物联网若干应用场景安全问题综述

**ABSTRACT**

**摘要**

随着智能家居、数字医疗、车联网等技术的发展, 物联网应用越发普及, 其安全问题也受到越来越多研究者的关注。本文首先对物联网3层逻辑架构进行了介绍, 阐述了每个层次的安全问题与研究现状重点;然后重点分析并讨论了物联网的主要应用场景 (智能家居、智能医疗、车联网、智能电网、工业与公共基础设施) 中需要特别关注的隐私保、入侵检测等安全问题；再次，归纳了现有研究工作中的不足与安全问题产生的主要原因，指出物联网安全存在的五大技术挑战：数据共享的隐私保护方法、有限资源的设备安全保护方法、更加有效的入侵检测防御系统与设备测试方法、针对自动化操作的访问控制策略、移动设备的跨域认证方法；最后，通过详尽分析这五大技术挑战，指出了物联网安全未来的研究方向。

**Key words** Internet of things; security;privacy;challenge;survey

**关键词** 物联网；安全；隐私；挑战；综述

自2005年国际电信联盟正式提 出物联网（Internet of things，IOT）概念以来，传感器网络、云计算、微型芯片等技术不断发展成熟，物联网产业也迅速发展扩 大．根据Statista门户网站最新统计数据，2016年互联设备数量已经达到176亿，预计到2020年突破300亿．国际数据公司预测，到2020年物联网市场规模将会突破７万亿美元。

在物联网飞速发展的同时，其安全面临着严峻挑战。物联网安全问题不仅能给用户带来财产损失，甚至会威胁用户的生命安全。2016年前FBI美国信息安全专家发现，现阶段市场上的心脏起搏器和胰岛素泵等无线嵌入式医疗设备普遍存在可利用的安全漏洞。物联网安全也是国家安全和社会稳定的基石。2010年曝 光的震网病毒对多国核电站、水坝、国家电网等工业与公共基础设施造成了大规模的破坏。2016年mirar僵尸网络通过控制大量的物联网设备对美国域名解析服 务提供商DYN公司发动DDOS攻击，造成美国东部大面积断网，许多热门网站停止服务。

通过调研近年网络与信息安全领域的论文，我们发现物联网安全相关研究成果逐渐增多，但其中大多数研究成果的适用范围较窄，应用价值不高。目前很少有研究者提出具有前瞻性且广泛适用的物联网安全措施。由于物联网研究范围十分宽泛，其安全问题也繁多杂乱，现有物联网安全调研报告主要存在两大问题：

１）讨论问题不全面

现有物联网安全调研报告大多从应用场景、逻辑层次和安全属性等单一角度来分类讨论物联网安全问题。但是物联网涵盖的内容较为分散，所以仅从某一个角度讨论物联网安全问题，无法全面了解物联网各个方面安全研究现状。

２）缺乏对物联网安全问题的深入分析

现有的物联网安全调研报告大多仅指出物联网现阶段的安全问题，并没有深入分析产生这些安全问题的根本原因。同时，这些报告也未指出解决这些安全问题所需克服的技术难点，无法为研究者提供具有指导意义的研究方向。

