可穿戴医疗设备的安全方法研究

张彩霞 王向东
(佛山科学技术学院自动化系 佛山 528000)

摘 要 针对可穿戴医疗设备应用中所存在的隐私保护和安全问题,在分析了已有生物密钥和量子密钥的优缺点的基础上,给出了将两者结合并用于可穿戴医疗设备安全保护中的思路;针对可穿戴医疗设备组成的异构网络的数据安全传输问题,在分析已有的密钥预分配方案的基础上,提出将其应用于可穿戴医疗设备构成的动态、异构网络中,为解决可穿戴医疗设备数据安全传输提供理论和技术基础。

关键词 可穿戴医疗设备,量子密钥,生物密钥,异构网络
中图法分类号 TP393 **文献标识码** A

Research on Safety Method of Wearable Medical Devices

ZHANG Cai-xia WANG Xiang-dong
(Department of Automation, Foshan University, Foshan 528000, China)

Abstract This paper researched on the security issues of wearable medical device, analyzed the strengths and weaknesses of biological key and quantum key, and gave an idea to protect wearable medical devices using both biological key and quantum key. Mereover, this paper researched on the security transmission of heterogeneous network composed by wearable medical devices. Based on the analysis of existing key pre-distribution scheme, we proposed to apply it to dynamic and heterogeneous network, to provide theoretical and technical basis for addressing the secure transmission of data.

Keywords Wearable medical devices, Biological key, Quantum key, Heterogeneous network

1 前言

世界卫生组织在2014年年底进行的全球性调查显示,目前全世界有75%的人处于亚健康状态。中国的亚健康人群高达77%。随着亚健康人群的增多和老龄化社会的步入,健康管理日益受到人们的重视[1]。可穿戴医疗设备通过其内置的各种传感器快速、实时、无创、连续地采集患者心率、血压、血氧含量、呼吸频率等各种生理参数,实现对病人关键生理信息的远程监控,改善医疗环境,提高患者生活质量,节约医疗资源(见表1)[2],对于解决我国目前医疗资源短缺、看病难、看病贵的问题具有重要意义。可穿戴设备已经被应用到慢性病管理、疾病预防、健康保健、居家养老等方面。

表1 发达国家在可穿戴医疗设备研究中的结论

研究疾病	地区	主题	结果
糖尿病	美国	出院后的远程监护	每个病人的全部医疗费用可以降低42%
高血压	美国	通过远程设备将主要生命体征信息传送到电子病历中	把两次发病看医生的间隔时间延长了71%
心力衰竭	欧盟	远程监护接受心脏起博器植入的病人	缩短住院时间的35%,降低住院后看医生次数10%
慢性阻塞性肺病	加拿大	远程监控有严重呼吸疾病的病人	降低住院次数10%

图1为携带可穿戴医疗设备的病人和外部网络共同组成的一个无线网络系统,病人信息、环境信息被传输到后台用于病情的监控和治疗。

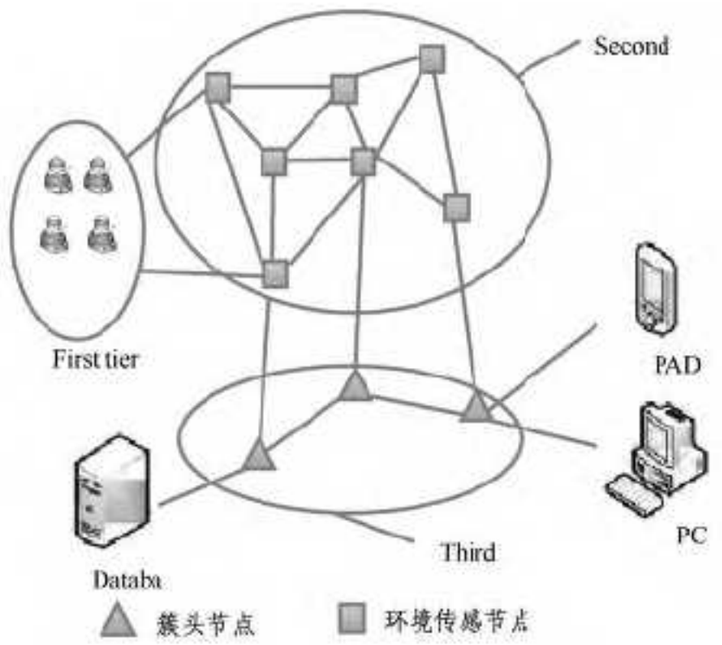

图1 持有可穿戴医疗设备的病人网络

ABI调查数据显示,全球可穿戴设备仅在2014年第一季度就获得30亿美元以上投资金额,全年出货量高达1300万[3],可穿戴设备产业生态体系逐步形成,消费认知不断提高,新技术、新产品大量涌现,跨国公司纷纷抢抓战略布局。

