物联网中认证技术研究

闫宏强[1,2]，王琳杰[3,4]

（1. 中国科学院计算机网络信息中心，北京 100190；2. 中国科学院大学，北京 100049；
3. 铜仁学院大数据学院，贵州 铜仁 554300；4. 贵州大学计算机科学与技术学院，贵州 贵阳 550025）

摘 要：物联网认证技术是物联网安全领域的关键技术，它确保接入物联网的用户和设备节点身份信息的真实性。由于物联网设备的低成本、低功耗、小存储和网络的异构性等特点，使传统计算机网络中的身份认证机制往往无法适用。首先介绍了物联网发展历程，分析了物联网安全风险和认证工作面临的挑战，着重比较了 5 种典型的认证协议的优缺点，进而对 RFID、智能电网、车联网、智能家居等几种实践场景下的认证技术进行总结和对比分析。最后，讨论了未来物联网认证技术的研究方向。

关键词：物联网；认证技术；轻量级协议；安全认证

中图分类号：TP309，TP311.13

文献标识码：A

doi: 10.11959/j.issn.1000−436x.2020131

Research of authentication techniques for the Internet of things

YAN Hongqiang[1,2], WANG Linjie[3,4]

1. Computer Network Information Center, Chinese Academy of Sciences, Beijing 100190, China
2. University of Chinese Academy of Sciences, Beijing 100049, China
3. School of Data Science, Tongren University, Tongren 554300, China
4. State Key Laboratory of Public Big Data, College of Computer Science Technology, Guizhou University, Guiyang 550025, China

Abstract: Identity authentication technology is a key technology in the Internet of things (IoT)security field which ensures the authenticity of the identity information of users and device nodes connected to the IoT. Due to the low cost, low power consumption, small storage of IoT devices and heterogeneity of IoT network, the identity authentication mechanisms in traditional computer networks are often not applicable. Firstly, the development process of IoT was introduced, the security risks of IoT and the challenges faced by the authentication work were analyzed. Then the emphasis was put on comparison of the advantages and disadvantages among five typical authentication protocols. Moreover, the authentication technologies in several practical scenarios of RFID, smart grid, Internet of vehicles, and smart home were summarized and analyzed. Finally, the future research direction was discussed.

Key words: IoT, authentication technique, light-weight protocol, secure authentication

1 引言

1.1 物联网概念发展历程

20 世纪 90 年代，美国麻省理工学院（MIT, Massachusetts Institute of Technology）的 Kevin Ashton 教授首次提出物联网（IoT, Internet of things）的概念[1]。1999 年，MIT 建立了自动识别中心（Auto ID），Kevin Ashton 教授是创建者之一。Auto ID 阐明了物联网的基本含义，是指将所有物品通过射频识别等信息传感设备与互联网连接起来的网络。

收稿日期：2020−03−20；**修回日期：**2020−05−26

通信作者：王琳杰，wanglinjie_66@hotmail.com

基金项目：国家自然科学基金资助项目（No.61962009, No.61662009）

Foundation Item: The National Natural Science Foundation of China (No.61962009, No.61662009)

2005 年，国际电信联盟（ITU, International Telecommunication Union）发布了《ITU 互联网报告 2005：物联网》对“物联网”的含义进行了扩展，指出物联网是人和物之间、物和物之间进行信息交换的全新通信形式。2017 年发布的国家标准 GB/T 33745-2017《物联网术语》给出物联网的定义，即“通过感知设备，按照约定协议，连接物、人、系统和信息资源，实现对物理和虚拟世界的信息进行处理并做出反应的智能服务系统”，其中，“物”即物理实体。随着物联网的发展成熟，其内涵和外延也在不断发生变化，系统一般包含用户、物联网设备和物联网服务 3 个实体，系统模型如图 1 所示。

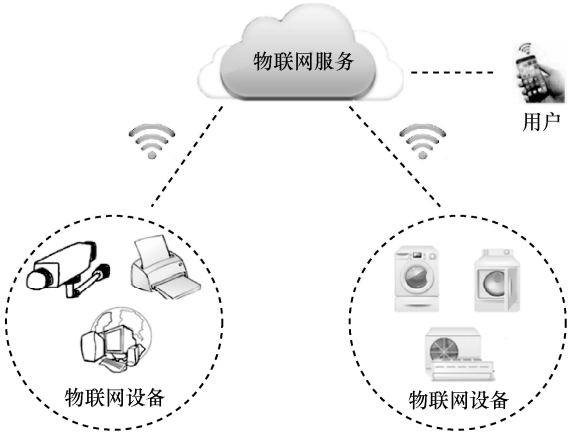


图 1 系统模型

1.2 物联网发展现状与趋势

近年来，随着信息通信技术的变革发展与创新突破，窄带物联网技术（NB-IoT, narrow-band IoT）、加强的机器类型通信（eMTC, enhanced machine-type communication）、远距离无线电技术（LoRa, long range）等低功耗广域（LPWA, low-power wide-area）技术和应用不断创新突破，在大数据、人工智能等技术飞速创新发展的推动下，物联网规模急速壮大，物联网应用层出不穷，物联网产业发展迅速，进入黄金发展阶段。

物联网中设备的数量呈指数级增长趋势，这些设备被广泛应用于公共卫生、智能电网、智能交通、垃圾管理、智能家居、智慧城市、智慧农业、能源管理等领域[2-3]。根据思科[4]基于第三方机构 IDC（Internet Data Center）的调研结果发布的一份预测报告显示，到 2022 年，全球将有 286 亿台物联网设备投入使用。文献[5-6]的报告估计，到 2025 年，物联网每年创造的价值将达到数万亿美元。

据 GSMA Intelligence 于 2019 年 11 月发布的第四次年度全球移动趋势报告《2020 年全球移动趋势》预测，到 2025 年，全球物联网设备连接数量将达 252 亿台，年平均增长率达 15%。2019 年《物联网技术行业应用年度研究报告》发布，预测到 2025 年，我国物联网连接数将达 53.8 亿台。卡巴斯基于 2020 年 2 月发布的《物联网商业应用成效与挑战》报告指出，当前 61%的组织在其业务中使用了物联网平台，IT 和电信行业的使用率更是达到 71%。