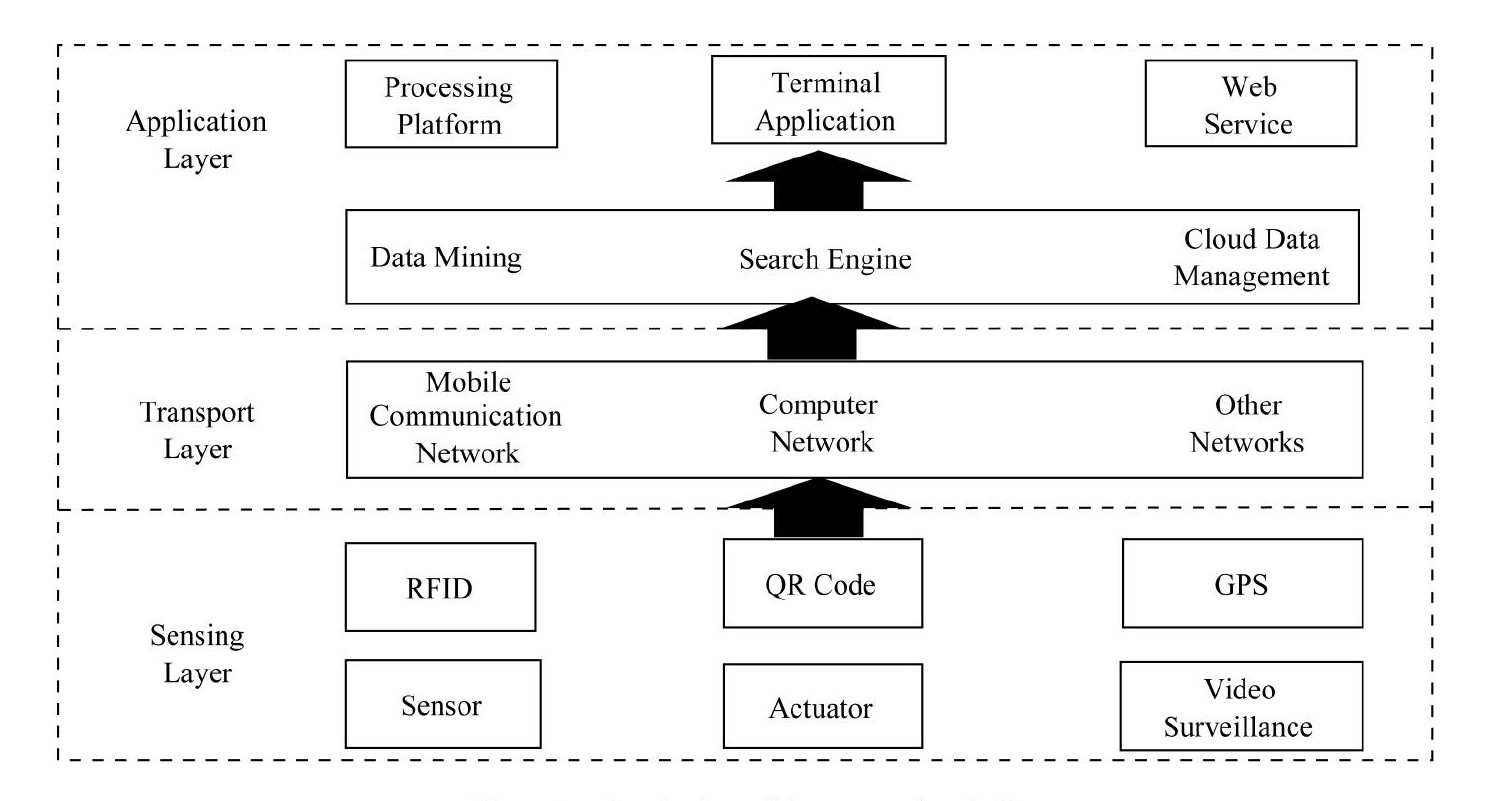
针对上述两大问题，本文对近年来已发表的大量物联网安全相关论文进行了调研，并做出以下分析：

１ 物联网架构安全研究现状

本节首先介绍物联网架构层次，然后分层次讨论其安全问题与研究现状。

１．１ 物联网逻辑架构简介

无论是最新提出面向服务的物联网架构，还是将应用层进一步划分的４或５层物联网架构，其本质均可分为３个逻辑层次．其从下至上依次为：感知层（Sensing Layer）、传输层（Transport Layer）和 应 用 层（Application Layer），如下图所示。



感知层是所有数据的来源，从智能标签RFID、GPS、环境传感器、工业传动器、摄像头等各种各样的智能设备中获取原始数据。物联网发展的最终目标是实现万物互联，所以感知层的目标是全面感知和收集所需的外界信息．这里特别注明学术界常把传感器网络归于感知层，但通过调研发现传感器网络的主要安全任务是传感器节点间信息安全传输，其与传输层的安全任务更为一致．所以本文把传感器网络的安全问题划分到传输层去讨论。

传输层通过各种有线和无线的网络通信技术（无线网络、有线宽带、移动网络等）把感知层收集的信息安全可靠地传输到应用层．主要包含两大安全任务：１）单一网络内部的信息安全传递问题；２）不同网络之间的信息安全传递的问题。

应用层的主要工作可以抽象概括为２个：

１）云端数据聚合与智能处理

首先应用层中的云服务平台将从传输层接收到的数据进行智能处理，即对海量分布式信息进行数据清理并提炼出含有较高信息量的数据。其主要技术包括搜索引擎、数据挖掘和云数据管理与共享等。