我国在可穿戴医疗设备发展上也表现出了良好的态势,

本文受广东省自然科学基金(2014A030313619,S2013010014485),广东省教育厅项目(2014KTSCX150,2014KZDXM063),广东省科技计划(2013B020314020)资助。

张彩霞(1976—),女,博士,主要研究方向为无线传感器网络安全、智能控制,E-mail:zh-eaixia@163.com;王向东(1962—),男,教授,主要研究方向为非线性数据处理。

据 GSM 对移动医疗业测算，到 2017 年我国可穿戴便携医疗设备市场销售规模将接近 50 亿元[4]。政府发布了《实施 2013 年移动互联网及 4G 产业化专项的通知》，将重点支持智能可穿戴设备的研发及其产业化[5]。国家发改委也将重点支持研发可穿戴设备应用程序、新型人机交互、新型传感、与智能终端互联共享等配套支撑技术，实现可穿戴设备产品产业化。2014 年 12 月，深圳也颁布了《深圳市机器人、可穿戴设备和智能装备产业发展规划(2014—2020 年)》及《深圳市机器人、可穿戴设备和智能装备产业发展政策》[6,7]，确定“可穿戴设备创新、传统产业智能化升级”等重大工程，财政上自 2014 年起连续 7 年每年安排 5 亿元作为市机器人、可穿戴设备和智能装备产业发展专项资金，支持产业发展。

2 问题的提出

目前，国内外对可穿戴医疗设备的研究大多集中在新型应用、情景感知、功耗控制、无线通信技术、MAC 协议等内容上。随着可穿戴医疗设备应用数量和范围的迅速扩大，其安全问题日益受到人们的重视。新技术给患者带来方便的同时，隐私保护将是一个不得不考虑的问题。美国 ONC(健康信息技术全国协调员办公室)[8]针对消费者和设备制造商发布了一系列用于移动健康数据保密的资源；2015 年初，欧盟网络和信息安全局也发布了一份名为“隐私和数据保护的设计_从政策到工程”的前沿报告以弥补法律框架和现有技术实施措施间的缺口[9]，报告展现了在设计隐私和数据保护原则时所面临的挑战和局限性。

可穿戴医疗设备对人体进行感知交互获得的数据必须实现保密性、可靠性、完整性，同时未经授权不能进行身份识别和跟踪等，这些在可穿戴医疗设备应用中显得尤为突出。但是无线信道的开放特性，导致可穿戴医疗设备面临传输信息被监听、位置暴露等安全威胁，由于其传输的数据多为个人健康状况、生活偏好或患者生理信息等个人隐私，因此存在敏感隐私数据泄露或者被恶意篡改、违法使用等风险。因而安全问题成为可穿戴医疗设备发展中不可回避的问题，用户的安全与隐私保障是可穿戴医疗设备得以更广泛应用的前提。

可穿戴医疗设备的隐私保护技术通常包括机密性、认证性、敏感和隐私数据的验证性、完整性、安全数据访问控制策略、不可否认性等方面。如何保证人体信息的机密性、数据产生的可靠性、数据融合的高效性和数据传输的安全性，是可穿戴医疗设备研究需要全面考虑的问题。其中以提供安全、可靠的保密通信为目标的密钥管理是可穿戴医疗设备安全研究中最基本 重要的内容之一[10]。高效的密钥管理方案可以促进可穿戴医疗设备进一步的广泛应用[11]。

