cloud computing environment, and the accuracy of network data security is higher.

Keywords: based on LabWindows; cloud computing environment; security framework

0 引言

自动测试与控制系统是云计算环境下虚拟仪器编程语言 LabWindows/CVI 的重要研究领域之一[1], 而 LabWindows/CVI 是 National Instruments 公司向市面推出的一套面向自动化测量控制领域的交互式 C 语言开发平台, NI 公司推出的一系列基于电脑客户端 PCI 总线的云计算环境下数据采集卡, 在 LabWindows/CVI 软件开发平台上控制云计算环境下各种数据的采集卡均需要网络数据采集驱动程序的支持[2-3]。NI 公司为其推出的全部网络数据采集卡提供了专业的驱动支持程序, 能够实现 NI 公司网络数据采集卡的实时操作, 为后续云计算环境下数据控制软件的设计开发提供方便, 用户可以节省开发数据采集卡驱动程序的成本[4]。它的操作的核心是 ANSI C, 同时将功能强大、灵活性好的 C 语言平台与云计算环境下的数据采集、处理、分析和控制的自动化测量控制专业化工具完美的融合[5]。由于它的集成化软件开发平台、交互式编程方式简单、丰富多样的控制元件以及库函数, 极大提高 C 语言的性能, 为熟知和利用 C 语言开发的工作人员建立更加完善的云计算环境安全检测系统、云计算安全自动测量环境、云计算环境下数据的采集系统、数据采集过程监控系统等提供一个更为理想的软件开发平台[6]。为保证网络数据传输过程中数据的保密性、完整性以及流畅性, 需要对云计算环境安全框架进行研究。目前的云计算环境安全框架系统设计方法主要是利用恩尼格码加密技术和分割二进制码技术实现当前云计算环境数据的安全传输与通信[7]。存在云计算环境下网络节点能量开销

收稿日期:2017-05-03; **修回日期**:2017-05-21。
基金项目:广东省大数据分析与处理重点实验室开放基金项目资助(2017013);广东教育学会"十三五"教育科研重点课题(GDESH13010)。
作者简介:唐卫国(1980-),男,广东韶关人,硕士,讲师,主要从事计算机软件、计算机网络、电子商务、职业测评系统开发、就业创业教育方向的研究。

较大，且数据安全性判断平均准确率较低的问题。降低网络节点能量的开销，提高数据安全性判断准确率，引起了众多学者的广泛关注，在实际应用过程中提出一系列行之有效的方法。

文献［8］提出一种基于生物免疫原理的云计算环境安全框架系统设计方法，首先利用生物免疫原理，建立云计算环境网络数据入侵特征库；然后引入粗糙集理论解决云计算环境中网络信息的不确定性与不完整性，建立云计算环境安全框架。该方法虽然提高云计算环境中网络入侵检测率，但检测准确性较低。文献［9］提出一种基于网络编码技术的云计算环境安全框架系统设计方法，首先利用网络编码技术计算接收到的云计算环境下网络数据包的线性相关性，判断其是否为非创新包；然后检测该网络数据包是否为污染包；再利用抗熵攻击与污染攻击的云计算环境网络数据包过滤算法创建云计算环境安全框架数学模型。该方法无法有效地防御云计算环境中的恶意网络攻击，增加了网络节点的能量开销。文献［10］提出了一种基于数字封信技术的云计算环境安全框架系统设计方法，首先将密码学的三大分支，即非对称加密机制、对称加密机制以及数字签名技术的优点进行有机结合；然后利用数据加密标准算法与数据高级加密标准算法设计出能够实现云计算环境下数据安全传输的系统框架。针对上述问题，本文提出一种基于 LabWindows 的云计算环境安全框架系统设计方法，实验结果证明，所提方法在网络入侵频发的情况下能够节省网络节点能耗，且对网络数据安全性判断准确率较高。

1　基于 LabWindows 的云计算环境安全框架研究

1.1　基于 D－S 的云计算环境数据安全性判断

首先运用 LabWindows 对云计算环境下的数据进行采集，然后利用证据信任度求取算法对云计算环境下的网络数据安全性进行判断。详细操作过程如下：

DS 证据理论要求证据在云计算环境下的所有命题产生一个信任度即 BBA。如果 Θ 表示云计算环境下的网络数据，云计算环境下的网络数据安全函数 $m:2^{\Theta}\rightarrow[0,1]$ 满足以下条件：

$$m(\Phi)=0 \tag{1}$$

$$\sum_{l\subseteq U}m(l)=1 \tag{2}$$

式中，$m(l)$ 表示云计算环境下各个时间网络节点的时间信息 l 在证据理论下的信任度 BBA。

根据上式，选取用于判断云计算环境下网络节点安全性的证据，包括网络时钟偏移量、网络路径延迟以及网络路径延迟变化，与其相对应的证据理论信任度 $m_i(l)$ 的计算过程分别如下：

