物联网安全
Internet of Things Security

第八章 物联网管道安全

冀晓宇
浙江大学

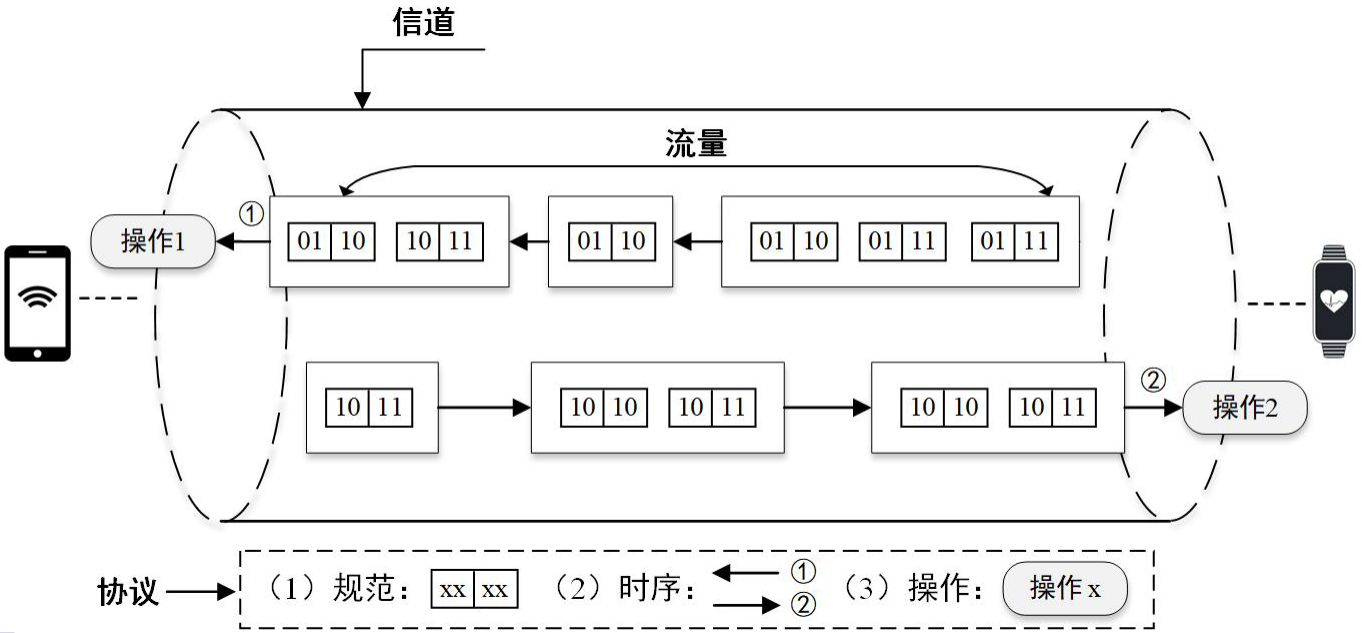
提纲

- 物联网管道定义
- 物联网管道安全威胁
- 物联网管道安全防护

内部使用，USSLAB版权

物联网管道

- **物联网怎么通信?**
  - 信道 — 传输的媒介（有线/无线信道）
  - 协议 — 数据交换的规范、时序和操作
  - 流量 — 特定时间内传输的数据统计分布特征



物联网管道示意图

CSLAB版权

8.1.1 通讯协议定义

- **定义**：任何物理介质中允许两个或多个实体之间传播信息的系统标准。协议定义了通信实体之间交换消息的**格式**和**顺序**，以及对消息的发送和接收时采取的**操作**

- **三要素**：语法、语义、规则

语法	语义	规则
数据的格式、编码和信号等级等	通信内容，包括数据信息、控制信息	通信的顺序、速率匹配和排序
“如何讲”	“讲什么”	“怎么做”

内部使用，USSLAB版权

8.1.1 通讯协议功能

分段

将数据分为**较小**的
长度受限的数据块
如：MTU

重组

数据接收侧重新把
数据组成消息
如：乱序重排

封装

在分段形成的数据块上
增加控制信息的过程
如：TCP/IP包头

连接控制

控制实体之间的
连接方式
如：TCP/UDP

附加功能：例如优先权、服务等级及安全设置

8.1.1 通讯协议功能

流量控制

接收实体对发送实体送出的数据单元的**数量或速率**进行控制

差错控制

对协议数据单元中的数据和控制信息进行**保护**

寻址

根据消息中给出的地址信息寻找**有效地址**

复用

在一个系统上支持**多个连接**

“例如，TCP协议具有分段、流量控制、差错控制，多路复用等功能，IP协议具有分段、重组、寻址等功能。”

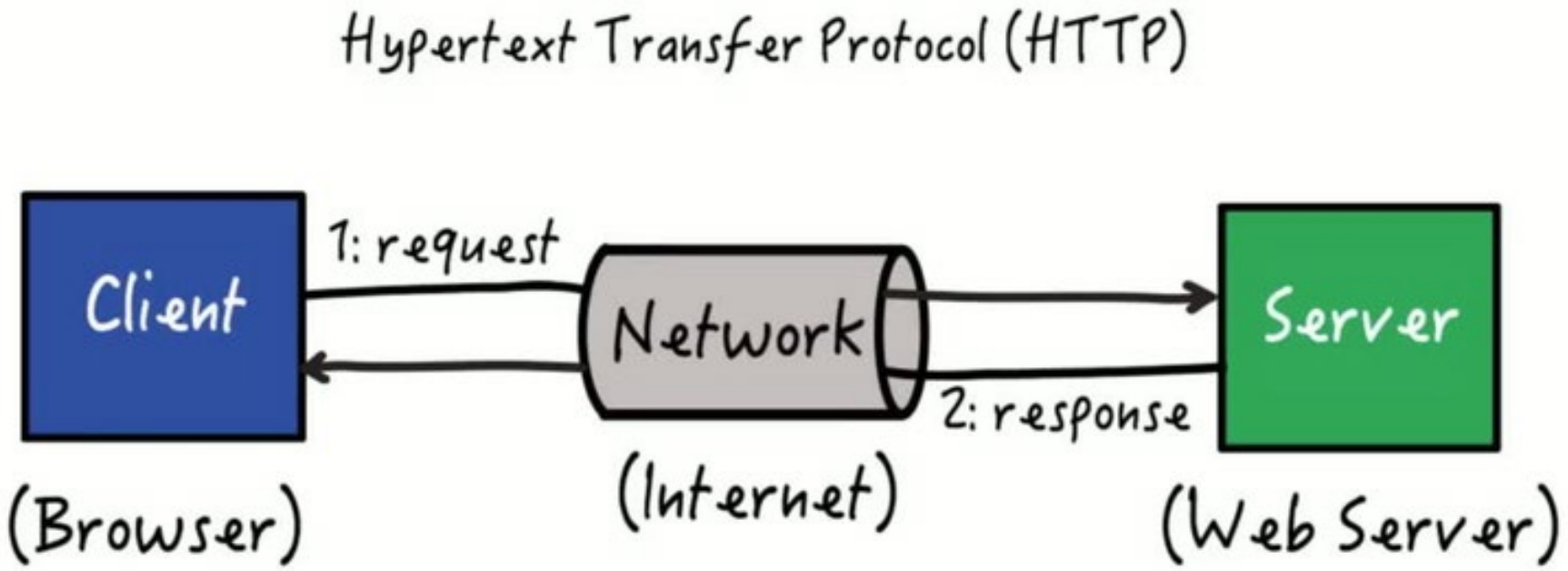
互联网时代，TCP/IP协议已经一统江湖，现在的物联网的通信架构大多也是构建在传统互联网基础架构之上。

物联网相关协议到底有什么特殊性？

内部使用，USSLAB版权

回顾：HTTP协议

版权



https://www.linkedin.com/pulse/how-does-http-protocol-work-pandurang-patil/

8.1.2 通讯协议新需求

- **海量连接**
  - 终端设备数量与种类激增
  - 无线接入需求增多
- **轻量化**
  - 设备资源受限
  - 设备功耗极低
- **高带宽、低延时与高可靠**
  - 高带宽场景：超高清视频、增强现实等
  - 低延时与高可靠场景：工业控制、智能驾驶控制等
  - 安全接入、认证能力

面向物理链路层的
无线通信协议

面向应用层的
轻量化消息传输协议

内部使用，USSLAB版权

8.1.3 物联网相关通信协议

- 物联网的特殊性，要求其**物理链路层**和**应用层**设计新的协议

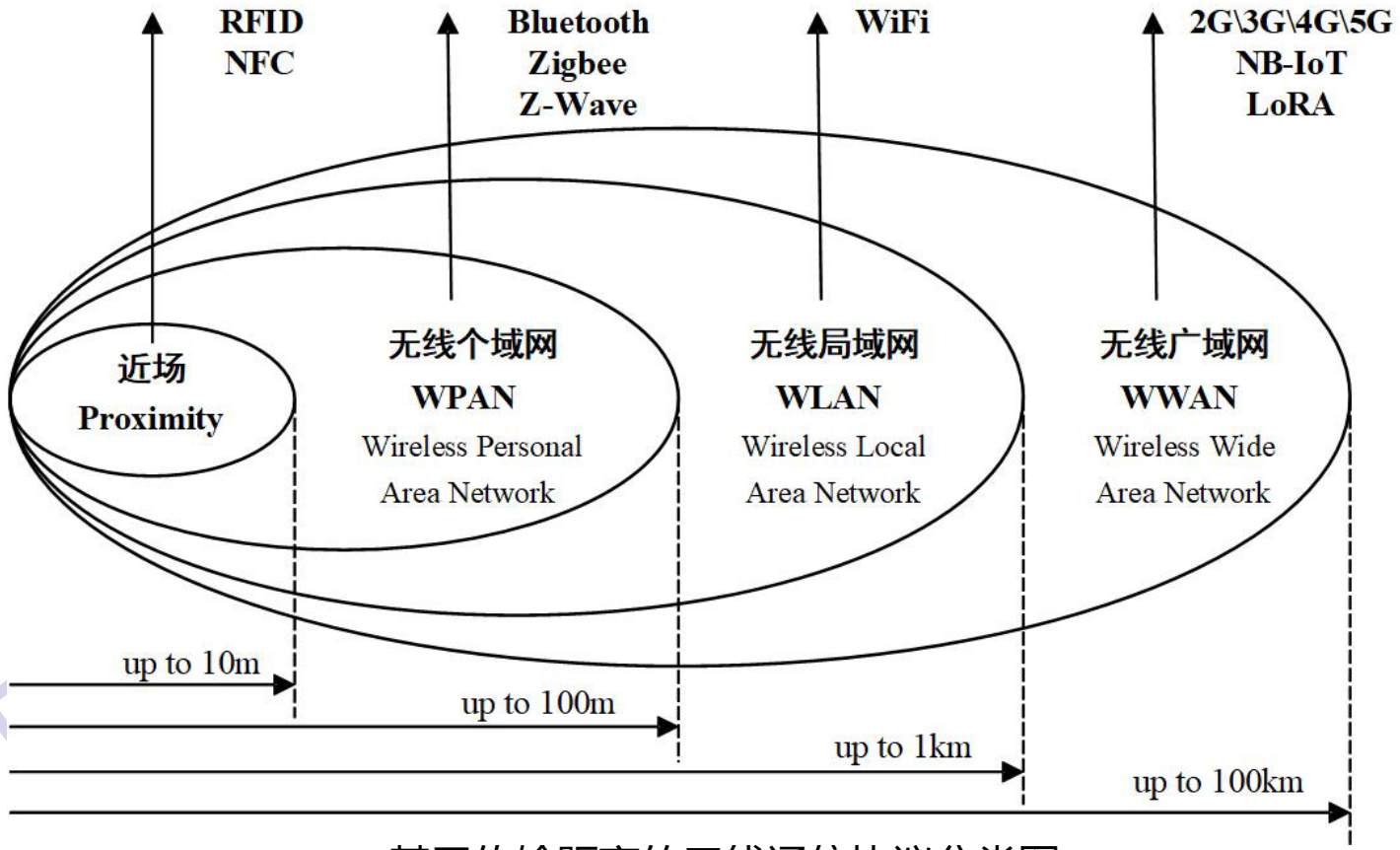
- **面向物理链路层的无线通信协议**
  - 物联网无线近场通信协议：RFID、NFC
  - 物联网无线个域网通信协议：Bluetooth(**BLE**/BT)、Zigbee、Z-Wave
  - 物联网无线局域网协议：Wi-Fi
  - 物联网无线广域网协议：2G/3G/4G/5G、NB-IoT、LoRa