然而，可穿戴医疗设备内部多种异构节点共存、多种类型数据并存、设备灵活可移，内部传感节点能量有限、计算能力有限、存储容量有限以及传输通信速率有限，在这样的前提下设计出资源严格受限的可穿戴医疗设备的高效的密钥管理方案的难度极大，且需要综合考虑以下几个带有挑战性的问题：1)在无线通信网络易泄漏有用信息和易受攻击的情况下，如何保证医疗数据隐私性和完整性不受侵犯？2)如何确保医生、护士等授权用户只能存取被授权的相应数据？3)是否在具有能耗较小、扩张方便、应用灵活的前提下具有良好的安全特性？

3 安全方法

3.1 生物密钥

可穿戴医疗设备内部存在多种传感节点，电能、计算能力和存储容量受限，设备灵活可移，因此传统的复杂密钥管理方式不能直接应用于可穿戴医疗设备安全的管理，研究合适的密钥管理方案需要综合考虑各种因素。根据持有者的生物特征生成密钥，从而保护传输数据安全，为可穿戴医疗设备的隐私保护提供了一条可行的解决途径，逐渐成为国内外关注和研究的热点。

生物密钥可分为直接生成法[12]和密钥绑定法[13]。2006 年，生物哈希技术(bio hashing)[12]利用用户生物特征和用户口令产生比特序列作为生物特征密钥。2008 年，Dodis[13]等提出了模糊提取和安全框架的概念，从生物特征中生成密钥，不保存生物数据和特征，该过程不可逆，变为二进制序列的生物密钥便于存储和通信。2010 年，文献[14]使用光电容积脉搏信号(PPG)和心电信号(EKG)使同一个内部生物传感器节点生成对称密钥。2011 年，Mana[15]等提出了一种将公钥体制与生物密钥结合的密钥分发方法，节点生成生物密钥后用中心的公钥加密发送，中心用自己的私钥解密，并与自己生的成参考生物密钥模版进行比较，认证后双方从节点生物密钥中生成会话密钥，该方法可辅助完成密钥分发，实现生物认证，但运算复杂且密钥序列很难做到完全一致。2012 年，Lee 等[16]提出一种具有匿名特性的基于生物特征密钥的协商协议。He 等指出文献[16]中方案不能抵抗特权用户攻击和拒绝服务攻击，并在文献[17]中提出改进协议，该协议使用切比雪夫多项式生成会话密钥，加密用户身份和被传送数据，计复杂度相对较高。以扩展切比雪夫映射为核心，Chen 等[18]对多生物特征 Fuzzy Vault 加密系统中出现的信死锁问题进行深入的研究，利用分离式 Vault 集合构造加密系统，从而通过简化单 Vault 集合构造中真实解锁点选择问题，较好地缓解了多生物特征示例的加密系统中的信息死锁问题。

国内学者对生物密钥也进行了大量的相关研究工作。2009 年，周庆[19]提出由生物特征直接生成系统所需的密钥的思路，其在方便用户操作的前提下降低了系统的成本和复杂性。2011 年，陈熙[20]通过利用手指静脉的细节点特征，并结合模糊保险箱算法，构建了一个生物特征密钥生成系统。邓琦等[21]提出采用切延迟椭圆反射腔混沌系统(TD-ERCS)原理经密钥提取算法直接从生物特征中提取出密钥的方法，并在此基础上提出一种低成本鉴别方案。2012 年，周俊等[22]在虹膜预处理基础上，应用随机映射函数从经过 Haar 小波提取的特征中提取密钥，并通过了 NIST 随机性测试。中国科学院的洪田等[23]设计了一种基于生物特征的躯感网密钥分发机制，即通过传感器节点采集的心血管信号提取心脏搏动间隔，进而生成二进制序列个体识别码，并进一步生成冗余个体识别码，结合模糊承诺法绑定密钥，实现密钥在躯感网内的保密传输，该机制有效降低了密钥分发错误拒绝率和汉明阈值，提高了密钥分发速度。2015 年，舒剑[24]使用切比雪夫多项式来生成会话密钥，使用基于混沌理论的对称密码机制加密用户身份和传送数据，从而实现通信双向认证，抵抗已知攻击。