（1）云计算环境下网络时钟偏移量证据理论信任度 $m_1(l)$。假设云计算环境下可信网络平台时钟服务器的布置是按照网络拓扑结构进行的，其网络流量与网络路径同时发生变化的可能性极小，云计算环境下的网络时钟偏移通常情况下在真实值附近。则云计算环境下网络时钟偏移量证据理论信任度 $m_1(l)$ 的计算公式如下：

$$\begin{cases} m_1(l_i)=\dfrac{\varepsilon_i}{\varepsilon}\times w_1 \\ \varepsilon=\displaystyle\sum_{i=1}^{n}\varepsilon_i \\ \varepsilon_i=\displaystyle\sum_{j=1,j\neq i}^{n}\frac{1}{|\varphi_i-\varphi_j|} \end{cases} \tag{3}$$

其中：φ_i 表示云计算环境下网络数据对应时间网络节点 i 的时间偏移值；φ_j 表示云计算环境下网络数据对应时间网络服务器节点 j 的时间偏移值；ε_i 表示云计算环境下网络服务器节点 i 的时间偏移系数；ε 表示云计算环境下网络节点的时间偏移系数；n 表示云计算环境下利用可信网络平台 NIP 同步算法计算出的其他网络服务器节点的时间数据信息。

（2）云计算环境下网络路径延迟证据信任度 $m_2(l)$。根据最小时延原理，云计算环境下服务器网络路径延迟越小，网络时间同步误差减小的可能性越大。则云计算环境下网络路径延迟证据信任度 $m_2(l)$ 的计算表达式为：

$$\begin{cases} m_2(l_i)=\dfrac{\beta_i}{\beta}\times w_2 \\ \beta=\displaystyle\sum_{i=1}^{n}\beta_i \\ \beta_i=\dfrac{1}{\delta_i} \end{cases} \tag{4}$$

其中：δ_i 代表云计算环境下对应时间的网络服务器节点 i 的路径延迟；β 代表云计算环境下网络节点的路径延迟系数；β_i 代表云计算环境下网络节点 i 的路径延迟系数。

（3）云计算环境下网络路径延变化证据理论信任度 $m_3(l_i)$。同理，根据最小时延原理，相对于云计算环境下网络最小路径延迟，如果网络路径延迟变大，网络时间同步误差减小的可能性越大。则云计算环境下网络路径延变化证据理论信任度 $m_3(l_i)$ 的计算公式为：

$$\begin{cases} m_3(l_i)=\dfrac{\eta_i}{\eta}\times w_3 \\ \eta=\displaystyle\sum_{i=1}^{n}\eta_i \\ \eta_i=\dfrac{1}{\delta_1-\delta_{im}} \end{cases} \tag{5}$$

$$\sum_{i=0}^{3}w_i=1 \tag{6}$$

式中，δ_{im} 表示云计算环境下网络数据对应时间网络服务器节点 i 的目前最小路径延迟；η 表示云计算环境下网络路径证据理论信任度系数；η_i 表示在云计算环境下网络节点 i 的路径证据理论信任度系数；w_i 表示云计算环境下 3 个时钟证据理论信任度 BBA 的比例系数，且它们 3 个的和为 1。

利用证据理论的合成规则，对上述 3 个云计算环境下网络时钟证据理论信任度 $m_i(l)$ 进行合成计算，其表达式为：

$$\begin{cases} m_i=\dfrac{\eta_i}{\eta} \\ \eta_i=m_1(l_i)+m_2(l_i)+m_3(l_i) \\ \eta=\displaystyle\sum_{i=0}^{m}m_1(l_i)+m_2(l_i)+m_3(l_i) \end{cases} \tag{7}$$

根据上述公式（7），获得云计算环境下各个服务器网络时间信息的证据理论信任度 $m(l)$。如果云计算环境下的某一时间段服务器网络时间信息证据理论信任度 $m(l)$ 低于预设的门限值 ζ，则判断该时段内的云计算环境下的网络数据存在安全隐患。