- **面向应用层的轻量化消息传输协议**
  - MQTT
  - CoAP
  - XMPP

内部使用，USSLAB版权

面向物理链路层的无线通信协议

- **物理链路层**：包含物理层和数据链路层
- 基于传输距离对无线通信协议进行分类

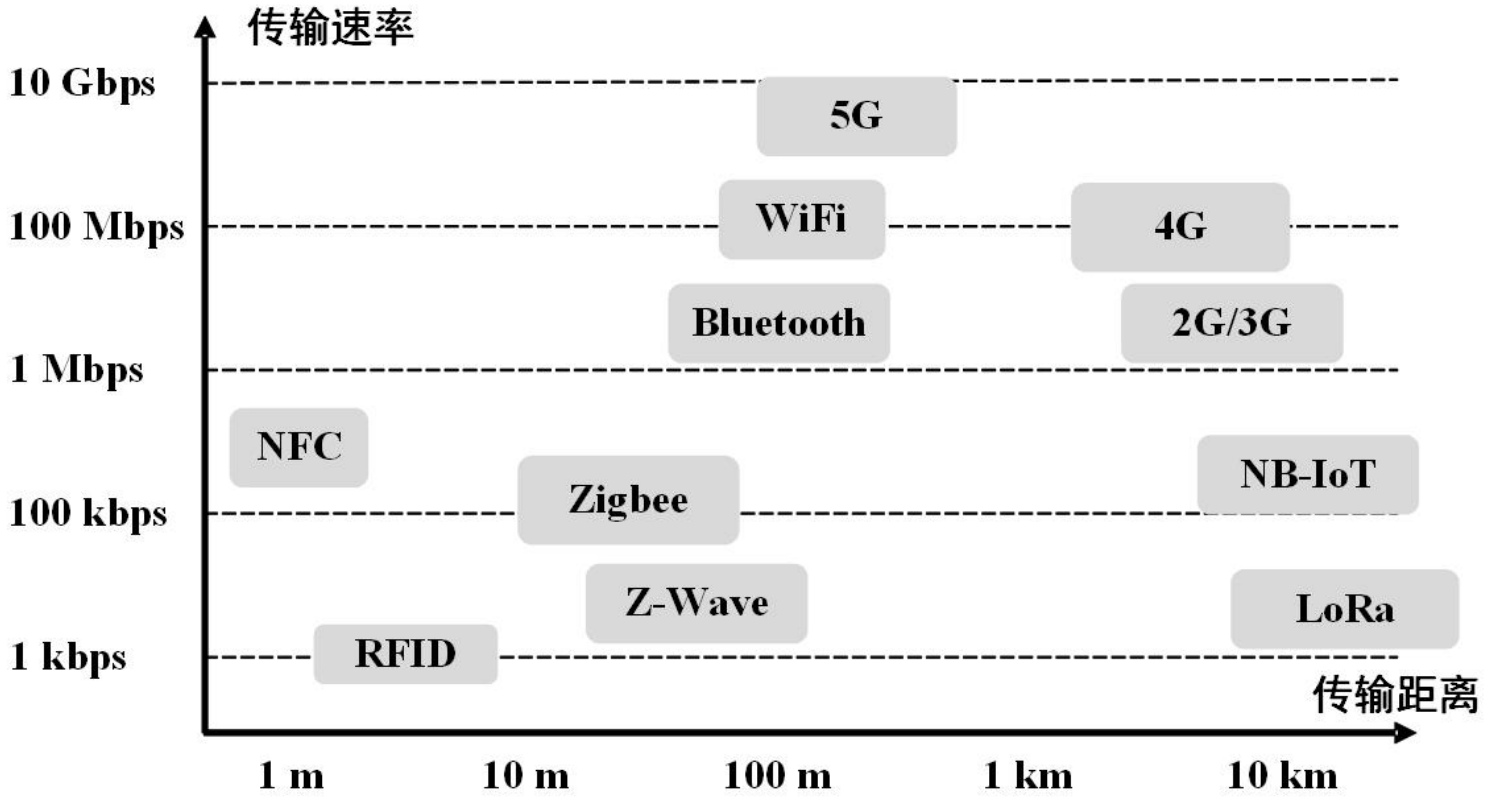


基于传输距离的无线通信协议分类图

KB版权

面向物理链路层的无线通信协议

- 常见物联网通信协议的传输速度与传输范围关系



常见无线通信协议的传输速度与传输范围关系图

版权

面向物理链路层的无线通信协议

- **1. 无线个域网通信协议（WPAN）**
  - Bluetooth、Zigbee、Z-Wave
  - Bluetooth4.0后支持节点数从8个提升到2^{32}个
  - Bluetooth5.0后最大传输距离可达300m

协议名称	Bluetooth/BLE	Zigbee	Z-Wave
工作频率	2.4GHz	2.4GHz/915MHz/868MHz	908.42MHz/868.42MHz
最大传输速率	1Mbps(1.2代)/24Mbps(4代)/ 48Mbps(5代)	250kbps	40kps
最大传输距离	300m	10m-75m	30m-100m
功耗（最大工作电流）	15mA(BLE)/30mA(BR)	40mA	23mA
拓扑结构	分散式网络/星状拓扑/ 网状拓扑（BLE）	星状拓扑/树状拓扑/ 网状拓扑	网状拓扑
最大支持节点数	2^{32}	65536	232

USSLAB版权

面向物理链路层的无线通信协议

- **2. 无线局域网通信协议（WLAN）**
  - WiFi：无限高保真协议，商用最新版本**WiFi6**
  - 传输速度：2.4GHz和5GHz两个频段上均可极限达到**9.6Gbps**
  - 传输距离：百米级别，理论最大传输距离可达几公里
  - 核心技术：
    - **MU-MIMO技术**Multi-User Multiple-Input Multiple-Output：在同一个时间和频率资源上同时为多个用户传输数据，这提高了频谱利用率和系统容量
    - **OFDMA技术**Orthogonal Frequency Division Multiple Access：将频谱分成多个正交子载波，提高了频谱利用率和系统容量
    - **ARget Wake Time**目标唤醒时间技术：一种用于节能的机制，它允许无线设备与接入点（AP）协商何时进入低功耗模式以及何时唤醒以进行数据传输降低Wi-Fi 6的功耗

内部使用，USSLAB版权

面向物理链路层的无线通信协议

- **3. 物联网无线广域网通信协议（WLAN），例如5G，其特点包括**
  - **增强移动宽带**
    （Enhanced Mobile Broadband，eMBB）
  - **海量机器连接**
    （Massive machine type communications，mMTC）
  - **低时延高可靠**
    （Ultra-reliable and low latency communications，uRLLC）
- **物联网物理层协议新形态：LPWAN低功耗无线广域网**
  - **代表协议：NB-IoT、LoRa等**
  - 适用于对**传输速率与网络延迟要求不高**的应用场景
  - 适用于终端设备不需要频繁移动，具有一定**固定性**的应用场景
  - 主要以终端设备的**上行数据**为主

内部使用，USSLAB版权

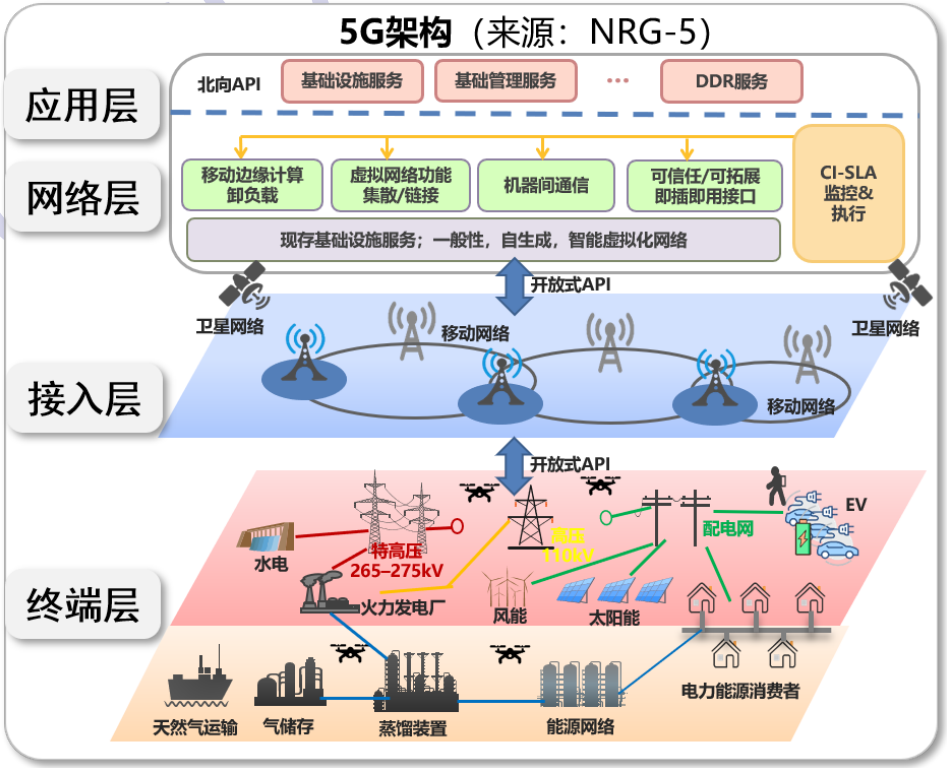
物理层协议案例：5G

- 5G：第五代移动通信技术，是新一代的移动通信技术
  - 5G具有高带宽、低延时、海量连接等特点，其架构包括应用层、网络层、接入层、终端层等。

eMBB
(增强移动带宽)
高带宽 | 异构无线网络接入

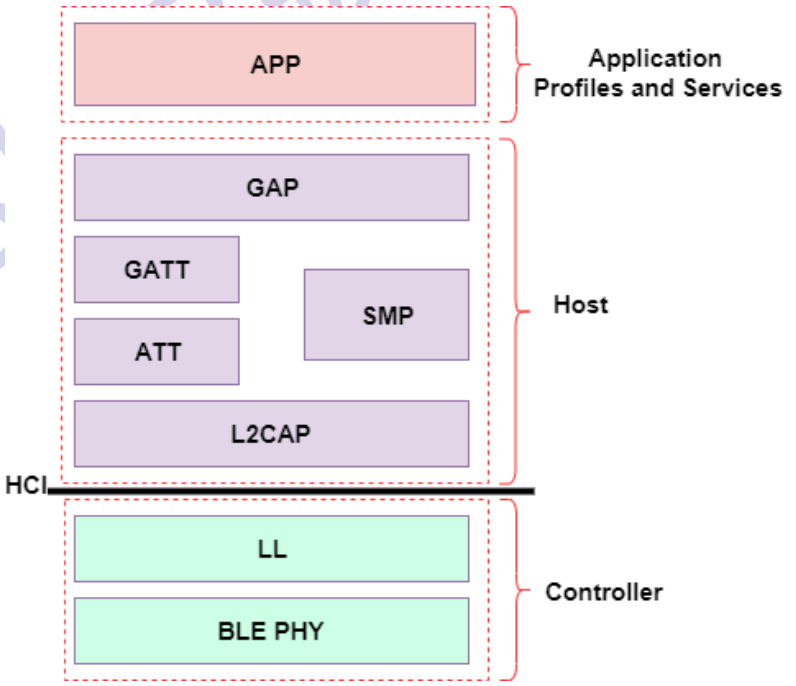
uRLLC
(超可靠低延时通信)
低时延 | 高可靠

mMTC
(海量机器类通信)
海量终端 | 极低功耗终端



物理层协议案例：Bluetooth (BT/BLE)