3.2 量子密钥

近年来量子密钥分发研究得到长足发展。量子密钥分发中身份认证法是一类共享量子信息法，该方法常使用纠缠态作为共享信息。Shi 等[25]对共享纠缠态操作后传输，可在获得密钥的同时验证身份。Li 等[26]将共享纠缠态作为认证密钥，使辅助粒子与认证密钥作用，通过 BELL 测量确认对方身份。基于量子信息认证法虽简便高效，但需要量子存储和纠缠态安全发放，这些问题还未解决，因而这类方法仍处于理论研究阶段。为了提高无线信道数据传输的安全性，有学者尝试在无线网络环境中应用量子密钥分发。2012 年，Djellab 等[27]提出将量子密钥应用于无线网络的方案，该方案使用认证中心分别与通信双方生成密钥，并进行部分密钥交换，从而实现认证与密钥分发。Huang 等[28]将 BB84 协议应用于 Wifi 网络，先用经典方法认证，再用量子密钥分发获取密钥，该方法在通信过程、网络结构方面较为复杂。2013 年，Shi 等[29]基于纠缠交换提出双方和多方的两个量子密钥协商协议；Liu 等[30]指出其多方协议易遭到参与者攻击的问题，并在文献[30]中利用单光子给出一个新的多方量子密钥协商协议。为进一步提高安全性，学者们更多地致力于利用不同量子物理性质[31,32]来实现 QKD，使设计的 QKD 具有更高的效率，更接近于目前的实验技术条件。冯志宏等[33]提出一种基于 Bell 态与其纠缠性质的量子密钥分发协议，用以提高量子密钥分发的效率、可行性和安全性，并给出相应的数学模型和仿真分析。申冬苏等[34]针对最大纠缠态两方量子密钥协议存在的发送方可单方控制共享密钥的问题，通过接收方的幺正操作代替安全检测，从而基本实现了参与者都贡献共享密钥生成和分配的基本要求，使抗发送方攻击不依赖于检测光子技术，该方案可有效抵抗外部攻击和参与者攻击。

3.3 异构网络密钥

生物特征密钥和量子密钥为可穿戴医疗设备实现个体信息传输中的隐私保护提供了较好的思路。但是对于图 1 所示的医疗网络，网络结构动态拓扑且传输数据信息复杂多样，对其数据传输保护需考虑利用简单、高效的无线传感器网络密钥管理方案。

密钥预分配被认为是目前最适用于无线传感器网络的解决思路[35,36]，最早由美国的 Eschenauer 和 Gligor[35]提出，该方案将随机图论引入到密钥管理中，但密钥池大小和预分配密钥环存在一定矛盾。Chan 等[36]提出 q-composite 方案对文献[35]的共享密钥进行改进，使部署后节点间至少共享 q 个密钥才能建立通信，该方案能够有效提高系统的抵抗力，但当被捕节点较多时，网络安全性变差。

异构无线传感器网络在不显著提高网络成本的前提下有效提高了网络的可扩展性和通信效率，能够降低网络的能耗需求，因此，基于异构网络的密钥预分配方案引起了学者的广泛关注[37]。Jolly 等[38]提出一种低能耗的层簇式异构网络密钥预分配管理方案，该方案对存储空间要求不高且计算复杂度低，但网络扩展性教差，多个簇头被捕获会导致整个网络瘫痪。文献[39]在文献[38]的基础上提出基于二元多项式的异构密钥预分配方案，该方案在被俘获簇头节点小于 t 时，二元多项式不会泄漏，从而提高了整个网络的安全性能。文献[40]提出了普通节点间不通信且仅预存 2 个密钥用于与簇头及基站间通信的方案，该方案计算复杂度低和存储消耗小，网络自恢复能力较强，但存在多个簇头节点被俘可能导致整个网络瘫痪的问题。2011 年，Doraipandian 等[41]提出基于 LU 分解且支持组通信和配对节点通信的密钥管理方案，其利用 ElGamal 公钥加密技术加强簇头与基站间的通信安全。2014 年，Khan 等[42]提出一种在线认证的密钥管理模式，其部分适应节点的移动性，但能耗需要进一步降低。JH Lee 等[43]提出利用传感器节点位置感知的方案提高网络安全性，但能耗需要进一步降低。