1) 物联网催生智慧城市等新兴应用领域。物联网的快速发展催生了智能家居、智慧城市、个人智能穿戴等新兴应用领域。卡巴斯基《物联网商业应用成效与挑战》报告指出，全球物联网增长最快的领域是智慧城市。通过自动感知、数据采集、智能控制，物联网推动打造智慧城市，在运输管理、交通控制和视频监控等领域实现精细管理和优化服务，提升城市效率，惠及百姓生活。当前，我国许多城市正在推进“智慧城市”规划，主要应用在公共安全、交通、医疗、社区、环保、地下管网监测、水务、教育等领域。这些应用均以自动感知为基础、以数据采集为手段、以智能控制为核心，实现了物联网技术的综合集成应用。

2) 物联网支撑传统行业数字化转型。物联网赋能传统行业，促进交通、医疗、物流、工业、农业、制造业、安防等行业数字化转型。例如，在智能物流领域，通过物联网技术实现对货物的检测和运输车辆的跟踪，实现了物流运输、仓储、配送等各个环节的全面感知和分析，提升了物流行业的运输效率和智能化水平；在工业和制造业领域，工业物联网（IIoT, industrial Internet of things）技术使企业将传感器连接到机器上，感知万物信息，并基于大数据分析技术，实现智能决策和判断，提高生产效率和产能。

2 物联网认证安全问题与挑战

物联网产业高速发展的同时，也带来了新技术应用的安全风险。物联网遭到攻击，可能导致网络瘫痪，基于国家安全、人身健康和生命财产安全都可能受到严重威胁和损失。近年来，物联网安全攻击事件日益频发，对用户隐私、数据安全、基础网络环境的安全冲击也越来越突出。根据 Gartner 报告，20%的组织在过去的三年中，至少经历了一次

物联网攻击[7]。

2.1　物联网安全风险点

与传统互联网相比，物联网的安全问题更加复杂。一般来说，物联网的网络架构主要包括终端接入层、网络传输层和应用服务层，其安全问题可分为终端、通信网络和应用服务的风险。

终端安全的风险主要表现在终端的物理安全、网络通信及结构安全、数据泄露、安全漏洞等[8-9]。如果终端被黑客利用或控制，还有可能成为 Mirai 僵尸网络[10-11]等安全威胁。通信网络的风险主要表现为无线数据的传输链路安全、非授权接入和访问网络等方面。应用服务由于其服务器存储大量数据、应用逻辑多样等特点，易被黑客利用系统的基础环境及组件存在的漏洞发起攻击。

据 Gartner 的另一项研究显示，2018 年全球企业在物联网安全方面的损失达到 15 亿美元。据估计，到 2022 年，用于故障补救、安全故障和召回等方面的预算资金将达到各个公司用于安全保护预算的一半[12]。近年来，全球发生诸多物联网安全事件。2016 年 10 月，攻击者利用摄像头安全漏洞，通过恶意软件对美国西海岸大批摄像头进行控制，进而对域名系统（DNS, domain name system）服务器发起分布式拒绝服务攻击，导致大面积通信瘫痪。2017 年，1 000 余台利盟（Lexmark）打印机在线暴露，研究人员确认这些打印机均没有设置密码保护，涉及众多国家政府部门。这意味着攻击者一旦在互联网上发现这些打印机，便可执行各种攻击操作，如添加后门、劫持打印作业等。2018 年，西班牙某工控物联网设备制造商将投向市场的某款电动汽车智能充电系统大范围暴露在公网之上，且存在未授权访问的漏洞。若存在攻击者，其不仅可以获取敏感信息，甚至可执行固件升级等操作。2019 年 12 月，美国密西西比州一间房屋的智能摄像头遭入侵，黑客不仅与屋内人对话，还可以看到屋里的一举一动，用户隐私和生活秩序受到严重威胁。

2.2　物联网认证流程

认证是用户和设备接入物联网系统的第一步，是确保信息资源被合法访问的重要保障。一个基本的用户相互身份认证方案基本由图 2 所示步骤中的两步、三步或者全部步骤构成。

在系统的初始阶段，每个用户都有自己的身份 ID_i 和相对应的初始密钥 k_i，(ID_i, k_i) 保存在云服务器中，用于最初的身份确认和后期的身份认证服务。

1) 用户使用自己的身份 ID_i 向云服务器发送会话请求。

2) 云服务器从自己存储的数据名单中查找 ID_i 及相对的初始密钥 k_i，随机选择新的通话密钥 μ_{key}，用 μ_{key} 和随机数 r_i 通过预存公式求得 y_i（例如 y_i=hash($\mu_{\mathrm{key}} \| r_i$)），然后使用密钥 k_i 利用轻量级密码算法 LigwEnc 计算 Y_i=LigwEnc$\{k_i, (\mu_{\mathrm{key}} \mid y_i)\}$ 并发送给用户。

3) 用户收到 Y_i 后，利用自己的初始密钥 k_i 可计算得到 μ_{key}。随机选择 z_i，用 z_i 和 y_i 通过预存公式计算 p_i，然后用新密钥 μ_{key} 计算 Z_i=LigwEnc$\{\mu_{\mathrm{key}}, (p_i \mid z_i)\}$ 并发给云服务器。

4) 云服务器收到 Z_i 后用密钥 μ_{key} 解密得到 z_i，计算 LigwEnc$\{k_i, (\mu_{\mathrm{key}} \mid z_i)\}$ 并发给用户。

通过上述过程，可以完成用户和云服务器的相互认证。

2.3　物联网认证安全问题与挑战

物联网设备的可信认证是确保信息资源被合法访问的第一道关口。物联网认证机制的安全目标是认证数据发送者身份信息的真实性，确保特定数据的有效性和数据完整性，确保接收数据的新鲜性，确保其没有重放过时的数据。提供可靠的用户和设备的身份