２）应用平台为用户提供服务

云端将处理后的数据传输给用户、企业和管理部门对应的服务程序（如远程医疗WEB服务、管理智能家居设备的APP、智能交通的信息监控与处理平台等），然后由这些应用平台利用这些数据为用户提供所需服务。需要注意：生活中提及的智能家居、智能交通、智能电网等物联网应用场景，并不直接对应物联网架构中的应用层的应用。这些应用场景是建立在完整的３层物联网架构之上的。这里应用层对应的只是这些应用场景中经过感知层收集数据和传输层传输数据后展示给用户的服务程序。

１．２ 感知层安全问题与研究现状

通过１．１节介绍可知，感知层主要负责数据收集，所以其安全措施也是围绕如何保证收集数据的完整性、机密性、可鉴别性来展开．为了实现这个目标，感知层的主要安全任务除了保障物联网感知层设备的物理安全和系统安全，还需为传输层安全通信提供基础保障．本节将分别围绕这３个主要安全任务进行讨论。

1. 感知层设备的物理安全会比之前的传统计算机受到更为严重的威胁。因为农业和工业环境中的传感器分布较广，若传感器运转正常可能长时间无人进行检查，很可能被敌手直接捕获；对于小型家用和医疗的智能设备，攻击者更加可以容易对其进行侧信道分析。同时，智能医疗设备、穿戴设备和智能家居设备等会比传统的个人计算机收集到更多敏感隐私数据．香港大学安全研究人员通过侧信道分析智能手表中移动加速度传感器收集的数据，实现对用户击键行为的成功预测。还有研究人员通过侧信道分析智能插座的用电量来推断与其连接电脑上的运行程序。

２）感知层设备受资源所限，只能执行少量的专用计算任务，没有足够的剩余资源用于实现细粒度的系统安全措施．此外许多工控专用设备其程序与系统依赖于特定的硬件架构，传统的访问控制、沙箱、病毒查杀等系统防御技术无法在这些特定设备上实现．这些因素都导致目前感知层设备的系统十分薄弱。Costin等人通过分析大量的嵌入式设备系统固件，发现了许多可利用的高危系统漏洞．有研究人员提出在嵌入式系统中建立轻量级可信执行环境来保护其系统安全，但 该方法计算开销较大，适用范围有限。还有研究人员设计了针对小型嵌入式设备系统的测试框架，但静态测试与漏洞检测方法无法实时动态保护嵌入式设备的系统安全。

３）感知层设备在利用传输层的协议进行通信时，必然需要为传输层安全通信提供基础保障．主要包括通信密钥生成、设备身份认证以及数据溯源等。同样由于感知层设备资源有限，经典的加密、认证以及其他密码算法直接部署在传感器等小型嵌入式设备上会严重降低设备处理效率，大幅增加设备功耗。大部分研究人员通过设计轻量级密码学算法或优化经典密码学算法实现方法来解决这一难题。还有研究人员提出了一些创新性的思路来解决这一难题。Majzoobi和Hiller研究团队分别提出基于设备自身独特的物理特性（Physical unclonable functions,PUF)的认证和密钥生成协议，该方法不仅节省了单独存储密钥的设备资源，而且可以有效抵御侧信道分析．也有研究人员利用穿戴设备获取的用户人体生物的特征如步态、滑动屏幕力度等来实现设备认证，该方法在节省资源的同时还可实现了设备和使用者的双重认证。综上，感知层３个方面的安全要求是相互依赖的，任何一个方面出现漏洞都会引发安全问题。例如有研究人员通过侧信道分析基于心率生成密钥的电信号信息熵，从而还原了用户心率信息获取了通信密钥。所以需要全面考虑感知层设备各个方面的安全要求以及相互之间的影响，才能设计出有效的安全防御策略。

１．３ 传输层安全问题与研究现状

传输层主要负责安全高效地传递感知层收集到的信息。因此传输层主要是各种网络设施，即包括小型传感器网络也包括因特网、移动通信网络和一些专业网络（如国家电力网、广播网）等。