- **定义及特点**
  - 用于短距离无线数据交换的技术标准，使用2.4 GHz ISM频段来进行通信，具有低功耗、低成本等特点
  - 蓝牙协议包括两种技术：经典蓝牙（BT）和低功耗蓝牙（BLE）
  - 蓝牙协议四个层次
    - 物理层
    - 逻辑层
    - 逻辑链路控制和适配协议L2CAP
    - 应用层



BLE架构图

内部使用，版权

图片来源: https://ww2.mathworks.cn/help/comm/ug/bluetooth-protocol-stack.html.

物理层协议案例：Bluetooth (BT/BLE)

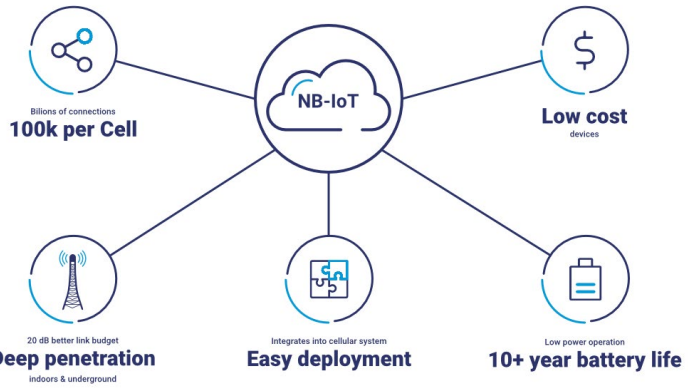
- **BLE与经典蓝牙BT的主要区别**
  - **连接方式**：BLE在完成发送和接收消息操作之后会**暂停**发射无线（但仍可以接收消息），等待下一次连接再激活；传统蓝牙是**持续保持连接**
  - **连接周期**：BLE完成一次连接(即扫描其它设备、建立链路、发送数据、认证和适当地结束)只需**3ms**；传统蓝牙完成相同的连接周期需要**数百毫秒**
  - **数据包与应用场景**：BLE的**数据包长度较短**，多应用于**实时性要求较高，但是传输速率较低**产品，遥控类的如键盘、鼠标、心跳带、血压计等；传统蓝牙使用的数据包长度较长，可用于数据量比较大的传输，如语音、音乐等。
  - **能耗**：BLE的最大工作电流为15mA，BT为30mA。

内部使用，USSLAB版权

物理层协议案例：NB-IoT

- 简介
  - NB-IoT（Narrow Band Internet of Things）：窄带物联网是一种基于蜂窝网络的低功耗广域网（LPWAN）技术，专门为了支持大规模物联网设备的接入而设计，广泛应用于需要低数据传输速率、长距离、低成本和长电池寿命的应用场景
  - 传输速度：160~250kbps
  - 功耗：正常工作时最大电流为20-50mA，但是在省电模式时平均工作电流只有**3~50μA**。
  - 应用场景：共享单车、智能水表、智能电表等终端。

NB-IoT特点

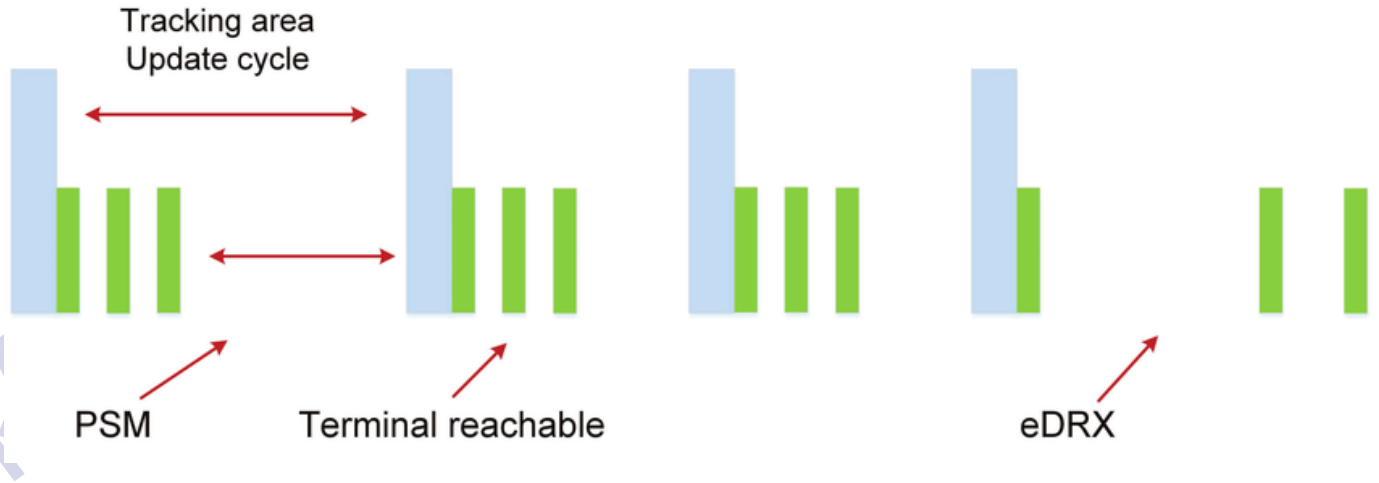


内部使用，USST版权

图片来源: https://www.grandmetric.com/2018/02/16/narrowband-internet-of-things-nb-iot-an-overview/

NB-IoT

- **关键技术**
  - **eDRX**：Extended Discontinuous Reception，增强型不连续接收。终端无需不间断监听网络，反而周期性进入睡眠状态，只在需要的时候被唤醒。eDRX是在DRX基础上进一步增加睡眠周期
  - **PSM**：Power Saving Mode，省电模式。当终端进入空闲状态时，相当于“关机”。虽然设备仍然注册在网络中，但是网络已经无法发送数据或者呼叫终端



eDRX与PSM技术示意图

参考文献： Chen, Min & Miao, Yiming & Hao, Yixue & Hwang, Kai. (2017). Narrow Band Internet of Things.

面向物理链路层的无线通信协议

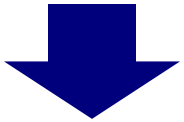
- **无线通信协议特性表**

协议名称	使用频率	传输速率	覆盖范围	能耗
RFID	多频段	100Bps - 1kbps+	10cm - 2m	低
NFC	13.56MHz	106kbps - 848kbps	0 - 20cm	低
Zigbee	2.4GHz，subGHz	250kbps	10m - 75m	低
Z-Wave	subGHz	40kbps	30m - 100m	低
Bluetooth/BLE	2.4GHz	1-3Mbps	10m - 300m	低
WiFi	2.4GHz, 5GHz	54Mbps-9.6Gbps	百米级别	低
2G/3G	蜂窝频段	10Mbps	2km - 10km	高
4G	蜂窝频段	100Mbps	1km - 3km	高
5G	蜂窝频段	10Gbps	百米级别	高
LoRa	subGHz	50kbps	**15km**	低
NB-IoT	蜂窝频段	200kbps	**2km - 20km**	低

B版权

面向应用层的轻量化消息传输协议

- **传统互联网应用层协议**
  - HTTP（HyperText Transfer Protocol，超文本传输协议）
  - FTP（File Transfer Protocol，文件传输协议）
  - 不足点：
    - 协议不适用于资源受限设备
    - 协议实时性低



改进方向：轻量化且实时性高

内部使用，USSLAB版权

面向应用层的轻量化消息传输协议

- 物联网新型传输协议：MQTT消息队列遥测传输（Message Queuing Telemetry Transport）

HTTP

- 同步协议
- 请求/响应模式
- 单向连接
- 相对复杂的标头和传输规则

- 不适用于不可靠或高延时网络
- 不适用于资源受限网络
- 客户端无法被动接收指令

MQTT

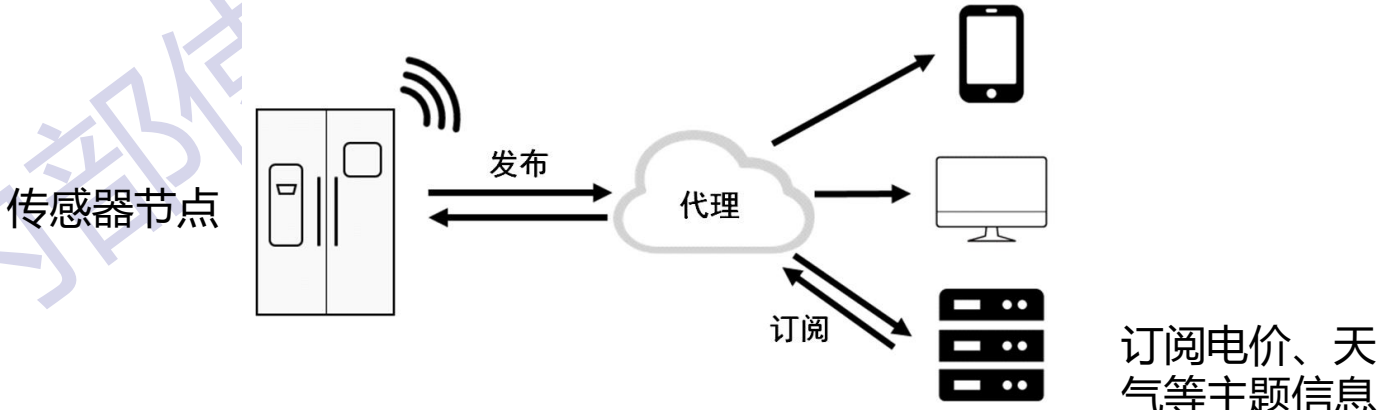
- 异步协议
- 订阅/发布模式
- 双向连接
- 仅两个字节的固定报头

- **适用于物联网资源受限或实时通信网络**
- 提供可靠传输（QoS）

内部使用，USSLAB版权

应用层协议案例：MQTT协议

- **定义**：消息队列遥测传输MQTT(Message Queuing Telemetry Transport)：一种基于**发布/订阅模式**的轻量级通讯协议，提供**多对多**的消息发布。
- **特点**：低开销、低带宽占用、即时通讯。MQTT传输层使用TCP提供可靠网络连接，提供有序无损连接。
- **消息代理Broker**：MQTT服务器，可以是一个应用程序或一台设备，位于消息发布者和订阅者之间。
- **主题Topic**：连接到一个应用程序消息的标签，该标签与服务器的订阅相匹配。服务器会将消息发送给订阅所匹配标签的每个客户端。
- 应用实例：电动车何时充电问题。