国内的许多学者也进行了相关的研究。2010 年电子科技大学的徐红兵等[44]利用多项式组成 LU 矩阵密钥池，提高了节点的抗捕获阈值，但能源开销与安全性仍需提高。哈尔滨工程大学的马春光等[45]提出一种基于按对平衡设计的异构无线传感器网络密钥预分配方案，其通过构造异构节点密钥环，在密钥连通率不变的前提下，降低了空间复杂度。2012 年，张彩霞等[46]提出一种基于哈希函数和多项式密钥矩阵的方法提高异构网络簇头安全的方案。覃荣华等[47]将双向散列链和双线性对等方法用于异构无线传感器网络的密钥预分配研究，提高了网络安全性，降低了网络的通信开销。王锁萍等[48]引入虚拟网格技术，采用基于 Blom 矩阵在簇头间通信，实现簇头被捕获时密钥的动态更新。2013 年，钟晓睿等[49]针对现有基于矩阵 LU 的分解的密钥预分配方案易受 LU 攻击的问题，采用扰动技术干扰 LU 的分解结果，有效地抵抗了窃听攻击、LU 攻击和节点捕获攻击。2014 年，胡小春等[50]提出基于树的异构网络密钥预分配方案，该方案以移动 Sink 节点为根节点，并与其通信范围内的传感器节点构成局部树，从而提高了网络连通性。黄廷辉等[51]引入管理节点负责密钥的预分发、成对密钥的建立及更新，有效延长了网络生命周期，但安全性需进一步提高。2015 年，李兰英等[52]将单位设计原理引入异构网络密钥管理中，以第三方服务节点完成簇头间通信，该方案具有较好的可扩展性，但簇头安全需进一步加强。

结束语　目前的生物密钥和量子密钥生成算法都较为复杂，用在电量、存储空间有限的可穿戴医疗设备上有一定的局限性，且单个生物密钥加密数据存在易被破解的危险，如何设计能量消耗较小且加密性能较高的密钥管理方案是一个具有挑战性的问题；另外，异构无线传感器网络的密钥管理研究目前大多集中在静态异构网络模型方面，对于可穿戴医疗设备组成的网络动态拓扑、节点移动频繁、数据多样的异构网络，不能直接应用。因此，研究安全性高、能耗小、网络动态变化的可穿戴医疗设备异构网络密钥管理方案也是一个具有挑战性的问题。

参 考 文 献

[1] 刘金芳. 可穿戴设备的信息安全风险及我国应对建议[J]. 信息安全与技术，2014(11)：10-12

[2] Chen B R，Patel S，Buckley T，et al. A Web-based system for home monitoring of patients with Parkinson's disease using wearable sensors [J]. IEEE Trans on Biomedical Engineering，2011，58(3)：831-836