传感器网络是物联网的基础网络，传感器设备收集的数据首先都要通过传感器网络才能向上传递给其他网络。同时，传感器网络与传统计算机网络有着许多不同，因此传感器网络的安全问题也成为近些年物联网安全研究的热点之一。首先由于传感器网络节点资源有限，特别是电池供电的传感器设备，很容易对其直接进行拒接服务（DOS攻击，造成节点电量耗尽。另外传感器节点分布广泛数目 众多，管理人员无法确保每个节点的物理安全．敌手可直接捕获传感器节点进行更加深入的物理分析，从而获取节点通信密钥等．特别一旦传感网关节点被敌手控制，会使整个传感器网络安全性全部丢失。现有许多研究人员通过对密码学算法与协议进行的轻量化处理来抵御传感器网络攻击．但这些轻量级算法与协议大多缺乏对设备电量和网络带宽消耗的测试，适用性有待提高。

虽然现阶段对传输层通信网络的攻击仍然以传统网络攻击（如重放、中间人、假冒攻击）等为主。但仅仅抵御这些传统网络攻击是不够的，随着物联网的发展，传输层中的网络通信协议会不断增多。当数据从一个网络传递到另外一个网络时会涉及到身份认证、密钥协商、数据机密性与完整性保护等诸多问题．因此面临的安全威胁将更加突出需要研究人员更多地关注。

１．４ 应用层安全问题与研究现状

通过１．１节的介绍可知，应用层需要对收集的数据完成最终的处理和应用．而数据处理与应用的过程都需要对应的安全措施保护。对于云端数据智能处理平台进行数据统计分析来满足应用程序使用的同时需要防止用户隐私信息

泄露．现阶段学术界主要采用同态加密来解决这一矛盾。同态加密的数据进行处理得到一个输出，将这一输出进行解密，其结果可以保证与用同一方法处理未加密的原始数据得到的输出结果是一样的。但全同态加密算法效率还有待提高，而部分同态加密算法可对加密数据进行的处理十分有限。保护用户隐私的 同 时，提高了服务器处理效率．有研究人员提出可以根据应用程序对数据的用途不同以及数据的敏感程度不同，对原始数据采用不同的处理方法。如为了防止心率等医疗数据被篡改可采用HASH算法；为了统计用户的用电量而不泄露其具体信息可采用同态加密算法；对于无需计算的隐私数据可采用数据混淆的方法。同时由于云服务器会保存大量的用户数据，云服务数据的存储、审计与恢复以及共享都需要更多的安全措施来保护。Ｔｈｏｍａｓ和 Ｎｅｄ利用区块链技术在实现

物联网设备匿名共享的方法值得学习与借鉴．此外物联网设 备 数 目 的 增 多 使得DDOS攻击的规模将会大幅提升，云端服务器还需要提高抵御DDOS攻击的能力。对于应用服务程序，其与用户联系最为紧密，所以其最重要的安全任务是在提供服务的同时保护用户隐私信息。Ｆｅｒｎａｎｄｅｓ等人通过分析程序源

码发现５０％以 上 的 三 星 智 能 家 居 平 台 上 的 应 用 都具有不必要的权能，可导致用户敏感数据泄露或智能家居设备被恶意控制。现有研究人员为保护程序中的敏感操作和隐私数据［５１－５２］设计了多种访问控制模型，但其适用性和安全性均有待进一步提高。

~~１．５ 小 结~~

~~以上虽然是分层次讨论了物联网架构中的安全问题，但各个层次的安全问题并不是相互独立而是相互依赖。最主要体现在数据隐私保护方面，任何一个环节出现问题都会使用户的隐私数据泄露。目前，研究人员提出了许多针对物联网设备的测试框架、安全评估模型以及入侵检测防御系统等．但这些框架与工具可检测出的安全问题并不全面，适用范围有限。本文统计了２０１２—２０１７年上半年中国计算机学会网络安全领域 ＣＣＦＡ 类和 ＣＣＦＢ类会议与期刊１６４篇论文的讨论主题（剔除了调研类的文章），列出各个层次中讨论次数较多的研究热点，如表１所示．~~

２ 物联网常见应用场景安全问题与研究现状

现阶段物联网应用场景逐渐增多，不同应用场景需求目标不同，应用技术也不尽相同，故各应用场景对应的安全任务侧重点并不相同。如果仅按层次整体讨论物联网安全现状，则无法全面深入地了解各个物联网应用场景的安全问题．所以本节将分别从智能家居、智能医疗、智能交通、智能电网以及工业与公共基础设施五大物联网应用场景深入讨论其安全问题与研究重点。