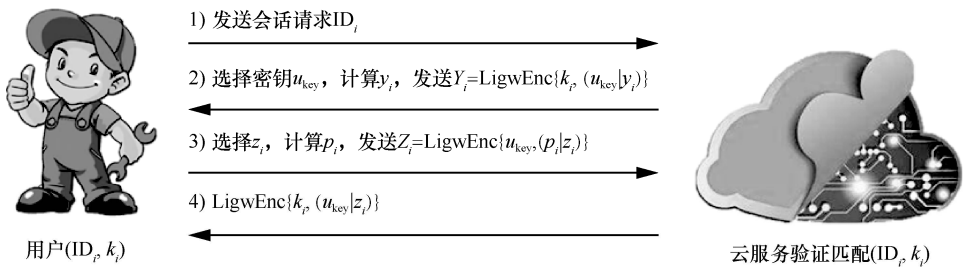


图 2　认证方案模型

接入认证和管理解决方案，能确保物联网设备的安全连接，给设备使用者提供安全授权访问。

由于物联网中的设备存在着对计算能力、内存存储要求、动态安全更新及物理变量捕捉的保护等方面的挑战，以及设备本身存在的一些局限性（有限的计算能力和存储空间、资源限制需求和支持动态更新等），使传统的计算机认证协议不能直接在物联网设备中使用，从而导致物联网面临一些安全问题和挑战[13-15]。物联网设备易被攻击者利用，来获取用户的身份认证信息，进而伪造用户身份或通信节点，并向其他物联网终端设备、接入网关等进行入侵和攻击。

1) 有限的计算能力和存储空间

在物联网环境中，互联设备（如物联网传感器）往往配置了低速处理器和有限的内存存储。这些设备不能执行需要高计算能力和高内存存储的昂贵计算操作，因此，设计一个能最大限度降低资源消耗（计算存储和内存存储）和最大限度提高安全性能的解决方案变得很有挑战性。鉴于此，在为这样的环境设计用户身份认证方案时，可以使用轻量级的加密操作，例如，高级加密标准（AES, advanced encryption standard）算法[13]、异或操作[16]、加密单向哈希函数[17]和椭圆曲线[18]。

2) 资源限制需求

在某些给定的环境中，大多数物联网设备的设计尺寸都很小，其固有的资源（电池、处理和存储）有限。当不需要工作时，这些设备将自动打开省电模式来节约能源，但是，由于电池资源存储量的局限性，导致的主要挑战是为高度受限的设备开发轻量级的安全机制。因此，为这种在资源受限环境中工作的设备设计一种用户认证方案时，最好采用轻量级的密码体制，如 AES 算法和加密单向哈希函数[13,16-17]。

3) 支持动态更新

为了克服现有某些方案的安全漏洞，需要保持最新的安全方案，因此就要进行方案计划的不定时更新。例如，在新智能设备添加或删除某些相连设备时，需要更新这个设备存储[16,18]。因此，设计一种既支持动态安装或更新又不影响安全性的方案，也是一个具有挑战性的任务。

3 物联网认证技术

3.1 认证技术简介

物联网应用中，通过身份认证来识别用户、设备并限制非授权用户非法操纵设备。在物联网中，组件之间可以相互通信，并且可以共享数据，这就要求每个用户或设备都能够对其他对象和设备进行身份认证。文献[19]中给出了几种常用的身份认证模型，如图 3 所示，模型描述如表 1 所示。在大多数情况下，网关节点（GWN, gateway node）无法直接使用用户发送的信息进行身份认证，这时远程部署的传感器节点可以帮助它们完成身份认证。

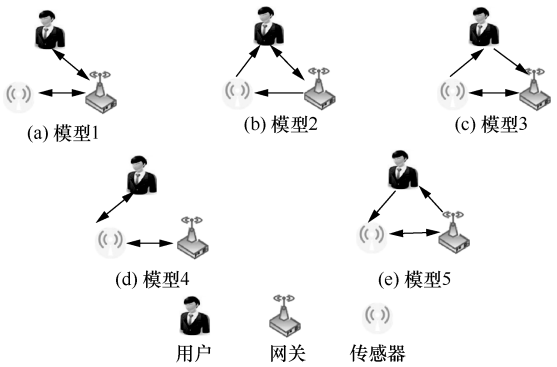


图 3 物联网网络认证模型

另外，在物联网中对跨异域设备进行身份认证也是一个巨大挑战。现有的方案依赖于用户名和密码，或者只使用单一的身份认证模式，可能这不是处理物联网异构性所需的合适解决方案，主要的原因是它很容易被破坏[20]。物联网中的设备在使用时有很多限制，如低功耗、有限的内存、移动性和支持多个网络协议[21]，基于这些原因，认证技术被认

表 1 物联网网络认证模型描述

认证模型	描述
模型 1	用户将身份认证请求发送给 GWN，GWN 将用户信息发送给传感器，传感器确认用户信息并将信息反馈给 GWN，GWN 收到信息后对用户进行身份认证
模型 2	用户将认证请求发送给 GWN，GWN 将其认证密钥发送给用户，并同时将用户信息发送给传感器，然后传感器对用户进行身份认证
模型 3	用户将认证请求发送给 GWN，GWN 将用户信息发送到传感器，然后传感器将自己的密钥反馈给 GWN 并同时认证用户
模型 4	用户将身份认证请求发送给传感器，然后传感器将请求返回给 GWN，GWN 向传感器发送确认信息，最后传感器认证用户
模型 5	用户将身份认证请求发送给传感器，然后传感器将请求返回给 GWN，GWN 对用户进行身份认证，并向传感器发送一个确认信息

为是物联网安全的关键技术，通过了可信认证的物联网设备对网络的正常运行至关重要[22]。

3.2　物联网认证协议的类型

在物联网中，身份认证是认证用户和设备节点可信身份的过程，该过程十分重要，可以保护物联网免受非法入侵和攻击。然而，由于不同的协议对认证的设计和保护机制各不相同，以及物联网低成本、低功耗、小存储和异构性等局限性，导致很多传统计算机网络中的身份认证机制无法在物联网中使用，因此需要设计符合物联网场景的身份认证方案。研究人员设计了数千种身份认证协议，根据文献[23]的分析基本可分为基于密码的身份认证、基于媒体访问控制（MAC, media access control）地址的认证、基于用户公开身份的身份认证、基于令牌的认证和基于生物特征的认证等。图 4 给出了物联网中身份认证的分类。

