智能家居安全综述（泛读）

计算机研究与发展 2018

目录

[摘要： 1](#_Toc36481082)

[调研来源： 1](#_Toc36481083)

[研究现状： 1](#_Toc36481084)

[贡献： 2](#_Toc36481085)

[背景： 2](#_Toc36481086)

[主要工作： 3](#_Toc36481087)

[可做的工作： 5](#_Toc36481088)

## 摘要：

随着物联网技术的发展，智能家居产业日益繁荣，其安全问题受到越来越多研究者的关注，目前 相关研究尚在起步阶段. 首先回顾了智能家居的发展历程及现状，总结并介绍了当前智能家居系统架构．在安全方面，归纳、分析和总结了近几年的国内外文献，将安全问题划分为３个方面：平台安全、设备 安全和通信安全，并分析了这３方面智能家居安全研究现状。

目前平台安全研究主要集中于设计安全的认证和访问控制方案，以及发现设备联动和智能音箱等新场景的安全问题；设备安全研究主要包括设备固件漏洞挖掘和设备侧信道分析；通信安全研究主要包括协议漏洞挖掘和网络流量分析

## 调研来源：

四大顶会发现智能家居安全相关研究成果逐年增多

## 研究现状：

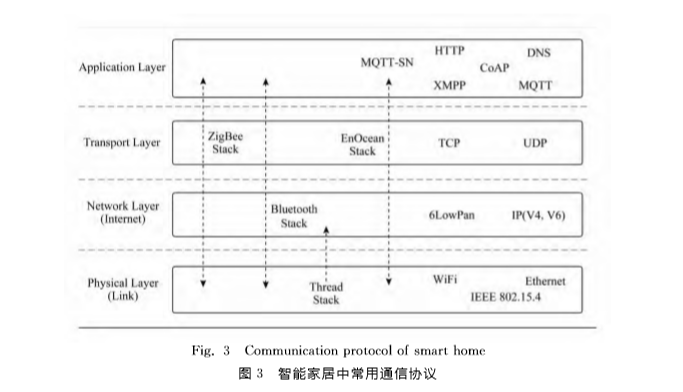
大多数研究侧重于挖掘智能家居系统安全漏洞，分析安全威胁，但研究仅关注于系统的单一 层次或环节．同时智能家居安全防护的研究文献较少，且大多数研究成果适用范围较窄，应用价值不高

## 贡献：

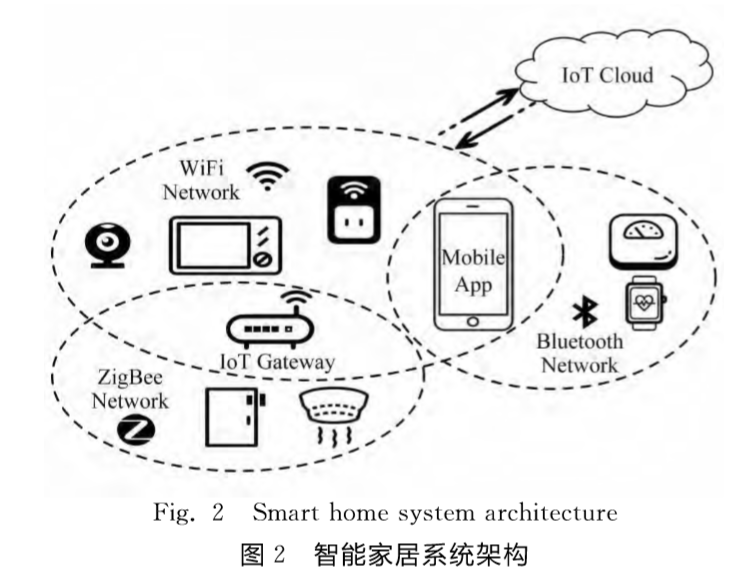
* 分析了智能家居的发展历程与现状，总结并介绍了当前智能家居系统架构．
* 深入调研了近几年国内外智能家居安全研究文献，从平台安全、设备安全和通信安全这３个方面介绍并总结了智能家居安全研究现状．
* 通过分析智能家居的安全问题以及现有研究工作的不足，指出了智能家居安全研究中面临的挑战与机遇，并为相关研究者指出了未来的热点研 究方向．

## 背景：

* 体系结构：
  + 终端设备
    - 受限设备
    - 能力设备
  + 移动 APP、
  + 物联网云端
    - 云端数据聚合与分析．平台将从设备端收集 到的数据进行存储及智能分析处理．
    - 管理、控制和协调不同的设备、系统和服务． 平台提供认证管理功能
  + 通信网络
    - 物理与链路层
    - 网络层
    - 传输层
    - 应用层
      * MQTT/CoAP/AMQP/XMPP
      * 不同的协议层次组成协议栈



* + 各种各样的终端设备与物联网云端联通，一部分终端设备可直接接入有线或无线网络从而与云端联通，另一部分设备由于缺乏直接接入互联网的通信接口，从而以网关或智能手机为跳板与云端联 通．联通后，设备会将自身感知或收集到的数据发送至云端，云端对数据进行存储、管理与分析处



## 主要工作：

* 智能家居用户身份认证 设计更为有效的认证协议 由于缺乏有效的输入输出设备
* 智能家居设备的访问控制
  + 使用第三方开发者的应用
  + 基于设备功能的访问控制机制
  + 基于上下文的权限控制系统
  + 基于风险的访问控制系统
* 智能家居设备联动安全
  + 根据一定的自定义触发规则，使得设备之间可以联动控制
* 智能音箱安全
  + 为构造恶意的语音样本攻击语音识别系统
* 设备安全
  + 设备安全漏洞挖掘与分析．研究集中于设备固件安全
  + 模糊测试 通过向目标系统提供非[预期](https://baike.baidu.com/item/预期/5738100)的输入并监视异常结果来发现[软件漏洞](https://baike.baidu.com/item/软件漏洞/3879396)的方法
* 智能家居设备的侧信道攻击
  + 侧信道攻击 针对电子设备在运行过程中的时 间消耗、功率消耗或电磁辐射之类的信息进行攻击 的方法
    - 设备攻击 通过破解智能设备在 使用过程中产生的如声音、光线、温度等物理现象来 获取用户的隐私信息
    - 网络通信攻击．当设备与设备或设备与云端 进行网络通信时，带宽、流量的消耗可能会发生变 化，攻击者通过分析这些信息的变化来获取相关的 隐私数据
* 通信安全
  + 协议漏洞挖掘
    - 通信协议安全
      * 物理层安全漏洞 ．物理层的协议主要解决的 是物体互联以及接入网络的问题．其常用的协议有  
        zigbee/bluetooth
      * 应用层协议安全漏洞
      * 智能家居网络流量分析

## 可做的工作：

* 用户身份认证的缺失 -- 多用户与单设备的交互
* 访问控制机制缺失 -- 权限粒度过粗
* 设备联动规则错误
* 仍然存在的设备固件漏洞 内存漏洞和逻辑漏洞
* 仅能够挖掘特定类型的内存漏洞或逻辑漏洞，漏洞挖掘的种类少，效率低
* 智能语音识别漏洞
* 漏洞源于自身算法设计时的固有问题
* 通信协议的漏洞