２．１ 智能家居

智能家居越发普及的同时，各种智能家居设备保存与传输的用户隐私信息也越来越多．这些隐私信息不仅包含传统意义上那些银行卡、手机号等身份信息，还包含用户日常生活的行为隐私信息．如温度传感器记录了家中内各个房间的 实时温度信息；网络摄像头可以直接远程实时查看家中的状况。攻击者通过控制这些智能家居设备，从而实现对用户隐私行为的监控．Ｊｏｈａｎｎｅｓ和 Ｍａｒｔｉｎ就分析市场上主要型号的网络摄像头，发现了大量可轻易利用的安全问题包括弱口令、ＨＴＴＰ 明 文 传 输等。此外用户隐私保护意识普遍较低，厂商对于设备收集哪些用户隐私数据也无明确声明，加剧了智能家居设备隐私信息泄露的问题。

综上所述，智能家居设备首要安全工作是保护用户的隐私数据．研究人员大多通过监控智能家居终端应用的控制流与数据流来防止隐私数据泄露，但该方法忽视了智能家居设备间的互用问题。例如市场上有些智能窗户控制器会根据温度传感器收集的室温自动打开或关闭窗户。在上述情景下敌手仅需控制温度传感器的温度值，从而间接实现对智能窗户的控制。

２．２ 智能医疗

在智能医疗领域，数据和设备安全显得尤为重要。因为医疗设备尤其是胰 岛素泵、心脏起搏器等人体嵌入式设备一旦被恶意控制会严重威胁用户的生命安全．Ｍａｒｔｉｎ调研了大量的智能医疗设备发现其存在弱密钥、过期证书等诸多的安全漏洞。为了给用户提供更加全面、及时、专业的医疗服务，智能医疗设备的隐私信息会共享给诸多医疗单位，但同时也加剧了用户医疗隐私信息泄露的风险。此外，针对远程医疗服务平台的网络攻击也逐渐增多，甚至勒索软件也开 始将智能医疗设备［６１］与医院数据库［６２］作为主要攻击目标。研究人员为提高智能医疗设备的安全性，提出了针对智能医疗设备的专用测试框架［５９］以及恶意程序的软［６３］、硬［６１］件检测方法．为了防止医疗隐私数据泄露，Ｄｕｆｆｙ等人提出针对医疗数据使用人员不同，对隐私数据采取不同的保护处理方法．例如对统计人员提供同态加密的数据，对医生提供只可读

不可写的数据等［６４］。董晓蕾设计了动态可撤销权能的多级隐私保护模型［６５］，可以实施更加灵活的医疗隐私数据保护策略．同时，对智能医疗设备行为进行可信记录，也有利于及时发现对其的网络攻击行为．Ｈｅｎｒｙ等人通过在胰岛素泵上增加可检测人体进食后肠道生物特征的电路模块，从而判定胰岛素泵的异常行为是否由网络攻击造成［５７］．在未来智能医疗设备生产中可以参考这样的设计方法，增加对设备行为的可信记录模块．随着人均寿命普遍延长慢性病人数逐渐增多，智能医疗设备会越发普及．提高智能医疗设备的安

全性显得尤为重要．一旦无法保障医疗设备的安全，医生与病人自然会对智能医疗服务望而却步，严重阻碍智能医疗的推广与发展。

２．３ 智能汽车

随着市场上联网的智能汽车逐渐增多，现实中对智 能 汽 车 的 电 子 攻 击 也 层 出 不 穷［６６］．ＰＴ＆Ｃ｜ＬＷＧ 司法咨询 服 务 公 司 指 出 ２０１３ 年 在 伦 敦 被 盗的汽车中４７％的汽车是通过电子攻击来窃取的［６７］．而受到攻击次数越多的汽车，其联网的部件也越多．文献［６８－６９］的研究也 指 出 现 阶 段 智 能 汽 车 普 通 存在大量安全漏洞．目前由于汽车系统固件为厂商所有，一般并不开源．所以学术界重点 关注控制器局域网总线技术［７０］以及 Ｖ２Ｘ［７１］等智能汽车与其他设备通信技术的安全问题．此 外，智能汽车云服务的隐私泄露问题［７２］也引起了许多研究人员的关注．随着车联网技术的发展，预 估 到２０２０年６０％～７５％的 汽 车 都 将 具 有 Ｗｅｂ服 务［６６］，无 线 联 网 的汽车数量将达到１．５亿．智能汽车的安全将面临更加严峻的挑战．为了全面提高智能汽车的安全性，需要厂商和研究人员更加深入的合作才能设计出更加全面实用的安全防御措施．