3.2.1　基于密码的身份认证

基于密码的身份认证是认证用户或设备的一种常见的方法。该认证模式需要用户提供一个唯一的 ID 和密码，该 ID 和密码组合存储在身份认证服务器的数据库中。当用户提供了 ID 和密码的组合时，协议将匹配所提供的组合和保存的凭据，如果匹配，则协议允许用户或设备执行所需的操作。该认证方式可以抵抗重放攻击、中间攻击、侧信道攻击等攻击，但是也存在以下缺点：需要额外的应用程序或协议来连接、不能抵抗可抵赖攻击、依靠复杂的计算、高安全性依靠高功耗和高处理代价、无法用于没有键盘鼠标等输入设备的物联网设备中。此项技术主要用于服务器/客户端身份认证环境。

3.2.2　基于 MAC 地址的认证

基于 MAC 地址的认证是通过使用 MAC 地址的模式进行认证的，MAC 地址是分配给网络接口的标识地址，主要用于内部网环境中的网络访问控制。当设备请求访问网络时，将服务器中注册的 MAC 地址与从设备请求的消息发送的 MAC 地址进行比较，从而进行身份认证的过程，它比基于密码的身份认证方法更简单、更快[24]。但是，随着物联网设备数量的增加，如果超出了 MAC 地址格式的最大标记数量，则需要定义新的地址格式标准。此外，由于 MAC 地址容易被伪造，因此容易受到伪造等欺骗行为的攻击[25]。

3.2.3　基于用户公开身份的身份认证

基于用户公开身份的身份认证是一个使用用户（客户端）ID 的公钥密码系统，它的公钥包括电子邮件地址、名称、公开的 IP 地址和签名，该方案在实现安全性的同时还提供身份认证。该模式具有密钥分配独立、算术运算量小、密钥长度相对较短等优点，但也存在易受身份欺骗攻击和不满足不可否认性的缺点。

3.2.4　基于令牌的认证

令牌是由身份认证服务器创建的一段数据，用于唯一地标识用户或设备。该种身份认证分为 2 种方式，一种是服务器填充一次性密码并将其发送到注册的通信媒体，该媒体与该账户相关联，并保留已传输的一次性密码的副本；服务器通过对该一次性密码与存储的一次性密码进行匹配而进行身份认证。另一种是在系统中嵌入一段信息以进行自我

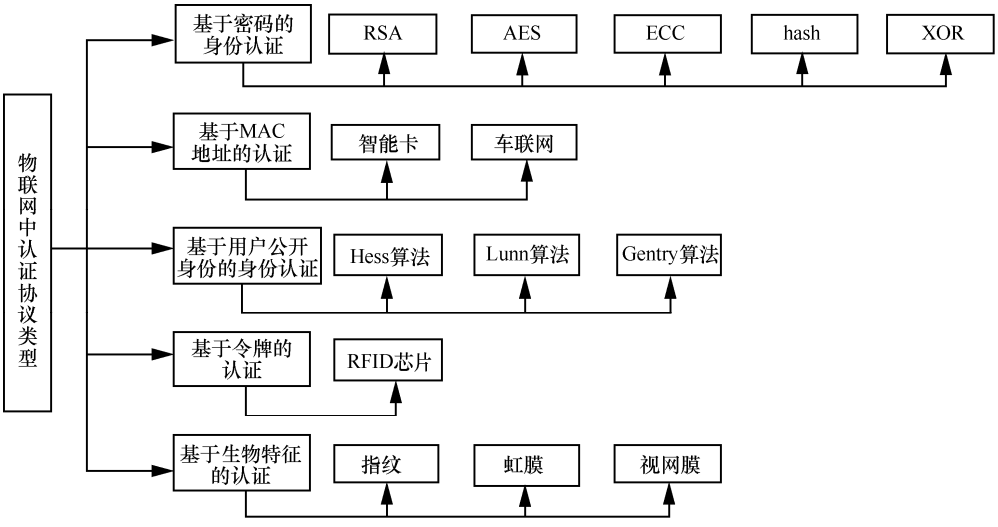


图 4　物联网中身份认证的分类

认证的小型设备或卡片，该系统都将对服务器的每个请求基于令牌的正确组合进行响应。

令牌身份认证设备，比如加密狗、智能卡和射频识别（RFID, radio frequency identification）芯片等，一般具有便于随身携带、价格相对便宜、简易性等优点，其记录的信息具有高可靠性与高保密性，因此令牌身份认证设备在实践中被广泛接受和使用。但是以该协议为基础的制成设备也存在一些不足，如不能实现用户的可追踪性、保证前向安全性、难以抵抗密码猜测攻击等。

3.2.5 基于生物特征的认证

生物特征的认证是基于人的生物学特性进行的，该方案是利用特定的生物扫描仪从用户收集独特的生物数据，并与通过注册过程收集的存储数据相匹配。常用的生物特征包括指纹认证、人脸认证、虹膜认证、视网膜认证、手势认证和语音认证等。其中，虹膜认证方法是使用数学模式来识别一个或2个虹膜，这对个人来说是独一无二的。同样，指纹认证在物联网机制中也很常见，通过预先在服务器中保留相同的信息来检查人类手指的纹路。

由于生物特征的独一无二性，基于该特征的认证技术可以抵抗窃听、冒充、拒绝服务等攻击。但是该认证方式也存在局限性，例如认证需要特定的生物特征设备、系统管理和建设成本比较高、工作范围常常受限（比如指纹和刷脸认证距离往往限于0.5～1 m）等。另外，随着技术的快速发展，某些时候生物识别特征也变得容易被伪造，为此需要开发不易伪造的生物识别技术。

3.3 不同应用认证技术对比分析

3.3.1 RFID技术

RFID是一种无线技术，通常由RFID标签和RFID阅读器两部分组成。RFID通常用于供应链、医疗、气候传感等领域[22]。

由于采用RFID的物联网设备CPU结构简单、存储容量小、计算能力弱，无法使用复杂的加密算法来进行身份认证。文献[26-27]提出了基于RFID物联网应用程序的相互身份认证方案，方案中使用了轻量级加密算法，可以加快认证速度、降低计算成本、增加安全存储能力。

Gope等[17]提出了一种应用于物联网的解决匿名的轻量级RFID身份认证方案。该方案基于网络模型的4个实体，包括2个服务器（即得到认证的云和后端数据库）、读取器和RFID标签。该方案以不可链接的匿名身份、备用密钥及哈希函数为基础，可以抵抗重播攻击、伪造攻击、克隆攻击、拒绝服务（DoS, denial of service）攻击和位置跟踪攻击等。除此之外，该方案可以实现相互身份认证、标签匿名性、可用性和可伸缩性、假数据注入攻击等安全属性。