MQTT协议示意图

内部使用，USSLAB版权

应用层协议案例： CoAP协议

- **CoAP**
  - CoAP（Constrained Application Protocol，受限制的应用协议）是一种基于面向资源受限设备的通信协议。
  - 采用“请求-响应”模型，可以理解成HTTP协议的简化版本，支持get、post等功能。
  - 区别：HTTP采用TCP，COAP使用UDP。

- **协议特点：**
  - 请求/响应模型
  - 双向通信
  - 轻量、低功耗
  - 传输层使用UPD协议

内部使用，USSLAB版权

MQTT和CoAP对比

- MQTT协议使用**发布/订阅**模型，CoAP协议使用**请求/响应**模型；
- MQTT是基于**TCP**的长连接，CoAP协议是基于**UDP**无连接；
- MQTT通过中间代理传递消息的**多对多**协议，CoAP协议是Server和Client之间消息传递的**单对单**协议；

特征	MQTT	CoAP
传输层协议	TCP	UDP
通信模型	订阅/发布	请求/响应
通信对象模式	一对一、一对多、多对一	一对一
能耗	MQTT >	CoAP
固定头大小	2个字节	4个字节
可靠性	3种QoS等级	4种消息类型
同步模式	异步	异步与同步
安全性	未定义，可使用TLS / SSL	DTLS或IPsec

SLAB版权

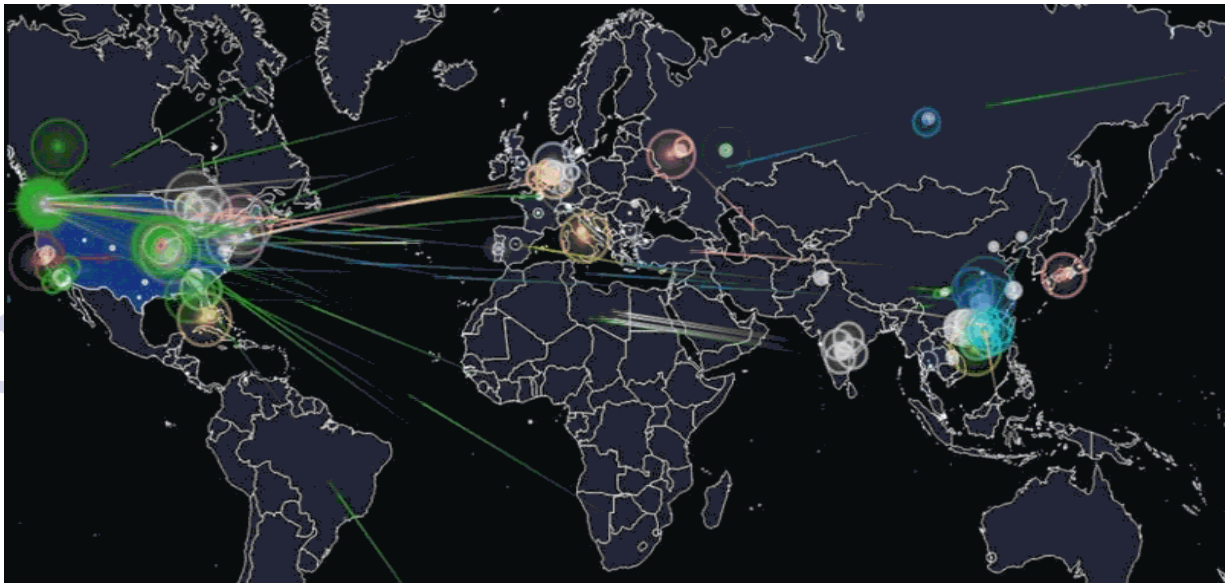
8.2 物联网管道安全风险

- 8.2.1 概述
- 8.2.2 物联网管道威胁分类
- 8.2.3 常见的针对物联网管道的攻击

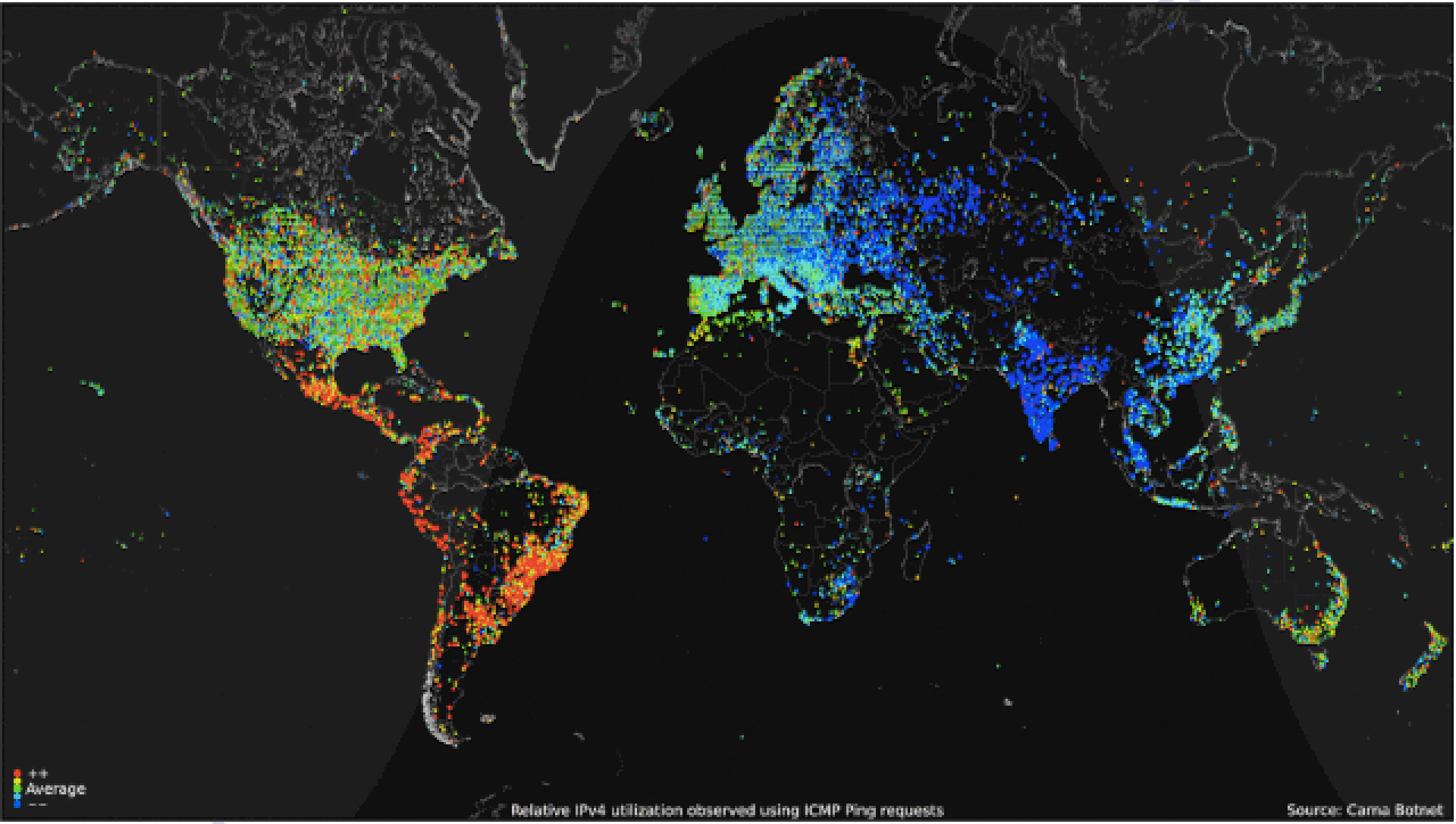
内部使用，USSLAB版权

引入：Mirai攻击

- Mirai：日语的“未来”的意思。要感染对象是网络上的消费级电子设备，例如网络监控摄像机和家庭路由器等。
- 事件：2016年10月，美国主要域名解析服务商DYN遭受来自物联网设备的DDoS攻击，牵涉到的受感染物联网设备数量众多。
- 攻击后果：使得很多重要网站无法正常打开，包括GitHub、 Twitter、Reddit、Netflix和Airbnb等。