1.2　基于 FTSP 的云计算环境下网络数据过滤

在上述云计算环境下网络数据安全判断结果的基础上，将异常漂移检测器与恶意节点 ID 号过滤器有机结合，剔除云计算环境中的恶意攻击数据。具体操作过程如下：

FISP（泛洪时间同步协议）利用一次元回归法估计云计算环境下网络节点本地时钟与网络标准时钟的时间偏移程度，并在时间每秒末尾对云计算环境下网络节点本地时间进行补偿，从而提高网络数据时钟的同步精度。则云计算环境下网络节点本地时钟与网络标准时钟时间关系的表达式为：

$$\begin{cases} T = at + b \\ a = 1 + d \end{cases} \tag{8}$$

其中：t 表示云计算环境下网络节点本地时间；T 表示云计算环境下网络标准时间；云计算环境下网络时间偏移程度通常用漂移率来体现，假设 d 表示云计算环境下时钟漂移率 2 个时钟之间时间差的速率，在稳定的云计算环境下，网络传感器节点的时钟漂移率也是处于相对稳定的状态，此时 d 的取值范围需满足以下条件：

$$\begin{cases} \rho \leqslant \dfrac{\mathrm{d}T}{\mathrm{d}t} - 1 \leqslant \rho \\ -\rho \leqslant \mathrm{d} \leqslant \rho \end{cases} \tag{9}$$

式中，ρ 表示云计算环境下网络时钟时间差系数。

根据上述公式（9），当云计算环境下传感器网络中的节点处于安全稳定且同步的情况下，每个网络节点的时钟漂移率均为一个相对稳定的值。由于云计算环境下网络中的每个节点都有一个稳定却不同于其他网络节点的时钟漂移率，则将该时钟漂移率视为云计算环境下网络节点的唯一标识 ID。云计算环境下的同一个网络节点在每个同步周期测量获得的网络时钟漂移率之间的偏差程度极小，通常情况下不大于 10^{-6}。

对上述计算进行进一步分析可知，当云计算环境下的网络标准时间（即网络发送时间标）T 被网络攻击恶意篡改，则云计算环境下的时钟漂移率 d 会出现明显偏差。将异常时钟漂移率检测器与恶意节点 ID 号过滤器有机结合，并加入云计算环境中，利用各个网络节点在安全同步状态下具有唯一固定的且不同于其他网络节点的时钟漂移率，检测受到网络恶意攻击而接收到的云计算环境下的网络标准时间，即网络发送时间标，同时将云计算环境中错误的同步时间数据信息丢弃，重新接收其他相邻节点发送的同步数据信息。如果云计算环境下的网络节点连续 2 次发送错误的网络标准时间，则需要将恶意网络节点 ID 号过滤淘汰，加入云计算环境下的网络黑名单中，并提示其他相邻网络节点拒收来自该恶意攻击节点的同步数据信息，以减少云计算环境下的网络开销。

为实现上述功能，过滤掉恶意网络节点发送的同步数据信息，需要对云计算环境中网络原始同步信息的数据包格式进行适当修改，同时在云计算环境中的网络同步数据信息中添加发送恶意节点的 ID 以及黑名单。

当云计算环境中各个网络节点时钟同步一定周期后，时钟漂移率基本处于稳定状态，且随着同步的周期越多，其精度越高，稳定性能越好。当时钟漂移率稳定时，在一定周期内创建一个记录各个网络节点时钟漂移率的平均值存储表 M。并通过实验结果分析，确定云计算环境下的网络时钟漂移率范围是 $\pm\theta$，则时钟漂移率的阈值范围计算表达式为：

$$-\theta \leqslant dthresh - old \leqslant M_n + \theta \tag{10}$$

其中：n 表示云计算环境下时钟漂移周期数。

根据上述公式（10），每个周期计算得到的网络时钟漂移率 d_n 都需要进入时钟漂移率的平均值存储表 M 中进行判定。如果当前周期的网络时钟漂移率在阈值范围内，则接收此次云计算环境下的网络同步数据信息并进行数据更新；反之，则丢弃该数据信息，重新接收云计算环境下其他相邻网络节点的同步数据信息。

1.3 基于身份的云计算环境下网络数据安全算法

基于身份的云计算环境下网络数据安全算法是利用数字证书对云计算环境下的客户端与服务器进行身份认证，确保云计算环境下网络数据的安全性。具体步骤如下：

在云计算环境下的椭圆曲线中使用的是有限域，$GF(q)$ 表示云计算环境下 q 阶有限域，也可记作 Fq，则云计算环境下有限域 F 上的维尔斯特拉斯函数方程表达式如下：

$$E: Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3 \tag{11}$$

$$F(X,Y,Z) = Y^2Z + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3 \tag{12}$$