相互认证是保护隐私的有效方式，实现RFID标签和阅读器之间的相互认证时，既要使用匿名技术处理设备标签信息，又要使用轻量级加密算法实现轻量级的认证。在未来的研究中，人们可以使用轻量级加密算法（如椭圆曲线加密），既实现匿名化处理又实现轻量级加密。

3.3.2 智能电网

智能电网以其高效性和方便性在传统电网领域占据优势，但其仍然面临着各种安全挑战。

文献[28-29]分别提出了基于默克尔树和基于哈希消息认证码（HMAC, hash-based message authentication code）的轻量级密码认证方案。文献[30-31]通过使用轻量级的Diffie-Hellman密码体制，实现了智能电表与其他系统组件相互认证。为了解决一些性能和安全方面的挑战，许多学者一直在研究轻量级的低存储成本和密钥管理的密钥体制，文献[32-34]讨论了基于HMAC和同态加密技术用于智能电网的多播认证一次性签名，减少了交换的数据量，通过隐藏智能电表的身份而保证隐私性。

通过上述的研究发现，智能电网中利用轻量级加密算法是实现轻量级认证的关键，在兼顾隐私性的基础上，智能电网系统中的轻量级认证方案可以大致利用下面的密码体制类型：1) 使用轻量级加密算法，如椭圆曲线加密；2) 将哈希函数与随机数或时间戳相结合；3) 使用简单的位操作。

3.3.3 车联网

将汽车连接到互联网上，形成汽车网络或车联网。车辆认证是车联网系统中的一个具有挑战性的课题。

文献[35]提出了一种协作消息认证方案，既减少了消息认证的开销，又降低了认证的时延。文献[36]提出了一种认证方案，来自多个车辆的请求可以分批进行认证，而不是逐个进行。文献[37]基于修改的DSA（digital signature algorithm）和ECDSA（elliptic curve digital signature algorithm）签名提出了一种由不同签名者和单个签名者生成的多个签名的批量认证方法，该认证方法比单独认证快7倍。

保证车辆身份信息的机密性和匿名性是车联

网的一个关键课题，需要开发既能保护隐私安全又能相互认证的密码体制。

3.3.4 智能家居

在智能家居中，用户使用移动设备或个人电脑实现与智能家居设备之间的相互认证，从而实现远程控制、监控和访问。

Miettinen 等[38]提出了一种基于上下文的设备互认证协议，该协议使用设备的相同位置作为共享机密，不需要输入密码，并且与其他解决方案相比具有显著的可用性。Sun 等[39]开发了一种允许智能家居用户通过网络远程与终端设备进行通信的方案，方案除了建立安全连接外，还允许通信双方进行相互认证，以建立数据的保密性。Jan 等[40]提出一种基于约束应用协议（CoAP, constrained application protocol）轻量级特性的物联网相互认证协议，作为客户端与服务器端通信的应用层协议。协议中利用 AES 密码的优点，提供了安全的通信通道，使客户端和服务器利用大小为 256 位的有效负载加密消息，通过交换有效负载进行认证，从而对彼此身份进行双向认证。

表 2 总结了不同应用领域的物联网身份认证方案，根据本节提出的分类方法进行了分类，并总结了它们的认证协议。通过上述研究发现，协议中相互认证的实现并不需要新的加密算法和技术，但是设计一个适合资源受限的物联网设备的认证体制，仍然是一个新的挑战。

表 2　物联网不同应用领域认证方案的分析

领域	认证协议	密码技术	实现目标	需要防范的攻击类型	文献
RFID	轻量级的相互认证	物理不可克隆函数（PUF, physical unclonable function）和轻量级密码	实现单个标签的高效认证	窃取、重放、溯源、克隆、异步	文献[41]
	轻量级隐私保护身份认证	理想的 PUF 环境	实现匿名认证和前向安全	隐私窃听、异步、模仿、物理、克隆	文献[42]
	轻量级的 RFID 读写器缓存互认证	GNY 逻辑证明认证协议的正确性	实现降低计算和传输成本	拒绝服务、追踪、欺骗、重放、窃听	文献[27]
	匿名的超轻量 NFC 相互认证	移位和 XOR 操作	实现低计算和存储开销	匿名、追踪、重放、异步	文献[43]
智能电网	轻量级的相互认证	Merkle-hash tree	实现高效计算和低通信开销	消息注入和重放	文献[28]
	隐私保护的身份认证	HMAC	实现传输和签名认证时延低	篡改设备和伪造身份	文献[29]
	智能电网互认证和智能电网管理	基于身份加密的公钥管理协议和基于 PKI 的通信	实现相互认证和密钥管理	防止各种攻击	文献[44]
	轻量级的相互认证	Diffie-Hellman、RSA、AES 和 HMAC	消息完整性、总体通信和计算开销低	重播和中间人攻击	文献[31]
	隐私保护和网关辅助身份认证	HMAC 和同态加密技术	隐私保护、不可否认性和可追踪性	内部攻击和流量攻击	文献[33]
车联网	分布式聚合隐私保护身份认证	聚合签名技术	密钥托管自由，低消息认证时延和丢失率，高效消息处理	消息认证和条件可链接性、错误信息	文献[45]
	预测双重认证的广播身份认证	椭圆曲线数字签名算法签名和时间有效流损失容忍（TESLA, time efficient stream loss tolerant authentication）	保证消息的及时真实性和不可否认性	数据分组丢失和内存拒绝攻击	文献[46]
	身份认证和重新身份认证方案	增强的双重认证和密钥管理技术	实现机密性和最优身份认证时延	重放攻击、拒绝服务、位置追踪、伪装攻击、不可否认	文献[47]
	车辆驾驶员身份认证	椭圆曲线密码术和隐写术技术	实现车辆驾驶员身份认证和隐私保护	信息窃听	文献[48]
	多跳认证的代理移动 IP	对称多项式密钥生成技术	实现及时切换，在不影响正在进行会话的情况下减少可能的攻击	伪造和串谋、重放、中间人和拒绝服务	文献[49]
智能家居	基于设备物理特性的 IoT 网设备安全部署新方法	PUF 和物理密钥生成的组合	篡改证据的安全保证	防篡改和不可克隆性	文献[50]
	基于 PUF 的物联网终端设备相互认证协议	BAN 逻辑证明对象生命周期的正确性	解决物理−网络空间映射过程中的机密性	模拟攻击、重放攻击、窃听攻击	文献[51]
	基于 PUF 的物联网设备认证方案	利用存储在网关内的挑战响应对（CRP, challenge response pair）数据，实现终端设备与网关之间的相互认证	用网关进行身份认证，并生成会话密钥与终端设备通信	重放攻击	文献[52]
	轻量级的物联网环境中真实物理对象的相互认证	AES 和 CoAP	计算效率高、连接开销小	资源耗尽、拒绝服务、重放和物理篡改	文献[40]