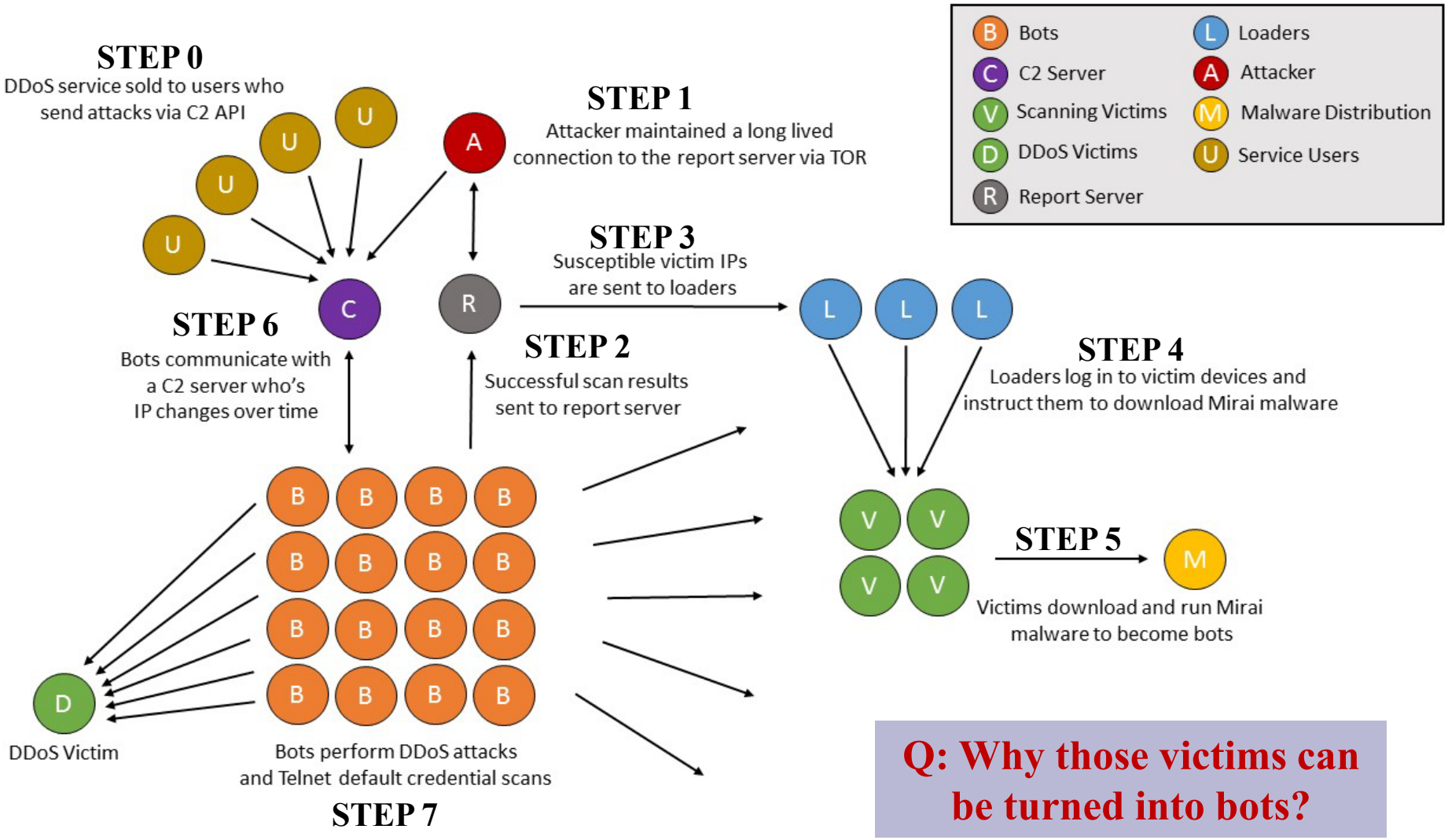


USSLAB版权



Source:
Carna Botnet Census of 2012
http://census2012.sourceforge.net/paper.html

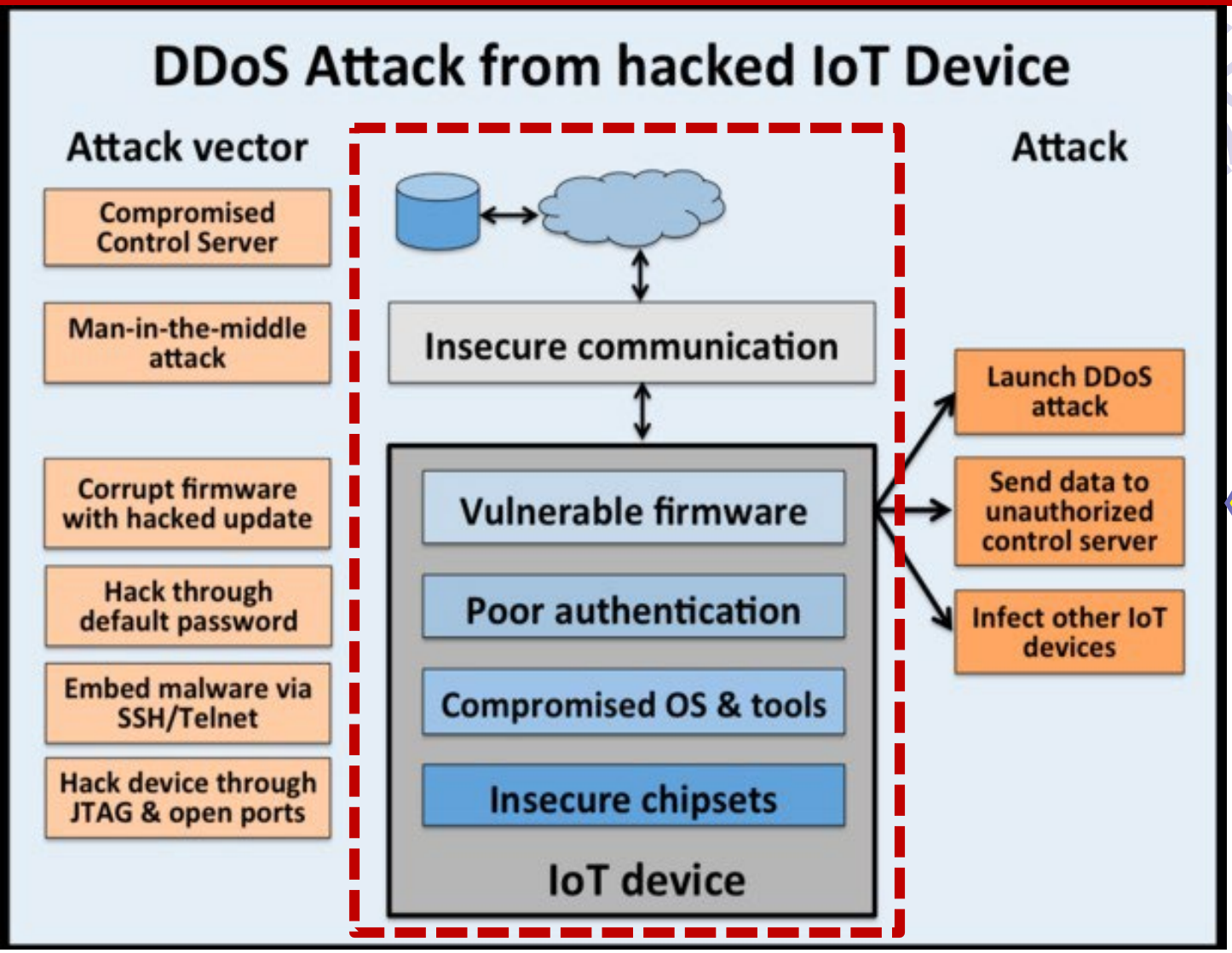
How Did Mirai Work?
DDoS Attacks of October 21, 2016



Q: Why those victims can be turned into bots?

Reference: Mirai Botnet - William Favre Slater, III

How Did Mirai Work?
DDoS Attacks of October 21, 2016



Infected IoT Devices:

1) Launch DDoS Attacks
2) Report data to C2 Servers
3) Infect other IoT Devices

Reference: Mirai Botnet - William Favre Slater, III

Mirai Botnet来源

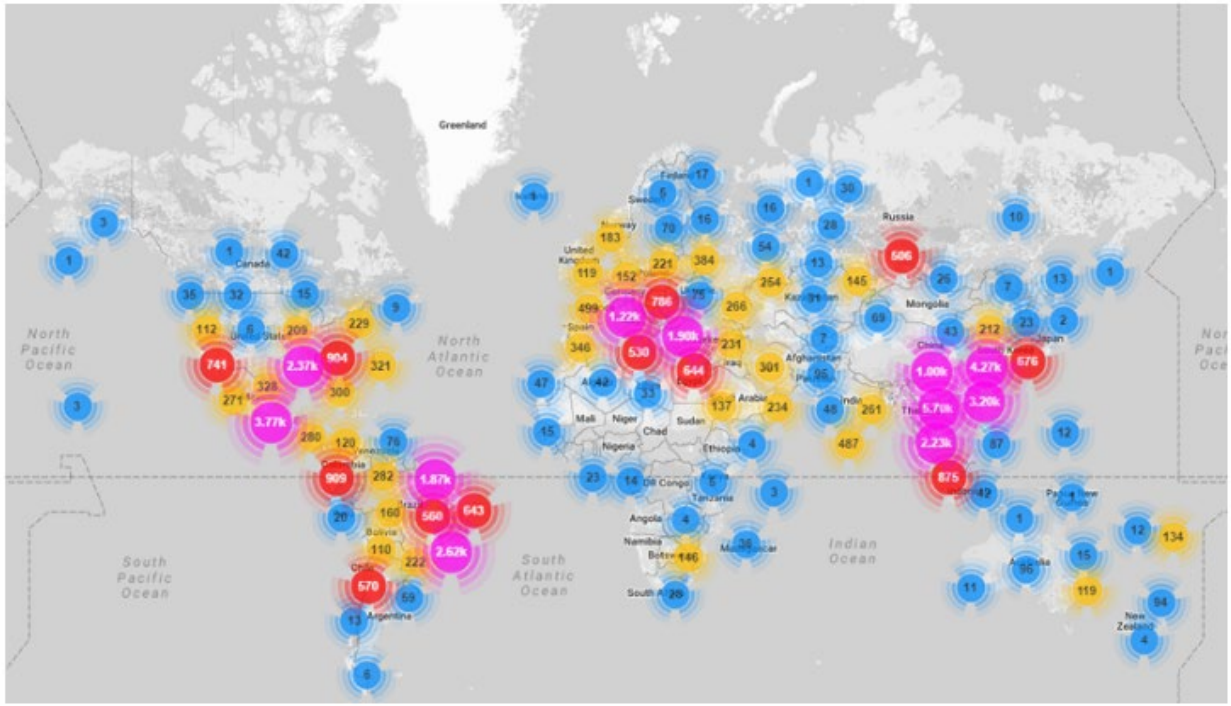


Figure 2: Geo-locations of all Mirai-infected devices uncovered so far

Country	% of Mirai botnet IPs
Vietnam	12.8%
Brazil	11.8%
United States	10.9%
China	8.8%
Mexico	8.4%
South Korea	6.2%
Taiwan	4.9%
Russia	4.0%
Romania	2.3%
Colombia	1.5%

版权

Source:https://www.incapsula.com/blog/malware-analysis-mirai-ddos-botnet.html

物联网通信安全——攻击分类体系

- 本章将从多维度对物联网通信过程中存在的常见攻击类型进行分类描述
- 每一行是针对物联网管道攻击的分类方式，列表示常见的攻击类型

	攻击作用点			攻击手段		攻击方式		攻击目的			攻击后果			
	流量	协议	信道	主动攻击	被动攻击	本地攻击	远程攻击	侦察	访问	阻塞网络	信息泄露	权限提升	拒绝服务	输出错误
嗅探攻击	■				■	■		■			■			
中间人攻击	■			■		■	■		■		■	■	■	■
暴力破解		■		■		■	■		■		■	■		
欺骗攻击		■		■		■	■		■		■	■		
重放攻击	■			■		■	■		■		■	■		■
DOS攻击	■			■		■	■			■			■	
DDOS攻击	■			■		■	■			■			■	
干扰攻击			■	■		■				■			■	
侧信道攻击	■		■		■	■		■			■			

电子CSLAB版权

物联网通信安全

- **攻击作用点**
  - 信道
    - 物联网无线通信信道的**开放广播特性**，使其容易受到干扰攻击
  - 协议
    - 物联网通信协议栈中存在**设计和实现**方面的安全漏洞
  - 流量
    - 物联网通信流量易被攻击者获取并被**分析和恶意利用**

版权所有，USSLAB版权

物联网通信安全

- **攻击手段**
  - **被动攻击**
    - 监听和窃取重要的机密信息
    - 不影响正常的数据通信，通常破坏**传输数据的机密性**
    - 举例：包括嗅探、侧信道攻击等攻击方式
  - **主动攻击**
    - 攻击者主动查看、控制、篡改数据包，进而可以数据和指令篡改、扩展、删除以及重放等
    - 主要破坏传输数据的**完整性和可用性**
    - 举例：包括中间人攻击、欺骗攻击、重放攻击、(D)DoS攻击等

内部使用 USSLAB版权

物联网通信安全

- **攻击方式**
  - **本地攻击**
    - 由物联网**边界内的主体**，即“内部人员”发起的攻击
    - 内部人员具有对基础结构的授权访问权限，甚至可能对存储敏感信息的服务器具有访问权限，如邮件服务器，数据库服务器等
    - 内部威胁不仅是员工，也可以是进入组织工作的承包商、供应商，甚至是志愿者
  - **远程攻击**
    - 攻击者位于**物联网网络实体范围**之外进行攻击
    - 攻击者通过不断的尝试与试错的方法来达到在物联网本地网络中成功访问的目的

