步骤 1. AH选取主节点.

AH内所有节点从各自本地存储的区块中读取h, 计算主节点, AH_i通过:

$$P = (h + v) \bmod n \tag{2}$$

随机决定主节点AH_p, p为主节点的编号. AH_i通过比对p与本节点编号, 判断本节点是否为主节点.

步骤 2. 主节点发起共识.

(1) 主节点AH_p验证m、A并用ECC对m的散列值进行数字签名获得m_{σ_p}, m_{σ_p}表示主节点已验证m、A.

(2) 主节点提取本地存储的区块信息生成包含存储区块版本号、前一区块散列值、h等信息的$block$, 并根据对m、A的验证结果判断是否对$block$使用ECC进行数据签名获得$block_{\sigma_p}$. 如果验证结果为同意接入, 则计算$block_{\sigma_p}$, 否则不计算$block_{\sigma_p}$.

(3) 主节点AH_p向AH中广播包含$< h, v, p, block, block_{\sigma_p} >$的消息, 发起共识.

步骤 3. 副本节点参与共识.

(1) 副本节点AH_i $(i \neq p)$ 收到主节点发送的消息后, 验证m、A, 并用ECC对m的散列值进行数字签名获得m_{σ_i}.

(2) 副本节点$AH_i (i \neq p)$ 根据对m、A的验证结果判断是否对$block$使用ECC进行数据签名获得$block_{\sigma_i}$. 如果验证结果为同意接入, 则计算$block_{\sigma_i}$, 否则不计算$block_{\sigma_i}$.

(3) 副本节点AH_i $(i \neq p)$ 向AH广播包含$< h, v, i, m_{\sigma_i}, block_{\sigma_i} >$的信息.

步骤 4. AH判定共识及操作.

(1) AH内任一节点依据收到的m_{σ_i}、$block_{\sigma_i}$的数量判定共识结果. 若m_{σ_i}、$block_{\sigma_i}$的数量满足关系: $n - f \leq m_{\sigma_i}$的数量$\leq n$, 且$block_{\sigma_i}$的数量$\geq n-f$, 共识结果为同意EH_j接入网络, 并同意生成区块, 此时节点在本地生成共识结果区块, 并将新生成的区块保存在本地; 若m_{σ_i}、$block_{\sigma_i}$的数量满足关系: $n - f \leq m_{\sigma_i}$的数量$\leq n$, $block_{\sigma_i}$的数量$\leq n-f$, 共识结果为拒绝EH_j接入网络, 并拒绝生成区块, 此时节点不做其他操作.

(2) 如果在当前视图下AH在经过$2^{v+i} * t$的时间间隔仍未达成共识或者接收到非法接入认证申请后, 可以更换视图, 直到AH成共识为止. 更换视图的方法为AH_i发起视图更换请求, 视图编号加 1, 当AH_i至少收到$n - f$个来自不同的副本节点返回的响应时, 则返回步骤 1, 重新开始新一轮达成共识的过程.

步骤 5. AH对共识的处理.

(1) AH内已确定共识结果的节点依据共识结果处理此次共识.

(2) 主节点AH_p在获知共识结果后, 处理共识结果, 将共识结果发送给EH_j, 并在AH中广播共识结果.

(3) 在收到主节点AH_p发送的共识结果时仍未知此次共识结果的节点接收主节点AH_p的共识结果, 依据共识结果处理此次共识.

4 实验及结果分析

依据以上对去中心化的网络接入身份认证问题的研究, 本文在 SDN 网络[24–27]中设计并实现了去中心化的接入身份认证方案 BchainNAC. 搭建如图 2 所示的原型环境.

实验环境如下: 一台 OpenDaylight 控制器[28,29]、一台普通交换机、3 台 OpenFlow 交换机、4 台主机. 在交换协议开发平台上部署 Open VSwitch[30,31](开放式虚拟交换机, 简称 OVS) 模拟 SDN 交换机. 使用网桥建立 OpenFlow 交换机与控制器的连接, 由普通交换机作为中转实现控制器与多台 OpenFlow 交换机连接. 主机$h1$、$h2$、$h3$、$h4$为已经连入 SDN 的主机. 主机$h5$为接入认证的申请者. 每一台主机的配置为: CPU 的个数为 1, 核数为 1; 内存容量为 1 GB.

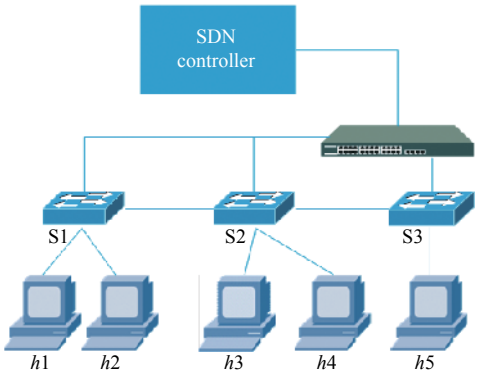

图 2 原型环境

测试场景: 向原型实验环境中逐渐加入 50 台主机, 且每 10 台为一组, 划分为 5 组.