4 物联网安全认证机制的新趋势

目前，互联网企业也对物联网安全身份认证方面进行了积极探索，如阿里云推出的 Link ID2 物理网身份认证安全解决方案，采用预共享密钥的对称密钥机制+证书方式的非对称密钥机制来实现设备级的双向认证。腾讯提出的基于硬件和密码学算法的下一代用户身份认证标准 TUSI（Tencent user security infrastructure），TUSI 采用 PKI 以及非对称密钥技术，向物联网行业推行新的身份认证标准。

文献[53]对现有的攻击、威胁及最新的解决方案进行总结，并以开发基于区块链的物联网应用进行了全面的综述，认为区块链是解决物联网安全问题的基础技术。区块链最大的特点是“不可篡改”和“去中心化”，从技术核心来看，区块链是一种基于密码学原理的分布式共识账本技术。就密码学而言，区块链使用了基于 SHA-256 和 RIPEMD-160 的哈希算法、基于椭圆曲线加密的密钥生成算法和非对称加密算法。未来将区块链技术应用到物联网中，可以有效提升物联网设备的身份认证能力。

沈昌祥院士提出可信计算已经发展到“可信计算 3.0”时代，物联网需要加快安全可信的可信计算 3.0 推广应用，筑牢基于 5G 的安全可信防线[54]。基于可信计算和等级保护的协同合作，把每个等级、每个环节基于可信任的安全认证作为根本的保障措施，利用等级保护的框架、感知域、计算域、边界与隔离，能更好地解决物联网安全问题。

鉴于物联网设备本身资源有限，导致传统计算机网络的安全机制无法与物联网环境完全集成。因此，对于微型嵌入式设备，应该开发有效的安全解决方案，而对于智能设备的设计和研究，应注重检测和从攻击中恢复的自主性。同时，为了应对物联网的安全挑战，如信任管理、识别、认证、隐私、访问控制和机密性等，需要新的软/硬件技术及识别机制，还应该考虑密钥管理的有效性。

5 结束语

本文根据物联网认证方案的相似点和主要特点，汇总分析了主要的物联网身份认证方案。物联网安全认证协议应具备以下 3 个特点：轻量级、隐私保护和相互认证[55]。在本文的工作中，通过物联网不同的应用方面，基于物联网不同的应用场景和物联网设备具备的不同安全能力来分析各种物联网认证协议的特征，针对不同的外部安全威胁提出安全需求，这种分类旨在实现一种安全的物联网环境。

通过对大量认证协议/方案的分析，本文认为，未来研究人员和开发人员在开发物联网网络和应用的新认证方案时，需要考虑以下问题。

1) 轻量级。设计认证方案时，在保证方案安全性的前提下，考虑到传感器（在内存、处理能力、电池等方面受到限制）是主要的终端设备，因此所提出的协议必须是轻量级的，以降低方案的计算成本、通信成本和存储成本，在成本和安全之间取得平衡。同时，由于所使用的无线通信协议的带宽有限，消息分组的大小也应该尽可能小。比如在智能家居和 RFID 中的应用。

2) 安全。由于存在各种已知和潜在的攻击（如女巫攻击、节点捕获、重播、密码猜测、消息伪造、蛮力、中间人、拒绝服务、选择明文等），因此需要结合攻击威胁水平，考虑和分析认证协议的稳健性。

3) 认证效率。在某些物联网应用中，实时超高速身份认证是此类资源受限设备面临的另一个挑战。特别是在车联网中，需要设计考虑低时延的超高速认证。

4) 软/硬件结合。与软件安全方法相比，物理上不可执行的函数是一个不可克隆的单向函数，它可以实现身份认证、访问控制和可跟踪性。因此可以考虑软件解决方案（更低的成本）和硬件解决方案（更安全）的组合，为物联网系统设计一种轻量级的保护隐私的身份认证方案。

5) 可扩展性。由于物联网是由不同通信范式和应用领域组成的大规模异构网络，因此不同的网络具有各自的需求和能力。因此，物联网认证方案应该是可扩展的，它可以管理大量的节点，并能够添加新的节点，而不需要进一步地设置或配置。另外，在物联网环境下的端到端身份认证机制中，设备身份的认证方案应该具有跨不同域的可伸缩性。

6) 认证机制。随着物联网设备的增加，物联网网络变得容易受到硬件缺陷的影响，因此在部署物联网设备之前，最好先在硬件上采用安全性机制，执行数据分组的处理等操作。否则，一旦大批量物联网设备部署到物联网环境中，就很难解决发现的漏洞。因此，需要一种有效的认证机制实现全面的物联网安全。

参考文献：

[1] GUBBI J, BUYYA R, MARUSIC S, et al. Internet of things (IoT): a vision, architectural elements, and future directions[J]. Future Generation Computer Systems, 2013, 29(7): 1645-1660.

[2] EL-HAJJ M, CHAMOUN M, FADLALLAH A, et al. Analysis of authentication techniques in Internet of things (IoT)[C]//In Proceedings of the 2017 1st Cyber Security in Networking Conference. Piscataway: IEEE Press, 2017: 1-3.

[3] EL-HAJJ M, CHAMOUN M, FADLALLAH A, et al. Taxonomy of authentication techniques in Internet of things (IoT)[C]//IEEE 15th Student Conference on Research and Development. Piscataway: IEEE Press, 2017: 67-71.