内部使用，USTAB版权

物联网通信安全

- **攻击目的**
  - **侦察型攻击**
    - 潜入被**攻击者网络内部**进行情报获取和收集，寻求可利用目标系统、完成进一步的攻击
    - 例如，攻击者使用**端口扫描**去发现任何易受攻击的端口。端口扫描之后，攻击者通常即可利用已知的漏洞
  - **访问型攻击**
    - 未经授权的入侵者可**创建访问权限**，进而造成物联网信息传输过程中受到非法添加、删除、替换等安全威胁
    - 例如，被Mirai病毒侵入的物联网设备使入侵者获得更高的访问权限
  - **阻塞网络型攻击**
    - 通过**降低系统速度**使系统崩溃或无法使用的攻击，例如拒绝服务攻击
    - 案例：Mirai发动了针对新加坡、利比里亚、德国的DoS攻击

内部使用，USSLAB版权

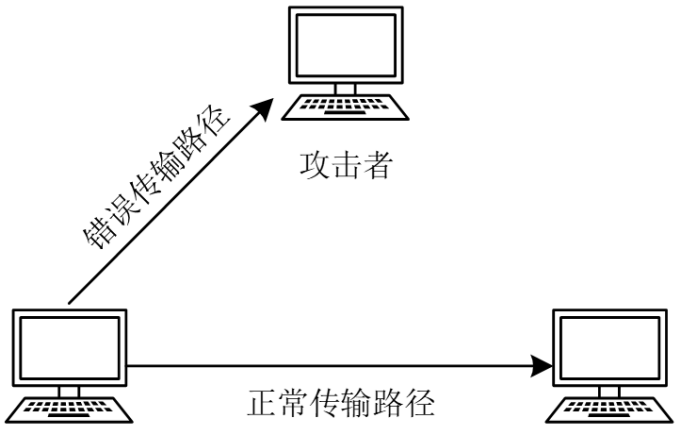
物联网通信安全

- **攻击后果**
  - **信息泄漏**
    - 攻击导致通信数据的泄漏，通常包括用户数据泄露和系统信息泄露，包括常见的嗅探攻击、侧信道攻击等
  - **权限提升**
    - 攻击成功后获得系统的一般用户访问权限甚至管理员权限，包括常见的密钥暴力破解、重放攻击等
  - **拒绝服务**
    - 影响物联网用户的相关服务或是发送方式，即影响相关物联网设备的通信或者使用
  - **输出错误**
    - “输出”是一个涵盖很广的概念，既表示物联网终端的显示、网络连接上所传输的数据，也代表系统目标，包括篡改攻击、重放攻击等

内部使用，USSLAB版权

物联网通信安全——嗅探攻击

- **嗅探攻击(Sniffing attack)**：攻击者通过特定的工具或软件，监听和捕获在网络中传输的数据包的行为。网络嗅探攻击是一种被动攻击方式，攻击者不需要主动干预数据传输，仅需监听并收集感兴趣的数据
- **常见嗅探工具**：许多合法网络分析工具可以被用于嗅探攻击，包括但不限于：
  - **Wireshark**：网络协议分析仪，用于捕获和分析数据包。
  - **Tcpdump**：命令行工具，能够捕获和分析网络接口上传输的数据包
  - **Ettercap**：支持中间人攻击的网络分析工具，能够执行嗅探、数据包注入等操作。



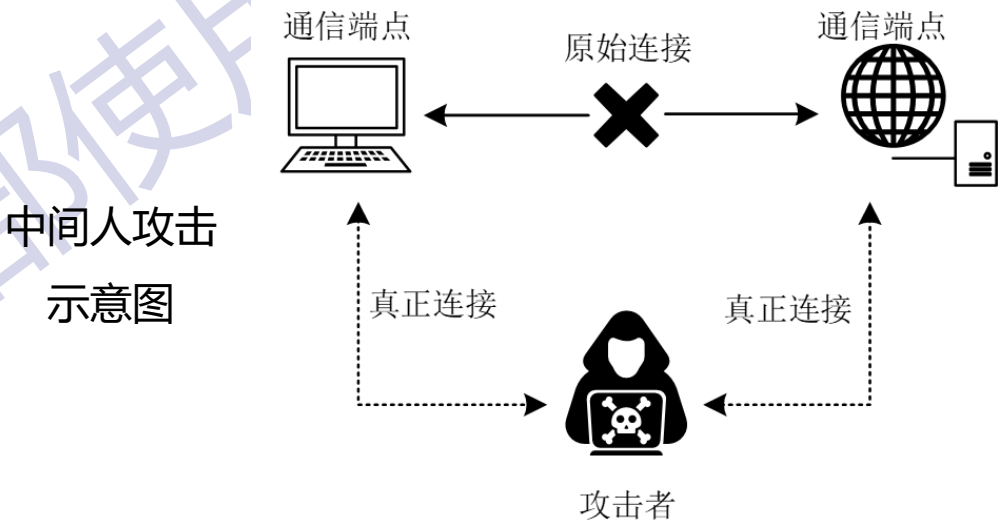
物联网通信安全——嗅探攻击

- **举例：** GSM短信嗅探(GSM Sniffing)是一种嗅探电话信息的方法
- **原理**
  - GSM协议安全漏洞：明文传输
  - 基站连接漏洞：根据信号强度判断
  - 伪基站攻击：利用移动信令监测系统监测移动通讯过程中的各种信令过程，获得手机用户当前的位置、短信验证码信息等

内部 BUPT USSLAB版权

物联网通信安全——中间人攻击

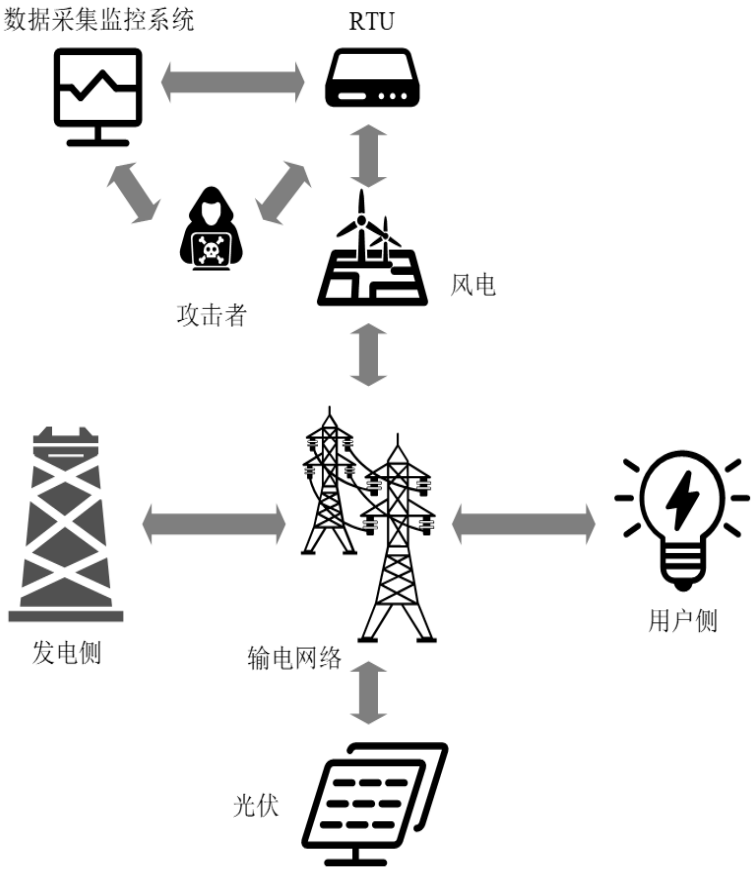
- **中间人攻击(Man-in-the-middle attack)**：攻击者与通讯的两端分别创建独立的联系，并交换其所收到的数据，使通讯的两端认为他们正在通过一个私密的连接与对方直接对话，但事实上整个会话都被攻击者完全控制
- 回顾：Diffee-Helman协议中的中间人攻击
- 流程：攻击者首先“嗅探”网络的流量以拦截一对合法通信节点的MAC地址，然后冒充两个受害者并最终建立与他们的连接



内部使用，USSLAB版权

物联网通信安全——中间人攻击

- **举例：电力虚假数据注入攻击**
  - 电力通信网络具有安全分区、网络专用、横向隔离、纵向认证的特点
- **原理**
  - 利用能量管理系统中的坏数据检测漏洞和状态估计器中不良数据辨识方法的局限性，通过中间人攻击的手段发送恶意篡改元件的量测值
- **结果**
  - 控制中心错误判断电网当前状态，造成电力系统安稳控制措施误动或拒动，影响电力系统安全稳定运行

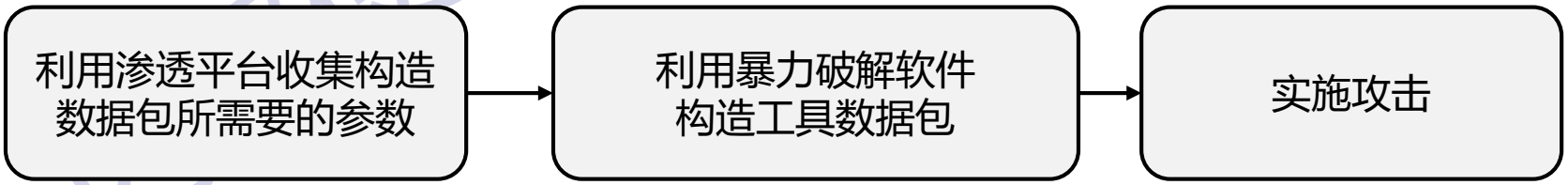


电网中的中间人攻击图示

内部使用，未经授权

物联网通信安全——暴力破解攻击

- **暴力破解(Brute-force attack)：**攻击者系统地组合所有可能的账户名和密码，尝试所有组合是否能够登录，破解用户的账户、密码等信息
- **举例**
  - SSH是建立在应用层基础上的安全协议，是为远程登录会话和其他网络服务提供安全性的协议
  - **SSH（Secure Shell）暴力破解**：是自Linux平台诞生以来就存在的一种攻击行为，至今已经衍生出针对Telnet、Ftp、Smtp等服务的暴力破解方式