式中，X、Y、Z 均表示有限域 F 上的维尔斯特拉斯函数随机变量；$a_{i'} \in F$，$(X,Y) \in F^2$ 且在云计算环境下的椭圆曲线上不存在非奇异点，则称集合 $E(F)$ 表示为云计算环境下有限域 F 上的椭圆曲线，其表达式如下：

$$E(F) = \{(X,Y) \mid (Y,Z)\} \bigcup \{0\} \tag{13}$$

式中，0 表示云计算环境下椭圆曲线上的无穷远点；如果 a_1，a_2，a_3，a_4，a_5，a_6 不全部为 0 时，云计算环境下该椭圆曲线是非奇异的，该椭圆曲线上的所有点集合即为椭圆曲线，则云计算环境下椭圆曲线的双线性映射定义如下；

假设 G_1 与 G_2 是两个在云计算环境下大素数 p 具有 q 阶有限域的循环群。G_1 表示云计算环境下有限域 F_p 上的椭圆曲线点群；G_2 表示云计算环境下有限域 F_{p^2} 上的椭圆曲线点子群。由此 G_1 组成一个云计算环境下加法群面 G_2 的乘法群。如果对于所有的云计算环境下网络数据 $P,Q \in G_1$，且 $a,b \in Z$，则云计算环境下网络数据的线性映射表达式为：

$$e(aP,bQ) = e(P,Q)^{ab} \tag{14}$$

根据式（14），对云计算环境下网络数据安全身份认证进行运算，主要分为数字签名与身份验证两部分：

云计算环境下的数字签名阶段：随机选取云计算环境中一个 k 比特长的素数，且 $k \in Z_q^*$，其中 Z_q^* 表示云计算环境下 q 阶有限域的密钥集合，按以下过程进行计算：

$$r_a = kQ_A \tag{15}$$

$$u_a = H_2(e(d_{Id},kQ_s) \tag{16}$$

$$t_a = kp \tag{17}$$

$$s_a = d_{Id} + kr \tag{18}$$

式中，d_{Id} 代表云计算环境下网络数据私钥；s 代表云计算环境下网络数据的主密钥；Id 代表云计算环境下网络数据的公钥；d_{Id} 代表云计算环境下网络数据的解密私钥；t_a 代表云计算环境下网络数据加密的密文；r_a 代表云计算环境下网络数据对原文生成的新密文；Q_A 代表哈希运算。

根据上述公式（15）～（18），将云计算环境下网路数据自身的身份 Id，t_a，r_a 以及数字签名 s_a 发送给网络安全中心。

云计算环境下网路数据的安全验证阶段：网络安全中心收到信息后，开始对发送者的身份信息进行验证，验证表达式为：

$$e(P,d_{Id}) = e(P_{pub},Q_A) * e(t_a,r_a) \tag{19}$$

如果上述公式（19）成立，则证明数字签名有效，身份认证通过且合法；如果不成立，则证明身份认证失败，云计算环

境下的网络会自动断开连接，保护云计算环境的安全运行。

1.4　基于 LabWindows 的云计算环境安全框架设计

综合上述计算，利用 LabWindows 设计云计算环境安全框架，如图 1 所示。

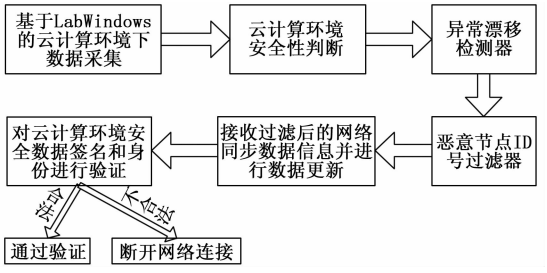

图 1　基于 LabWindows 的云计算环境安全框架

从图 1 中可以看出，云计算环境安全框架系统包括以下 4 个部分：一是基于 LabWindows 的云计算环境数据采集模块；二是云计算环境安全性判断模块；三是云计算环境下的网络数据过滤器，包括异常漂移检测器和恶意节点 ID 号过滤器；四是云计算环境安全验证模块。

利用上述设计的基于 LabWindows 的云计算环境安全框架能够保证云计算环境下网络数据传输与通信的安全性。

2　实验结果与分析

实验仿真软件环境为 NS2，300M * 300M 的区域内布置 800 个网络节点和 10 个基站，每个网络节点的原始能量开销为 3J，网络基站是能够携带较多能量的网络节点，可以不考虑其能量开销问题，只考虑云计算环境下的普通节点能量开销。