[4] 思科. 2020 年全球网络趋势[R]. (2019-10-24)[2020-03-20].
CISCO. 2019 networking report[R]. (2019-10-24)[2020-03-20].

[5] BUGHIN J, CHUI M, MANYIKA J. An executive's guide to the Internet of things[J]. McKinsey Quart, 2015(4): 92-101.

[6] McKinsey & Company. The Internet of things: mapping the value beyond the hype[R]. (2015-06-01)[2020-03-20].

[7] MARESCH D, GARTNER J. Make disruptive technological change happen—the case of additive manufacturing[J]. Technological Forecasting and Social Change, 2018, doi:10.1016/j.techfore.2018.02.009.

[8] HERNANDEZ G, ARIAS O, BUENTELLO D, et al. Smart nest thermostat: a smart spy in your home-black hat[R]. (2014-08) [2020-03-20].

[9] TRAPPE W, HOWARD R, MOORE R S. Low-energy security: limits and opportunities in the Internet of things[J]. IEEE Security Privacy, 2015(13): 14-21.

[10] AHMED M E, KIM H. DDoS attack mitigation in Internet of things using software defined networking[C]//IEEE Third International Conference on Big Data Computing Service and Applications (Big Data Service). Piscataway: IEEE Press, 2017: 271-276.

[11] McAfee. McAfee labs threats report[R]. (2017-06)[2020-03-20].

[12] PANARELLO A, TAPAS N, MERLINO G, et al. Blockchain and IoT integration: a systematic survey[J]. Sensors, 2018, 18(8): 25-75.

[13] WAZID M, DAS A K, ODELU V, et al. Secure remote user authenticated key establishment protocol for smart home environment[J]. IEEE Transactions on Dependable and Secure Computing, 2020, 17(2): 391-406.

[14] BERTINO E, ISLAM N. Botnets and Internet of things security[J]. Computer, 2017, 50(2): 76-79.

[15] YANG Y, PENG H, LI L, et al. General theory of security and a study case in Internet of things[J]. IEEE Internet Things Journal, 2017, 4(2): 592-600.

[16] GUPTA A, TRIPATHI M. Poster: a lightweight mutually authenticated key-agreement scheme for wireless body area networks in Internet of things environment[C]//Proceedings of the 24th Annual International Conference on Mobile Computing and Networking. Piscataway: IEEE Press, 2018: 804-806.

[17] GOPE P, AMIN R, HAFIZUL ISLAM S K, et al. Lightweight and privacy-preserving RFID authentication scheme for distributed IoT infrastructure with secure localization services for smart city environment[J]. Future Generation Computer Systems, 2018(83): 29-37.

[18] KUMARI S, M KARUPPIAH, DAS A K, et al. A secure authentication scheme based on elliptic curve cryptography for IoT and cloud servers[J]. Journal of Supercomputing, 2018(74): 6428-6453.

[19] NANDY T, IDRIS I B, NOOR R M, et al. Review on security of Internet of things authentication mechanism[J]. IEEE Access, 2019(7): 151054-151089.

[20] ATWADY Y, HAMMOUDEH M. A survey on authentication techniques for the Internet of things[C]//2019 International Conference on Computer and Information Sciences. Piscataway: IEEE Press, 2019: 1-5.

[21] HOSSAIN M M, FOTOUHI M, HASAN R. Towards an analysis of security issues, challenges, and open problems in the Internet of things[C]//IEEE World Congress on Services. Piscataway: IEEE Press, 2015: 21-28.

[22] EL-HAJJ M, FADLALLAH A, CHAMOUN M, et al. A survey of Internet of things (IoT) authentication schemes[J]. Sensors, 2019(19): 1-43.

[23] HONG S. Authentication techniques in the Internet of things environment: a survey[J]. International Journal of Network Security, 2019, 21(3): 462-470.

[24] HONG S. P2P networking based Internet of things (IoT) sensor node authentication by blockchain[J]. Peer-to-Peer Networking and Applications, 2020(13): 579-589.

[25] LETSOALO E, OJO S. Survey of media access control address spoofing attacks detection and prevention techniques in wireless networks[C]//IST-Africa Week Conference. [S.n.:s.l.], 2016: 1-10.

[26] LEE J Y, LIN W C, HUANG Y H. A lightweight authentication protocol for Internet of things[C]//2014 International Symposium on Next-Generation Electronics. Piscataway: IEEE Press, 2014: 1-2.

[27] FAN K, GONG Y, LIANG C, et al. Lightweight and ultralightweight RFID mutual authentication protocol with cache in the reader for IoT in 5G[J]. Security and Communication Networks, 2016(9): 3095-3104.

[28] LI H, LU R, ZHOU L, et al. An efficient merkle-tree-based authentication scheme for smart grid[J]. IEEE Systems Journal, 2014(8): 655-663.

[29] CHIM T, YIU S, HUI L C, et al. PASS: privacy-preserving authentication scheme for smart grid network[C]//2011 IEEE International Conference on Smart Grid Communications. Piscataway: IEEE Press, 2011: 196-201.

[30] FOUDA M M, FADLULLAH Z M, KATO N, et al. Towards a light-weight message authentication mechanism tailored for Smart Grid communications[C]//2011 IEEE Conference on Computer Communications Workshops. Piscataway: IEEE Press, 2011: 1018-1023.

[31] MAHMOOD K, CHAUDHRY S A, NAQVI H, et al. A lightweight message authentication scheme for Smart Grid communications in power sector[J]. Computers & Electrical Engineering, 2016(52): 114-124.

[32] JI C, KIM J, LEE J Y, et al. Review of one-time signatures for multicast authentication in smart grid[C]//2015 12th International Conference & Expo on Emerging Technologies for a Smarter World. Piscataway: IEEE Press, 2015: 1-4.

[33] CHIM T W, YIU S M, LI V O, et al. PRGA: privacy-preserving recording & gateway-assisted authentication of power usage information for smart grid[J]. IEEE Transactions on Dependable and Secure Computing, 2015(12): 85-97.

[34] LI Q, CAO G. Multicast authentication in the smart grid with one-time signature[J]. IEEE Transactions Smart Grid, 2011(2): 686-696.