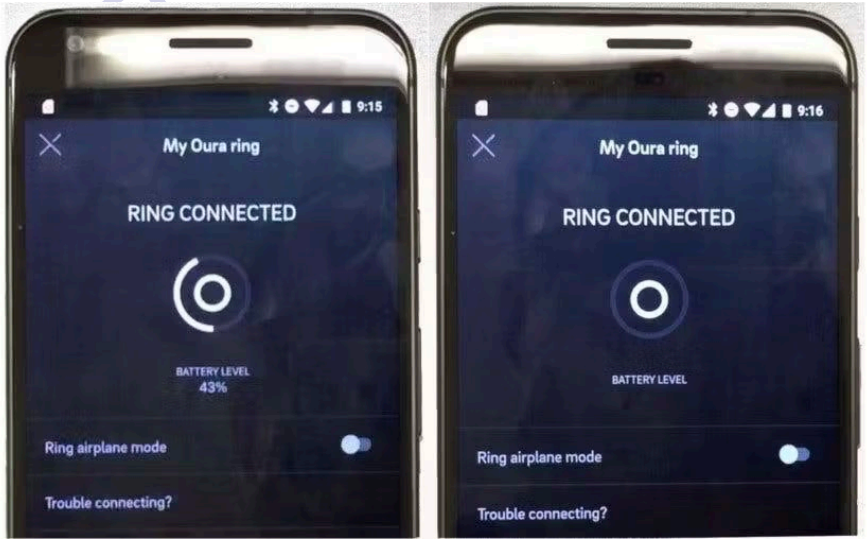


暴力破解攻击示意图

仅供使用 SSLAB版权

物联网通信安全——欺骗攻击

- **欺骗攻击(Spoofing attack)**：其中攻击者伪装成合法实体，以欺骗目标系统或用户，攻击可以发生在不同层次的网络通信中，例如网络层、传输层和应用层甚至是物理层。
- 举例：蓝牙低功耗漏洞——BLESA。攻击者假装是先前配对的服务器设备，拒绝来自客户端的身份验证请求设备，然后将欺骗数据提供给客户端



内部资料 USSLAB版权

物联网通信安全——重放攻击

- **重放攻击(Replay attack)：**攻击者发送目的设备已接收过的数据包/信号，来达到欺骗系统的目的，主要用于身份认证过程，破坏认证的正确性
- **举例：** RFID重放攻击中攻击者利用USRP、HackRF等攻击设备，读取受害者身上的射频卡信息，然后通过将这些数据写入空白卡进行重放攻击，获取他人的身份验证或者其它敏感信息

内部使用 USSLAB版权

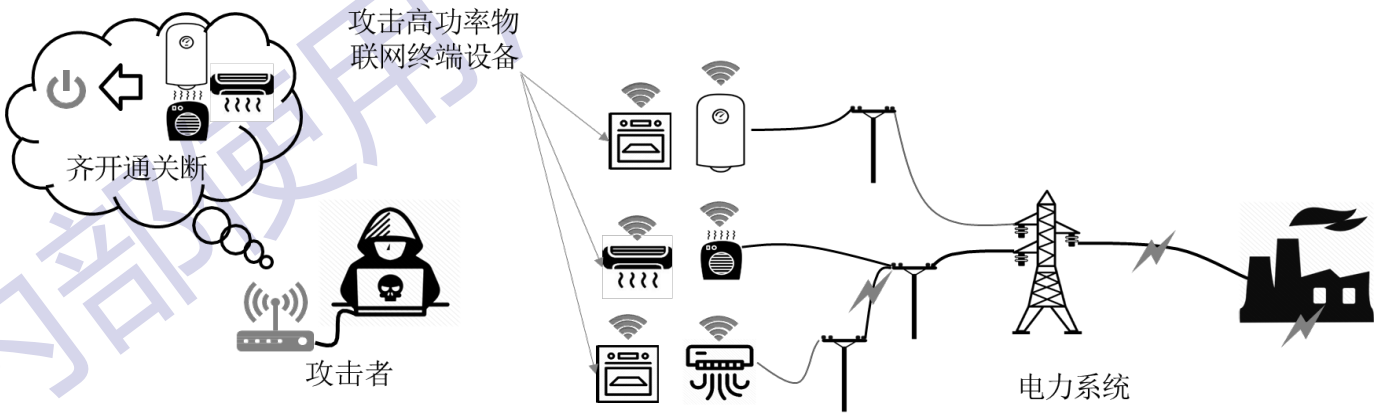
物联网通信安全——拒绝服务攻击

- **拒绝服务攻击(Denial-of-service attack)**：通过向目标设备或服务器中注入大量的请求，消耗目标系统的资源（如网络带宽、处理能力、内存等），使合法用户无法访问这些资源，暂时或无限期地中断连接到网络的服务来使设备或网络资源无法供其预期的用户使用
- **分类**：单一来源的拒绝服务攻击（单一DoS）和分布式拒绝服务攻击（DDoS）
- **攻击类型**
  - 流量耗尽型攻击：ICMP 洪泛攻击、UDP 洪泛攻击
  - 协议攻击：利用协议漏洞达到攻击目的，例如SYN洪泛攻击发送大量的TCP SYN请求包但不完成握手过程，导致目标服务器的资源耗尽

内部使用，USSLAB版权

物联网通信安全——分布式拒绝服务攻击

- **分布式拒绝服务（DDoS）攻击：**通过同时利用多个受控计算机或设备（通常称为“僵尸网络”）发动的拒绝服务攻击
- **举例**
  - 物联网操纵需求（MadIoT）攻击：攻击者可以通过恶意控制物联网设备来操纵总电力需求从而破坏电网的正常运行
  - MadIoT攻击可导致电网频率不稳定、线路故障甚至级联故障等



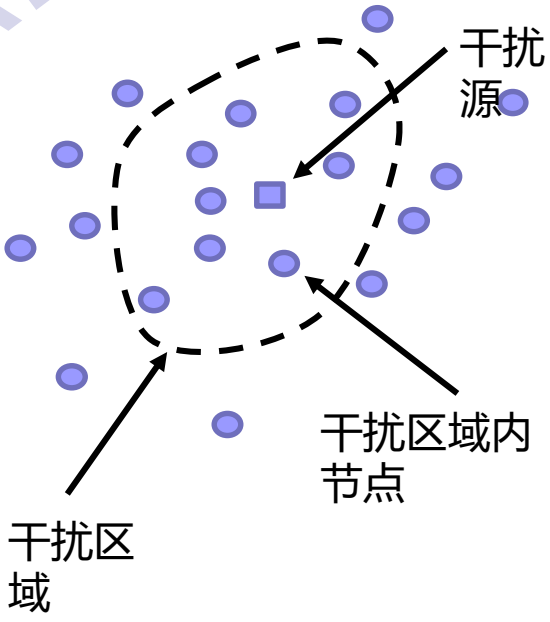
物联网操纵需求攻击（MadIoT）示意图

内部使用 USTLAB版权

Saleh Soltan, et. al., BlackIoT: IoT Botnet of High Wattage Devices Can Disrupt the Power Grid, USENIX Security'18

物联网通信安全——干扰攻击

- **干扰攻击(Jamming attack)：**
  - **定义**：通过占用网络节点通信信道，使其不能进行正常数据收发的攻击方式，干扰攻击的发起者称之为干扰源
  - 干扰者是一个有意进行信号的发送和接收通讯的实体，目的是干扰合法无线通信，通过阻止实际流量源发出数据包，或阻止接收合法数据包来实现此目标
  - 实例：通过干扰特斯拉超声波测距传感器，使其检测不到障碍物



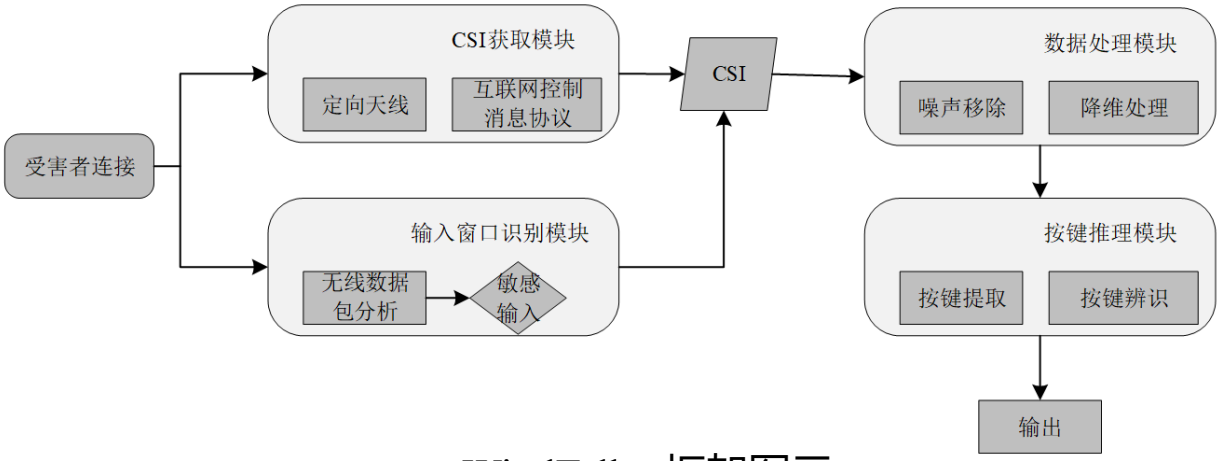
干扰攻击示意图

信道安全的本质问题：物理通信信道的开放性

内部使用 ISSLAB版权

物联网通信安全——侧信道攻击

- **侧信道攻击(Side-channel attack)**
  - **定义**：原指基于从密码系统的物理实现中获取的信息的一种攻击手段。现在可以扩展到利用报文、时间、功耗、物理信号对系统的攻击
  - 举例：WindTalker攻击，通过基于WiFi的侧信道信息来推断移动物联网设备键盘敲击动作，具体来讲，攻击者利用CSI信号波动与按键之间的强相关性来推断用户输入的数字

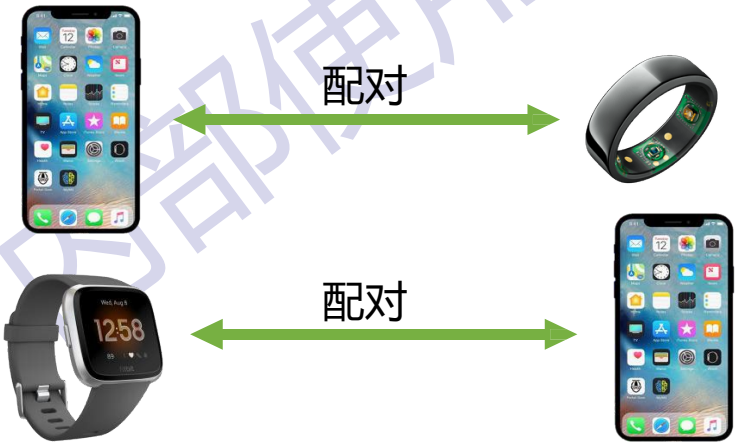


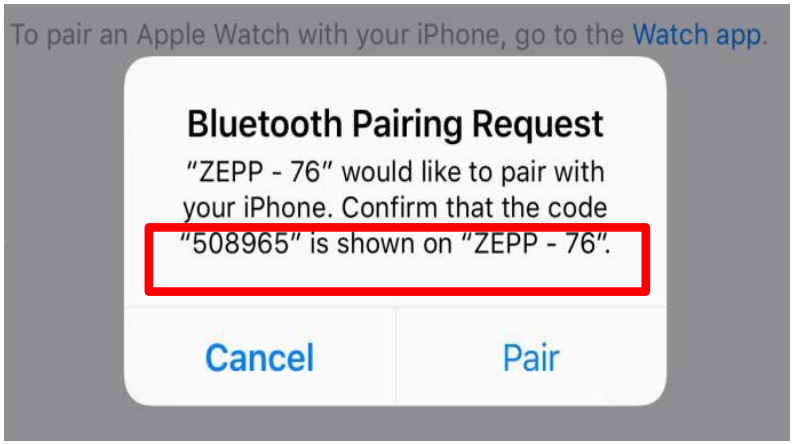
WindTalker框架图示

内部 HIT CSSLAB版权

攻击案例1：针对蓝牙协议的攻击

- **案例背景**
  - 低功耗蓝牙(BLE)漏洞——BLESA：利用了协议实现中的重连接过程中的漏洞，使攻击者能够在蓝牙设备重连接时伪造身份并与设备进行通信，从而可能导致数据泄露或设备控制。BLESA漏洞源于设备掉线后**重新连接**过程中发生的**身份验证问题**
  - 攻击者假装是先前配对的服务器设备，拒绝来自客户端的身份验证请求设备，然后将欺骗数据提供给它，该漏洞可能影响数十亿物联网设备，并且在安卓设备中仍然未修补