[3] 2015—2020 年中国可穿戴设备行业分析与投资决策咨询报告[R/OL]. (2014). http://www.chinairr.org

[4] 阮晓东. 可穿戴设备:强势布局移动医疗[J]. 新经济导刊,2015(Z1):46-49
[5] 张越. 我国可穿戴设备产业现状[J]. 中国信息化,2014(17):14-15
[6] 深圳将重点培育机器人可穿戴设备[J]. 领导决策信息,2014,44:14
[7] 深圳发布智能装备产业发展规划政策[J]. 中国安防,2014,24:17
[8] 王宇. 美国网络安全与信息保障研发计划简介[J]. 信息安全与通信保密,2015(1):116-120
[9] 欧盟网络和信息安全局发布前沿报告[J]. 信息安全与通信保密,2015(2):12
[10] Rico J,Sancho J,Díaz Á,et al. Low power wireless sensor networks:secure applications and remote distribution of FW updates with key management on WSN [M]// Trusted Computing for Embedded Systems. Springer International Publishing,2015:71-11
[11] Harris M A,Patten K P. Mobile device security considerations for small-and-medium-sized enterprise business mobility [J]. Information Management & Computer Security,2014,22(1):97-114
[12] Poon C C Y,Zhang Y T,Bao S D. A novel biometrics method to secure wireless body area sensor networks for telemedicine and m-health [J]. IEEE Communications Magazine,2006,44(4):73-81
[13] Dodis Y,Ostrovsky R,Reyzin L,et al. Fuzzy extractors:How to generate strong keys from biometrics and other noisy data [J]. SIAM Journal on Computing,2008,38(1):97-139
[14] Venkatasubramanian K K,Banerjee A,Gupta S K S. PSKA:Usable and Secure Key Agreement Scheme for Body Area Networks [J]. IEEE Transactions on Information Technology in Biomedicine,2010,14(1):60-68
[15] Mana M,Feham M,Bensaber B A. Trust Key Management Scheme for Wireless Body Area Networks [J]. IJ Network Security,2011,12(2):75-83
[16] Lee C C,Chen C L,Wu C Y,et al. An extended chaotic maps-based key agreement protocol with user anonymity [J]. Nonlinear Dynamics,2012,69(1):79-87
[17] He D,Chen Y,Chen J. Cryptanalysis and improvement of an extend-ed chaotic maps-based key agreement protocol [J]. Nonlinear Dynamics,2012,69(3):1149-1157
[18] Chen H,Zhao H,Pang L,et al. Multi fuzzy vault based on secret sharing for deadlock restoration [J]. International Journal of Information Technology and Management,2012,11(1):50-60
[19] 周庆,胡月,廖晓峰. 一种基于 TD-ERCS 的生物特征密钥产生算法[J]. 物理学报,2009(7):4477-4484
[20] 陈熙. 鉴别生物特征提取及密钥生成研究[D]. 成都:西南交通大学,2011
[21] 邓琦,佟国香. 一种基于 TD-ERCS 生物特征密钥提取的鉴别方案[J]. 微计算机信息,2011(1):197-199
[22] 周俊,曹琦,王帅. 基于虹膜特征的密钥生成研究[J]. 计算机工程与应用,2012(21):31-34
[23] 洪田,鲍淑娣,张元亭. 基于生物特征的躯感网密钥分发机制[J]. 传感器与微系统,2012,31(2):19-31
[24] 舒剑. 一种使用扩展混沌映射的基于生物特征密钥协商协议[J]. 小型微型计算机系统,2015(3):524-528
[25] Shi B S,Li J,Liu J M,et al. Quantum key distribution and quantum authentica-tion based on entangled state [J]. Physics Letters A,2001,281(2/3):83-87
[26] Li X,Chen L. Quantum authentication protocol using bell state [C]// The First International Symposium on Data,Privacy,and E-Commerce. IEEE,2007:128-132
[27] Djellab R,Benmohammed M. Securing encryption key distribution in WLAN via QKD [C]// 2012 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery. IEEE,2012:160-165
[28] Huang X,Wijesekera S. Quantum cryptography based key distribution in WiFi networks [C]// 2012 International Conference on Information Networking. IEEE,2012:251-256
[29] Shi R H,Zhong H. Multi-party Quantum key agreement with bell states and bell measurements [J]. Quantum Information Processing,2013,12(2):921-932
[30] Liu B,Gao F,Huang W,et al. Multiparty Quantum key agreement with single particles [J]. Quantum Information Processing,2013,12(4):1797-1805
[31] Simon D S,Lawrence N,Trevino J,et al. High-capacity quantum Fibonacci coding for key distribution [J]. Physics Review A,2013,87(3):032312
[32] Leverrier A,García-Patrón R,Renner R,et al. Security of continuous-variable quantum key distribution against general attacks [J]. Physics Review Letters,2013,110(3):030502
[33] 冯志宏,谭晓青,梁翠. 基于 Bell 态与其纠缠性质的量子密钥分发 [J]. 计算机应用研究,2015(3):873-876,880
[34] 申冬苏,马文平,尹逊汝,等. 两方量子密钥协商协议的改进[J]. 西安电子科技大学学报,2015(1):86-90,186
[35] Eschenauer L,Gligor V D. A key management scheme for distributed sensor networks [C]// Proceeding of the 9th ACM Conference on Computer and Communications Security. Washington,2002:41-47
[36] Chan H,Perrig A,Song D. Random key predistribution schemes for sensor networks [C]// 2003 IEEE Symposium on Security and Privacy. Berkeley,USA,2003:197-213
[37] Babar S D,Prasad N R. CMKMS:Cluster-based mobile key management scheme for wireless sensor network [J]. International Journal of Pervasive Computing and Communications,2014,10(2):196-211
[38] Jolly G,Kuscu M C,Kokate P,et al. A low-energy key management protocol for wireless sensor networks [C]// Proceedings of the Eighth IEEE International Symposium on Computers and Communication. Turkey,2003:335-340
[39] Cheng Y,Agrawal D P. An improved key distribution mechanism for large-scale hierarchical wireless sensor networks [J]. Ad Hoc Networks,2007,5(1):35-48
[40] Wang W,Li F,Ma J. Efficient and secure group key management for high delay networks [J]. Chinese Journal of Electronics,2007,16(4):721-726
[41] Doraipandian M,Rajapackiyam E. An efficient and hybrid key management scheme for three tier wireless sensor networks using LU matrix [J]. Communications in Computer and Infor-