实验仿真的硬件环境为惠普笔记本电脑，Windows10 操作系统，显卡型号是 GTX1050，硬盘内存为 1 T，内存容量为 8 GB，显存容量为 2 GB。实验使用 LabWindows 进行开发设计实现。实验数据来源于云计算环境下的随机一组网络数据，中途的恶意网络入侵次数有 50 次。

为验证本文所提方法的有效性，对云计算环境安全框架系统设计方法的能量开销进行分析。主要针对云计算环境中处理器 CPU 与射频模块（RF）的能量开销进行分析。

在没有设计出云计算环境安全系统框架的情况下，网络节点的能量开销分布数据如表 1 所示。其中，能量单位表示为 μJ；网络消息长度单位表示为 byte，云计算环境下处理器表示为 E_CPU；云计算环境下射频模块表示为 E_RF；云计算环境下网络节点的整体能量开销表示为 E_Sum。

表 1　无安全服务时网络节点的能量开销分布

网络消息长度	*E_CPU*	*E_RF*	*E_Sum*
10	24	972	998
20	25	1128	1157
30	28	1286	1324
40	29	1858	2108

根据表 1 可知，云计算环境下网络节点上的数据信息处理程序相对简单，对于上述的 4 种长度消息 E_CPU 能量开销仅占网络节点整体能量开销的 1.2%；而 48%的能量被云计算环境下的射频模块部分 E_RF 消耗。当云计算环境下的网络消息长度增加时，网络处理器 E_CPU 的能量开销只有细微的增加；而云计算环境下的射频模块 E_RF 能量开销却发生明显变化。对于 10～40 byte 的网络消息长度，云计算环境下的射频模块部分 E_RF 的能量消耗随着网络消息长度的变化呈线性增长。当网络消息的长度从 30 byte 增加到 40 byte 时，由于云计算环境下 XMesh 协议规定的数据包最大负载量是 37 byte，传送 40 byte 的网络数据需要消耗较大的能量惩罚，云计算环境下的射频模块部分 E_RF 的能量消耗增加了 64.2%。

为了验证本文所提方法的有效性，采用文献［8］、文献［9］方法与本文方法对云计算环境中恶意攻击次数与网络节点能量变化之间的关系，分析结果如图 2 所示。

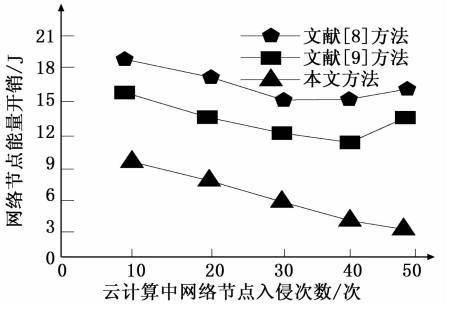

图 2　云计算环境中恶意入侵次数与网络节点能量变化之间的关系

根据图 2 可以看出，文献［8］方法与文献［9］方法的网络节点能量开销随着云计算环境中恶意入侵次数的增加呈现上升趋势，无形中造成了云计算环境下网络节点的能量浪费；而本文方法的网络节点能量开销随着云计算环境中恶意入侵次数的增加逐渐下降且趋于平稳状态，节省云计算环境下网络节点的能量消耗。

为了进一步验证本文所提方法能够保证云计算环境的安全，具有良好的性能，利用 1.2 节中的网络时钟漂移率阈值 θ 对云计算环境下网络数据安全性判断准确率的影响进行分析，分析结果如图 3 所示。

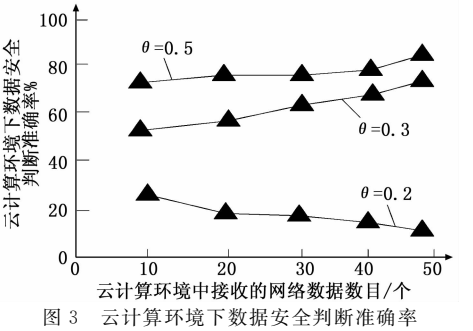

图 3　云计算环境下数据安全判断准确率

定义云计算环境下网络数据安全性判断准确率为：云计算环境下被准确接收并进行同步更新的数据信息/云计算环境下的所有数据信息。

从图 3 中可以看出，当网络时钟漂移率阈值 $\theta=-0.2$ 时，云计算环境下网络数据安全性判断平均准确率为 20%左右；当网络时钟漂移率阈值 $\theta=0.3$ 时，云计算环境下网络数据安全性判断平均准确率为 45%左右；而当网络时钟漂移率阈值 $\theta=0.5$ 时，云计算环境下网络数据安全性判断平均准确率在 75%左右，由此可知，只有将网络时钟漂移率阈值 θ 控制在

（下转第 149 页）