将从申请者发起接入申请到申请者获得认证结果所用的时延记作Tt. 统计每一组加入 SDN 时使用的平均时延Tt, 实验结果如图 3 所示.

测试结果及分析: 参与共识的主机数与完成接入申请所用时延成正比. 从 1 台到 50 台接入 SDN, Tb的增幅不大, 增幅维持在 1 s 之内.

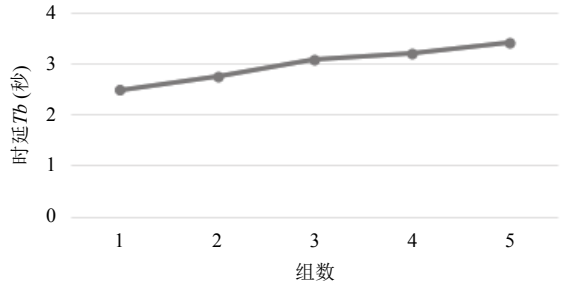

图 3 时延Tb

以组为单位, 分别统计参与共识的主机的 CPU 利用率、内存的使用率, 实验结果如图 4、图 5 所示.

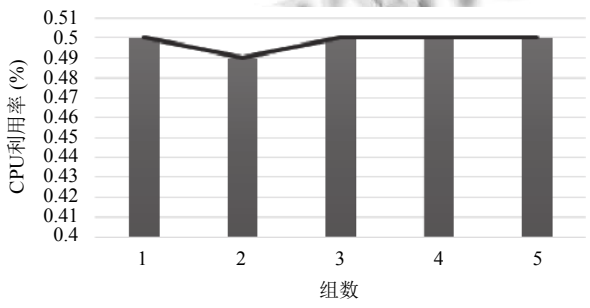

图 4 CPU 利用率

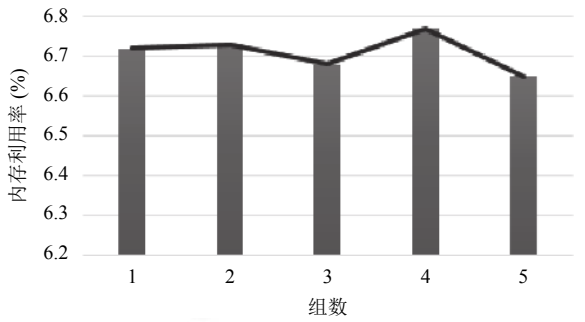

图 5 内存使用率

测试结果及分析: 参与共识的主机 CPU、内存消耗不大, 且每台主机的 CPU 利用率维持在 0.5%、内存使用率维持在 0.67%.

将身份认证共识分成两个部分: 对接入者身份达成共识、通知申请者认证结果和其他节点存储认证结果. 前者使用的时延记作Tc, 后者使用的时延为Tt. 以组为单位, 分别统计每组内平均时延Tc与平均时延Tt占身份认证共识时延的百分比, 实验结果如图 6 所示:

测量结果及分析: 对接入者身份达成共识所用时延为身份认证阶段主要时延. 通过分析, 得知影响共识的主要因素包括: 参与共识的主机的个数; 主机之间通信的质量; 加、解密算法的复杂度.

通过以上实验可知, 在 SDN 网络中, 去中心化的接入身份认证所用时延会随着接入 SDN 网络中主机数的增多而有所提升, 但增幅稳定, 在接受范围之内. 主机因参与共识消耗的 CPU 及内存较低. 通过分析身份认证共识, 可以从影响共识的因素入手, 优化共识过程.

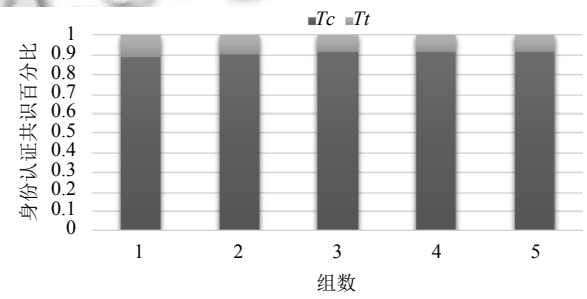

图 6 Tc与Tt占身份认证共识的百分比

5 总结

本文研究去中心化的网络接入身份认证问题, 提出的身份认证方案不泄露除自身公钥以外的任何额外信息, 既满足移动主机接入网络的灵活需求, 又充分考虑网络中主机的不确定性. 下一步将继续优化共识机制的效率, 以便在更大规模网络中推广应用.

参考文献

1 Matias J, Garay J, Mendiola A, *et al*. FlowNAC: Flow-based network access control. Third European Workshop on Software Defined Networks. London, UK: IEEE. 2014. 79–84. [doi: 10.1109/EWSDN.2014.39]

2 王秀磊, 张国敏, 胡超, 等. SDFAC: 软件定义的流接入控制机制. 通信学报, 2015, 36(S1): 188–196.