mation Science,2011,192(3):111-121

[42] Khan S U, Lavagno L, Pastrone C. Online Authentication and Key Establishment Scheme for Heterogeneous Sensor Networks [J]. International Journal of Distributed Sensor Networks, 2014,2014:1-11

[43] Lee J H,Kwon T,Ehlers F. Location-Aware Key Management for General Deployment of Wireless Sensor Networks [J]. International Journal of Distributed Sensor Networks,2014,2014:1-17

[44] Dai H,Xu H. Key predistribution approach in wireless sensor networks using LU matrix [J]. IEEE Sensors Journal,2010,10(8):1399-1409

[45] 马春光,张秉政,孙原. 基于按对平衡设计的异构无线传感器网络密钥预分配方案 [J]. 通信学报,2010,31(1):37-43

[46] Zhang C X,Cheng L L,Wang X D. Efficient key pre-distribution protocol for Heterogeneous wireless sensor networks [J]. Journal of Computational Information Systems, 2013, 9(11): 4583-4592

[47] 覃荣华,解永生,袁晓兵. 异构分组无线传感器网络密钥管理机制 [J]. 华中科技大学学报(自然科学版),2012,40(4):19-42

[48] 掌明,王锁萍,徐鹤. 基于分簇的无线传感器网络动态密钥管理方案 [J]. 南京邮电大学学报(自然科学版),2012,32(1):98-103

[49] 钟晓容,马春光. 一种抗 LU 攻击的传感器网络密钥预分配方案 [J]. 计算机学报,2013,36(6):1155-1167

[50] 胡小春,陈燕,梁俊斌,等. Sink 移动的无线传感网中高连通性密钥预分配方案研究[J]. 数学的实践与认识,2014,44(6):128-134

[51] 黄廷辉,杨旻,崔更申,等. 基于 LEACH 协议的无线传感器网络密钥管理路由方案[J]. 传感技术学报,2014(8):1143-1146

[52] 李兰英,易春焕,孙建达,等. 基于单位元的无线传感器网络密钥管理方案[J]. 计算机工程与应用,2015(2):94-98

(上接第 341 页)

API)。其认证过程如图 7 所示。用户会对 GUI 服务器提供一个认证码的 OpenID 认证请求。OP 服务器通过调用 API 服务器来提取消息摘要,并与数据库存储的消息和上次个人登录标识进行对比,若一致则不是钓鱼网站,否则可能是钓鱼网站。若确定安全,前端会调用认证请求 API,并返回需要重定向的所有 OpenID 参数。GUI 服务器会分析信息并向 UA 发送重定向命令。UA 会重新定向 OP,并进行验证,一旦验证成功,OP 会把 UA 重定向到 GUI 服务器,并调用认证验证 API 对所有的过程进行验证,成功就会允许用户登录界面,否则就失败