２．４ 智能电网

智能电网是最早应用于公共基础设施上的物联网技术，其安全研究也开始较早，研究成果较多．故本节先讨论智能电网安全研究现状，在第２．５节再讨论其他工业与公共基础设施的安全问题．早期智能电网的安全研究重点关注智能电网的实时电价调 整 协 议［７３］以 及 其 他 通 信 协 议 的 安 全 问题［７４］．随着智能 电 网 技 术 不 断 发 展，更 短 时 间 间 隔的使用电量信息被统计收集，这些信息与用户用电行为的相关程度逐渐升高．此外，Ｄｉｍｉｔｒｉｏｕ和 Ｋａｒａｍｅ发现不仅用电信息会泄露用户用电行为，智能电网计划分配给用户的电量信息也会泄露用户的用电习惯［７５］，故对用户用电信息的隐私保护的研究逐渐增多．研究者大多利用之前提及的同态加密等密码学的算法［７６－７８］在不影响用电信息统计的前提下，实现用户用电信息的隐私保护．在未来不只是智能电表、智能水表和智能燃气表等其他智能抄表设备收集的用量信息会泄露更多的用户生活隐私．研究人员需要提前防范智能抄表带来的用户隐私泄露问题．

２．５ 工业与公共基础设施

这里讨论的智能工业与公共基础设备主要包括

闭路电视、数字视频记录仪等视频监控系统以及监测控制与数据采集［７９］等工业控制系统［８０］。震网病毒［４］的出现使工业与公共基础设备的信

息安全面临更加严峻的挑战．由于工业设备在设计之初没有考虑受到网络攻击的可能，所以当工业设备联 网 后 会 受 到 更 加 严 重 的 网 络攻击威胁［８１］。Ｌｕｉｉｊｆ［８２］还指出工业设备的设计与操作人员普遍存在侥幸心理，认为攻击者不具备相关专业知识无法实施网络攻击．此外，这些设备专用于完成特定的工业任务，其软硬件架构与传统计算机均不相同．普通计算机系统 防 御 措 施 如 防 火 墙、杀 毒 软 件 等［８３］，无法直接应用于上述设备，而单独为每种设备设计相应的系统防御措施开销过高．现阶段的安全研究人员主要通过设计入侵检测与防御系统来提高工业与公共基础设备的安全性．

有研究人员指出［８４－８５］由于工业设备的异构性，常用的基于通信网络中异常行为进行模式匹配的入侵检测方法，漏报率过高并不适用于工业系统．为了更加有针对性地保护关键工业设备，应该首先统计分析对关键设备的控制命令参数，从而确定其正常的值域范围；然后将其用来与实时通信流量中的控制命令参数进行比较，任何实际观察值在正常值范围之外时，就认为有入侵发生．Ｃｏｌｂｅｒｔ等人［８６］进一步指出为了提高入侵检测的准确率，对于关键参数的值域范围还需参考专业的操作人员和设计专家的意见进行人工辅助确定．Ｈｅｎｒｙ研究团队［８７］总结了现有的许多工业设备入侵检测模型，对未来设计更加有效的入侵检测模型有很高的参考价值．随着工业和公共基础设施中联网设备数目的增多，其所受到 的 网 络 攻 击 也 将 逐 渐 增 多［８８］．但 现 阶

段的工业与公共基础设备普遍缺乏网络与系统安全保护措施［８９－９１］．如何有效检测与防御对这些专用设施的网络攻击需要更加深入的研究．

２．６ 小 结

随着物联网技术的发展，物联网应用范围会愈发广 泛．此 外，诸如电动车与智能电 网交互供电（ｖｅｈｉｃｌｅ－ｔｏ－ｇｒｉｄ，Ｖ２Ｇ）等跨场景物联网应用技术，在节约能源与方便用户生活的同时，也带来了更多的安全与隐私泄露问题［９２－９３］．有效解决物联网应用场景中的安全问题将对未来物联网应用设计与发展起着重要作用．本文从１．５节调研的物联网安全相关论文中选