3 Nayak A, Reimers A, Feamster N, *et al*. Resonance: Dynamic access control for enterprise networks. Proceedings of the 1st ACM Workshop on Research on Enterprise Networking. 2009. 11–18. [doi: 10.1145/1592681.1592684]

4 Lamport L, Shostak R, Pease M. The Byzantine generals problem. ACM Transactions on Programming Languages and Systems, 1982, 4(3): 382–401. [doi: 10.1145/357172.357176]

5 Eduroam Web site: https://www.eduroam.org.
6 公绪晓, 付中南, 吕洁. 基于 eduroam 和 SDN 的无线漫游认证授权技术研究. 华东师范大学学报 (自然科学版), 2015, (S1): 157–162.
7 樊蕊. 跨域身份认证系统的研究与实现[硕士学位论文]. 西安: 西安电子科技大学, 2007.
8 袁勇, 王飞跃. 区块链技术发展现状与展望. 自动化学报, 2016, 42(4): 481–494.
9 Swan M. Blockchain thinking: the brain as a decentralized autonomous corporation. IEEE Technology and Society Magazine, 2015, 34(4): 41–52. [doi: 10.1109/MTS.2015.2494358]
10 Wilson D, Ateniese G. From pretty good to great: Enhancing PGP using bitcoin and the blockchain. Network and System Security. In: Qiu M, Xu S, Yung M, Zhang H, eds. Network and System Security. NSS 2015. Lecture Notes in Computer Science, vol 9408. Springer, Cham. 2015. [doi: 10.1007/978-3-319-25645-0_25]
11 Kraft D. Difficulty control for blockchain-based consensus systems. Peer-to-Peer Networking and Applications, 2016, 9(2): 397–413. [doi: 10.1007/s12083-015-0347-x]
12 李琳, 岳建华. 基于零知识证明的匿名身份认证机制. 计算机科学, 2013, 40(12): 197–199. [doi: 10.3969/j.issn.1002-137X.2013.12.041]
13 李殿伟, 王正义, 赵俊阁. 椭圆曲线密码体制安全性分析. 计算机技术与发展, 2012, 22(4): 227–230.
14 Base58check web site. https://en.bitcoin.it/wiki/Base58Check_encoding.
15 韩家炜, 坎伯. 数据挖掘: 概念与技术 (第 3 版). 机械工业出版社, 2012.
16 Marshall B, Alon R, Manuel S, *et al*. Proofs of Useful Work. http://eprint.iacr.org/2017/203.pdf. [2017-2-27] .
17 韩璇, 刘亚敏. 区块链技术中的共识机制研究. 信息网络安全, 2017, (9): 147–152. [doi: 10.3969/j.issn.1671-1122.2017.09.034]
18 Daniel Larimer. 授权股权证明机制白皮书. http://www.8btc.com/dpos_bitfarm. [2014-04] .
19 卢风顺, 宋君强, 银福康, 等. CPU/GPU 协同并行计算研究综述. 计算机科学, 2011, 38(3): 5–9. [doi: 10.3969/j.issn.1002-137X.2011.03.002]
20 Yu D, He S, Huang Y, *et al*. A fast parallel matrix inversion algorithm based on heterogeneous multicore architectures. 2015 IEEE Global Conference on Signal and Information Processing (GlobalSIP). Orlando, FL, USA. 2015. [doi: 10.1109/GlobalSIP.2015.7418328]
21 范捷, 易乐天, 舒继武. 拜占庭系统技术研究综述. 软件学报, 2013, (6): 1346–1360.
22 王秀群. 可实用的拜占庭容错系统理论研究[博士学位论文]. 杭州: 浙江大学, 2007.
23 Haber S, Stornetta WS. How to time-stamp a digital document. Journal of Cryptology, 1991, 3(2): 99–111.
24 张朝昆, 崔勇, 唐翯祎, 等. 软件定义网络 (SDN) 研究进展. 软件学报, 2015, 26(1): 62–81.
25 左青云, 陈鸣, 赵广松, 等. 基于 OpenFlow 的 SDN 技术研究. 软件学报, 2013, (5): 1078–1097. [doi: 10.3724/SP.J.1001.2013.04390]
26 江国龙, 付斌章, 陈明宇, 等. SDN 控制器的调研和量化分析. 计算机科学与探索, 2014, 8(6): 653–664.
27 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. 软件学报, 2016, 27(4): 969–992. [doi: 10.133280.cnki.jos.005020]
28 许名广, 刘亚萍, 邓文平. 网络控制器 OpenDaylight 的研究与分析. 计算机科学, 2015, 42(S1): 249–252.
29 唐宏, 刘汉江, 陈前锋, 等. OpenDaylight 应用指南. 电信科学, 2017, 33(S1): 267.
30 杨帆, 晏思宇, 黄韬. OVS 的编程扩展技术. 电信科学, 2017, 33(5): 21–28.
31 王文涛, 王奇枫, 郭峰, 等. 基于 Open vSwitch 的 SDN 网络平台构建方法. 中南民族大学学报 (自然科学版), 2014, 33(4): 99–104. [doi: 10.3969/j.issn.1672-4321.2014.04.023]