[35] LIN X, LI X. Achieving efficient cooperative message authentication in vehicular Ad Hoc networks[J]. IEEE Transactions on Vehicular Technology, 2013, 62(7): 3339-3348.

[36] JIANG S, ZHU X, WANG L. A conditional privacy scheme based on anonymized batch authentication in vehicular Ad Hoc networks[C]//

IEEE Wireless Communications and Networking Conference. Piscataway: IEEE Press, 2013: 2375-2380.

[37] CHEON J, YI J. Fast batch verification of multiple signatures[C]//Public Key Cryptography-PKC. Berlin: Springer, 2007: 442-457.

[38] MIETTINEN M, NGUYEN T D, SADEGHI A, et al. Revisiting context-based authentication in IoT[C]//55th ACM/ESDA/IEEE Design Automation Conference. Piscataway: IEEE Press, 2018:1-6.

[39] SUN X, MEN S, ZHAO C, et al. A security authentication scheme in machine-to-machine home network service[J]. Security and Communication Networks, 2012(8): 2678-2686.

[40] JAN M A, KKAN F, ALAM M, et al. A payload-based mutual authentication scheme for Internet of things[J]. Future Generation Computer Systems, 2019(92): 1028-1039.

[41] XU H, DING J, LI P, et al. A lightweight RFID mutual authentication protocol based on physical unclonable function[J]. Sensors, 2018, 18(3): 760.

[42] GOPE P, LEE J, QUEK T Q S. Lightweight and practical anonymous authentication protocol for RFID systems using physically unclonable functions[J]. IEEE Transactions on Information Forensics and Security, 2018(13): 2831-2843.

[43] FAN K, SONG P, YANG Y. ULMAP: ultralightweight NFC mutual authentication protocol with pseudonyms in the tag for IoT in 5G[J]. Mobile Information Systems, 2017: 1-7.

[44] NICANFAR H, JOKAR P, BEZNOSOV K, et al. Efficient authentication and key management mechanisms for smart grid communications[J]. IEEE Systems Journal, 2014, 8(2): 629-640.

[45] ZHANG L, WU Q, DOMINGO-FERRER J, et al. Distributed aggregate privacy-preserving authentication in VANETs[J]. IEEE Transactions on Intelligent Transportation Systems, 2017(18): 516-526.

[46] LALLI M, GRAPHY G.S. Prediction based dual authentication model for VANET[C]//2017 International Conference on Computing Methodologies and Communication. Piscataway: IEEE Press, 2017: 693-699.

[47] REKIK M, MEDDEB-MAKHLOUF A, ZARAI F, et al. Improved dual authentication and key management techniques in vehicular Ad Hoc networks[C]//IEEE/ACS 14th International Conference on Computer Systems and Applications. Piscataway: IEEE Press, 2017: 1133-1140.

[48] KUMAR A, PRAKASH A, SHARMA S, et al. Vehicle authentication and message hiding protocol for vehicle to vehicle communication[C]//2015 1st International Conference on Next Generation Computing Technologies. Piscataway: IEEE Press, 2015: 383-387.

[49] CESPEDES S, TAHA S, SHEN X. A multihop-authenticated proxy mobile ip scheme for asymmetric VANETs[J]. IEEE Transactions on Vehicular Technology, 2013(62): 3271-3286.

[50] HUTH C, ZIBUSCHKA J, DUPLYS P, et al. Securing systems on the Internet of things via physical properties of devices and communications[C]//Proceedings of 2015 Annual IEEE Systems Conference. Piscataway: IEEE Press, 2015: 8-13.

[51] ZHAO M, YAO X, LIU H, et al. Physical unclonable function based authentication protocol for unit IoT and ubiquitous IoT[C]//2016 International Conference on Identification, Information and Knowledge in the Internet of Things. Piscataway: IEEE Press, 2016: 179-184.

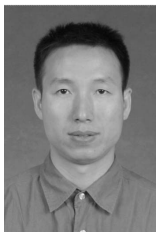
[52] MUHAL M A, LUO X, MAHMOO Z, et al. Physical unclonable function based authentication scheme for smart devices in Internet of things[C]//IEEE International Conference on Smart Internet of Things. Piscataway: IEEE Press, 2018: 160-165.

[53] KHAN M A, SALAH K. IoT security: review, blockchain solutions, and open challenges[J]. Future Generation Computer Systems, 2018(82): 395-411.

[54] 沈昌祥. 用可信计算 3.0 为网络安全筑牢免疫系统[R]. (2019-08-21)[2020-03-20].
SHEN C X. Using trusted computing 3.0 to build an immune system for network security[R]. (2019-08-21)[2020-03-20].

[55] YANF T, ZHANG G H, LIU L, et al. New features of authentication scheme for the IoT: a survey[C]//2nd Workshop on the Internet of Things Security and Privacy. New York: ACM Press, 2019: 44-49.

[作者简介]



闫宏强（1972− ），男，河北卢龙人，中国科学院博士生，主要研究方向为个人信息与隐私保护。

王琳杰（1981− ），男，山东平度人，贵州大学博士生，主要研究方向为网络与信息安全。

收录声明

本刊对发表的文章，拥有出版电子版、网络版版权，并拥有和其他网站交换信息的权利。本刊支付的稿酬中已经包含上述费用。

Journal on Communications has the copyright to publish electronic edition, online edition of the published articles, and has the right to exchange information with other sites. The expenses have been included in the fee paid by editorial department.

道德声明

本刊发表的论文是作者独立取得的原创性研究成果，无一稿多投；论文内容不涉及国家机密；未曾以任何形式用任何文种在国内外公开发表过；论文内容不侵犯他人著作权和其他权利。若发生一稿多投、侵权、泄密等问题，论文作者将承担全部责任。

The authors of *Journal on Communications* guarantee that their submitted articles are original and contain nothing confidential. The said article is only submitted to *Journal on Communications*. The said article has not been published before and has not been submitted elsewhere for print or electronic publication consideration. The said article is no way whatever a violation or an infringement of any existing copyright or license from the third party. Otherwise, the authors of the said article shall take the blame for the violation or infringement of the related copyright and the leakage of secrets.

通信学报

Journal on Communications

发行代号：国内2-676 / 国外M395

2020年7月25日出版　定价：98.00元

ISSN 1000-436X

CN 11-2102/TN