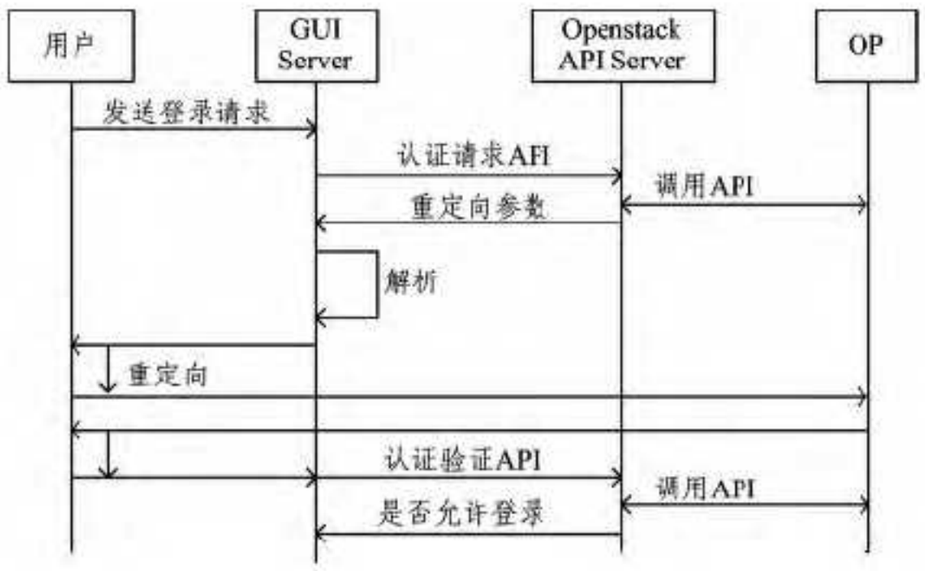

图 7 openstack 中 OpenID 的认证流程

结束语 安全是信息化时代最重要的问题,随着云计算的发展,如何保障信息安全不被泄露,也是云计算进一步发展所必须要考虑的问题。身份认证作为访问云计算资源的第一步,身份认证的安全性问题是当前云计算安全领域最重要的问题,其研究也受到了各界的广泛关注,近年来也取得了一定的进展。本文主要对当前云计算中主流的身份认证技术 SAML、OAuth 和 OpenID 做了大致的介绍,重点讲解了身份认证机制原理并在此基础上提出了 OpenID 身份认证当前的一些缺陷,同时做了一些改进。对 openstack 中的认证组件 Keystone 框架进行了深层解析,通过对其对象模型和认证原理的研究,分析出了当前 Keystone 组件的安全性问题,并将 OpenID 身份认证改进方案应用到 openstack 中,更进一步增加了其安全性。

参 考 文 献

[1] Hu Luo-kai, Ying Shi, Jia Xiang-yang, et al. Towards an Approach of Semantic Access Control for Cloud Computing[C]// Cloud Computing, 2009. Beijing, China: Springer Berlin Heidelberg,2009:145－156

[2] OASIS Standard. SAMLV2.0[EB/OL]. (2005). http://docs.oasis-open.org/security/saml/v2.0

[3] 江浩浩,徐东升. SAML 在集成身份认证中的应用[J]. 电信网技术,2012(7):17-21

[4] 王群,李馥娟,钱焕延. 云计算身份认证模型研究[J]. 电子技术应用,2015,41(2):135-138

[5] 江伟玉,高能,刘泽义,等. 一种云计算中的多重身份认证与授权方案[J]. 信息网络安全,2012(8):7-10

[6] 秦晓娜,郝平,何恩. 基于 OpenID 安全认证的 Web 实时通信系统[J]. 信息安全与通信保密,2013(4):70-72

[7] 夏晔,钱松荣. OpenID 身份认证系统的等级模型研究[J]. 微型电脑应用,2011,27(4):20-23

[8] Wei J,Zhang M,Ding X,et al. Research on Multi-Level Security Framework for OpenID[C]// International Symposium on Electronic Commerce & Security,2010. 2010:393-397

[9] 吴志勇,孙乐昌. 针对钓鱼攻击的防范技术研究[J]. 信息安全与通信保密,2006(11):126-128

[10] 张进铎,毛承国,李硕,等. Openstack 开源云平台主模块的架构分析[J]. 信息化技术与信息化,2014(4):244-247

[11] Sitaram D, Phalachandra H L, Vishwanath A, et al. Keystone Federated Security[C]// ICITST. 2013:659-664

[12] 熊微,房秉毅,张云勇,等. OpenStack 认证安全问题研究[J]. 邮电设计技术,2014(7):21-25

[13] Khan R H,Ylitalo J,Ahmed A S. OpenID Authentication As A Service in OpenStack[C]// Internation Conference on Information Assurance & Security,2011. 2011:372-377

[14] Chadwick, David W, Matteo C. Security APIs for My private cloud-granting access to anyone, from anywhere at anytime[C]// Third IEEE International Conference on Cloud Computing Technology and Science,2011. 2011:792-798