取与特定场景相关 的论文，然后统计智能家居（ｓｍａｒｔｈｏｍｅ）、智 能 医 疗（ｄｉｇｉｔａｌｈｅａｌｔｈｃａｒｅ）、智 能

汽车（ｉｎｔｅｌｌｉｇｅｎｔｖｅｈｉｃｌｅｓ）、智能电 网 与 其 他 工 业 与公 共 基 础 设 施 （ｓｍａｒｔｇｒｉｄａｎｄｉｎｄｕｓｔｒｉａｌｐｕｂｌｉｃｉｎｆｒａｓｔｒｕｃｔｕｒｅ）各场景 中 的 研 究 热 点，如 表２所 示．因为智能电网也属于工业与公共基础设施，且单独讨论工业和公共基础设备安全的论文较少，所以表２中将这２个场景的研究热点划为一类进行统计．

４ 未来研究方向

针对第３节介绍的五大物联网安全技术挑战并

结合物联网安全现状，总结出未来物联网发展中的

五大安全研究热点：

１）隐私数据保护

随着共享单车、共享汽车等物联网共享服务的

增多，如何防止这些共享服务中用户隐私信息的泄

露将成为物联网安全研究的一大热点．数据统计与

分析技术的发展依赖于大量的用户数据，而这也带

来了更大的隐私泄露风险．研究人员需要提出更加

实用 的 基 于 隐 私 保 护 的 数 据 挖 掘［１０９］与 机 器 学

习［１１０］方法．

２）轻量级安全机制

小型嵌入式系统设备在未来会更加普及，需要

研究者提出更加有效的轻量级系统与通信安全机

制．研究人员在设计轻量级安全机制时，主要需要满

足以下要求：首先对设备的电量和资源消耗要降到更

低，其次不能大幅增加原有设备的成本和设计难度．

３）入侵检测与防御系统

物联网设备和通信协议种类不断增多，需要研

究人员提出适用范围更广的入 侵 检 测 与 防 御 系

统［１０３］和设备安全测试工具［９５］

．近年来，对工业与公

共基础设备的网络 ＡＰＴ（高 级 持 续 性 威 胁）攻 击 逐

渐增多，如果这些关键的基础设施长期停止工作或

被恶意控制，国家和社会将受到严重危害．研究人员

需要对这些工业和公共基础设施设计出更加有效的

入侵检测与防御系统．

４）针对自动化操作的访问控制策略

随着机器学习技术的不断发展以及物联网设备

计算能力的不断提升，设备的自动化操作会逐步取

代人为操作．研究者需为物联网设备的自动化操作

设计出更加有效的访问控制策略来防止攻击者的恶

意利用．

５）移动设备的跨域认证方法

当前学术界对物联网移动设备安全问题的研究

还不够全面，没有意识到移动设备安全问题带来的

严重危害．敌手可利用移动设备不安全的跨域认证，

进而对其进行控制并传播恶意代码．研究人员需要

总　　结

关于物联网安全的研究虽然逐渐增多，但其整

体进度还处于起步阶段．物联网的系统、应用、网络

各个方面缺少具有代表性的安全研究成果．本文在

调研大量物联网安全论文后，首先从物联网架构层

次和应用场景２个角度阐述了物联网安全问题和研

究现状．物联网架构３个逻辑层次的主要安全工作

分别为：感知层需要在有限资源的设备上实现更加

有效的安全措施来保证收集数据的完整性、机密性、

可鉴别性；传输层需要着重解决数据跨网络传输时

产生的安全问题；应用层在为用户提供更多服务的

同时需要充分保护用户的隐私信息．不同的物联网

应用场景需要侧重解决的安全问题也有所不同：智

能家居和智能医疗设备需要更多的隐私保护机制，

从而尽可能降低用户隐私泄露的风险；智能电网等

工业基础设施需要更加有效的入侵检测和防御系

统，从而抵御大规模的拒绝服务攻击和长期潜伏的

ＡＰＴ 攻击．

然后，通过深入分析物联网安全问题产生的根

本原因与现有工作的不足，总结出物联网安全面临

的五大技术挑战．最后指出物联网安全未来的研究

热点，为相关研究人员提供更有针对性的设计参考．

只有尽快发现并解决物联网安全研究中的诸多难

点，才能有效地抵御愈发严重的物联网攻击，使人们

安全地享受物联网时代带来的便捷．