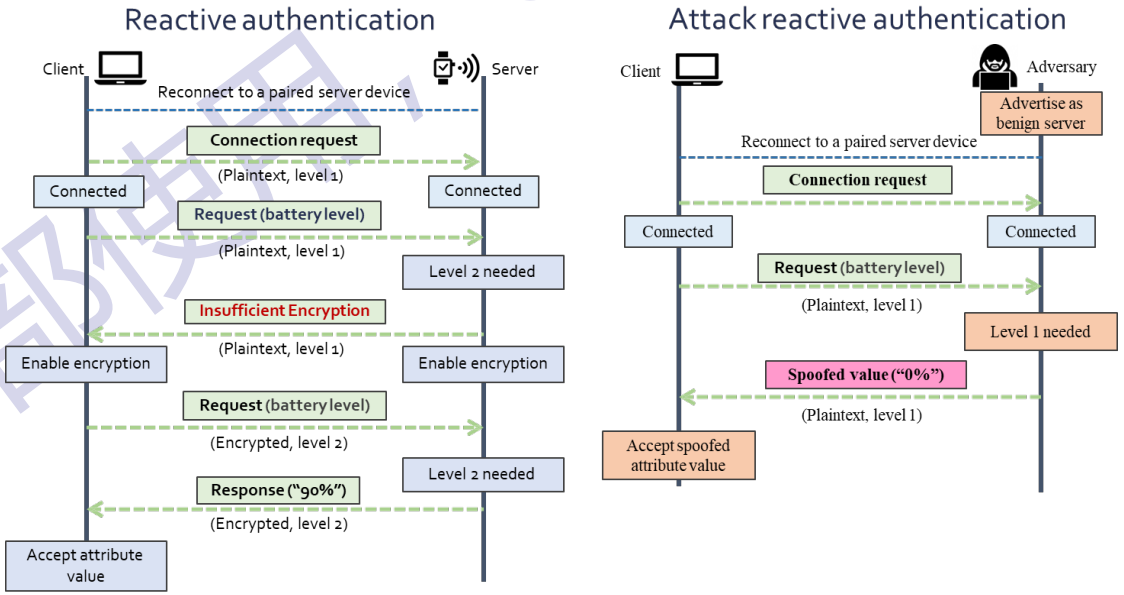




仅供使用，USSLAB版权

攻击案例1：针对蓝牙协议的攻击

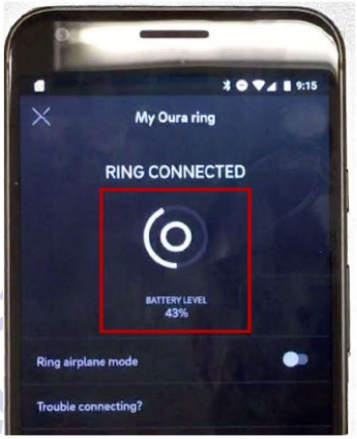
- **攻击原理**
  - BLE 的安全等级包括leve l和leve 2，分别是明文传输和加密传输
  - **降级攻击**：攻击者拦截客户端的安全等级读取请求，并以欺骗值进行响应。由于客户端没有遇到任何错误消息，因此**错误地假定可以在最低安全级别**（即明文传输）访问该值，客户端不启用加密/身份验证，它接受欺骗属性值



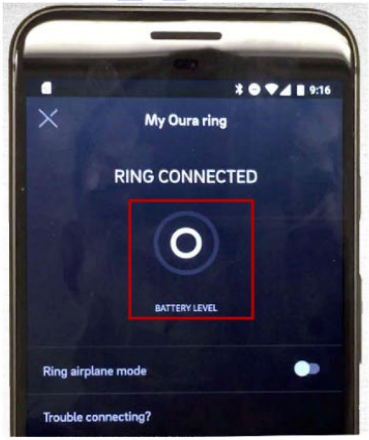
内部使用，USTC版权

攻击案例1：针对蓝牙协议的攻击

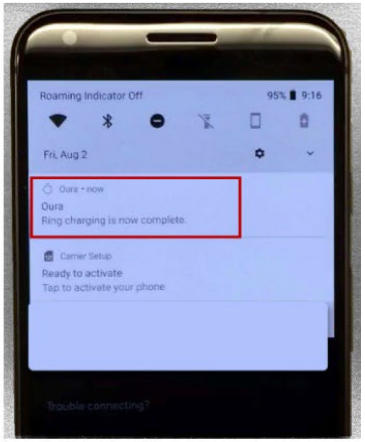
- **攻击效果**
  - OuraRing设备实际电池电量是43％，攻击者利用BLESA漏洞成功注入了欺骗性电池电量（100％）数据和通知充电完成
  - 伪造消息让应用程序认为电池电量为100％、即充电完成，并向用户显示了错误通知



良性电池电量（43％）



欺骗电池电量（100％）



伪造的充电通知

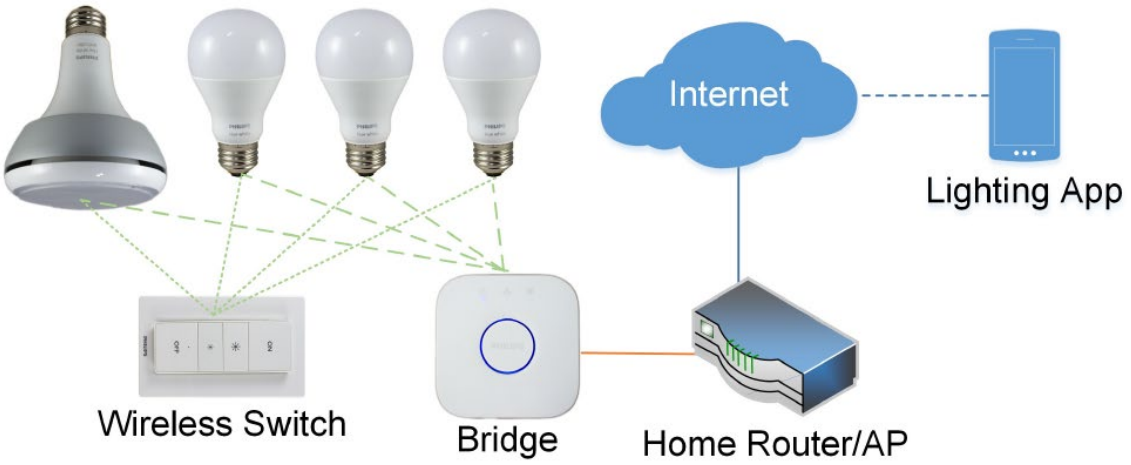
在Google Pixel手机上的Oura Ring应用程序演示BLESA对数据显示的影响

USSLAB版权

参考文献： J. Wu, “BLESA: Spoofing Attacks against Reconnections in Bluetooth Low Energy”, in Usenix Security Woot 2020

攻击案例2：IoT Goes Nuclear

- **案例背景**
  - 智能灯泡控制系统中，控制器与灯泡之间通过Zigbee协议进行通信，并且基于ZigBee Light Link（ZLL） 标准
  - 设备中使用Atmel生产的Zigbee芯片并自带有加密功能
  - **ZLL临近检测漏洞**：ZLL配对过程中，设备或者配对信息在进行传输时未能完全实现加密或者未能实现充分的身份验证



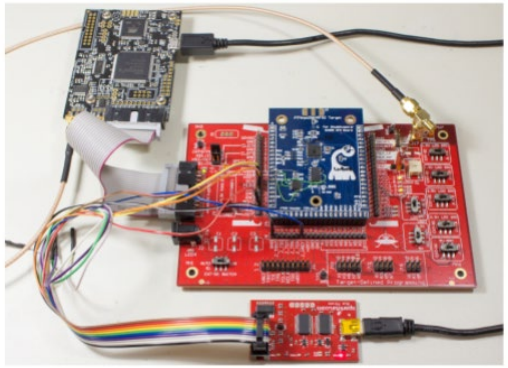
ZLL结构示意图

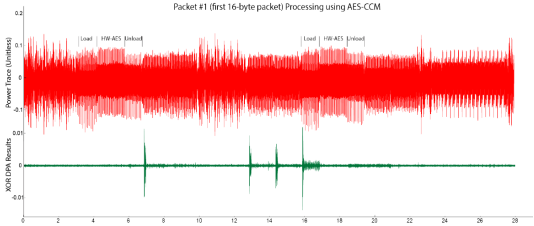
内部资料 CSLAB版权

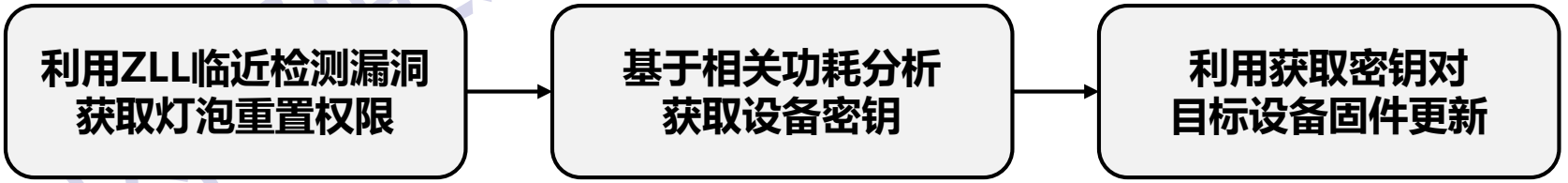
参考文献： Ronen E et al. IoT goes nuclear: Creating a ZigBee chain reaction.

攻击案例2：IoT Goes Nuclear

- **攻击原理**
  - **Step1**：利用ZLL临近检测漏洞重置灯泡
  - **Step2**：利用相关功耗分析，分析设备加密时产生的功耗推测设备密钥
  - **Step3**：利用获取的密钥实现对目标设备Over-the-air(OTA)固件更新。由于设备之间可相互通信，因此单点设备被攻击后可接着重置相邻设备，进而实现攻击的扩散







攻击机理示意图

参考文献：Eyal Ronen, etc., Ronen E et al. IoT goes nuclear: Creating a ZigBee chain reaction, in Usenix Security 2017

攻击案例2：IoT Goes Nuclear

- **攻击效果**
  - 实现对飞利浦灯泡的重置与固件更新，并进而实现对其的恶意开关操作
  - 通过单点设备感染其相邻设备，实现蠕虫病毒的规模扩散
  - 通过插入一个被感染的灯泡来打开或关闭所有的灯泡
  - 研究者在大学校园里进行实验，成功控制了汽车沿路建筑物中安装的所有Hue智能灯

内部使用，USS 版权

参考文献： Ronen E et al. IoT goes nuclear: Creating a ZigBee chain reaction.

如何对物联网通信安全防护?

内部使用，USSLAB版权

物联网通信安全——攻击分类体系

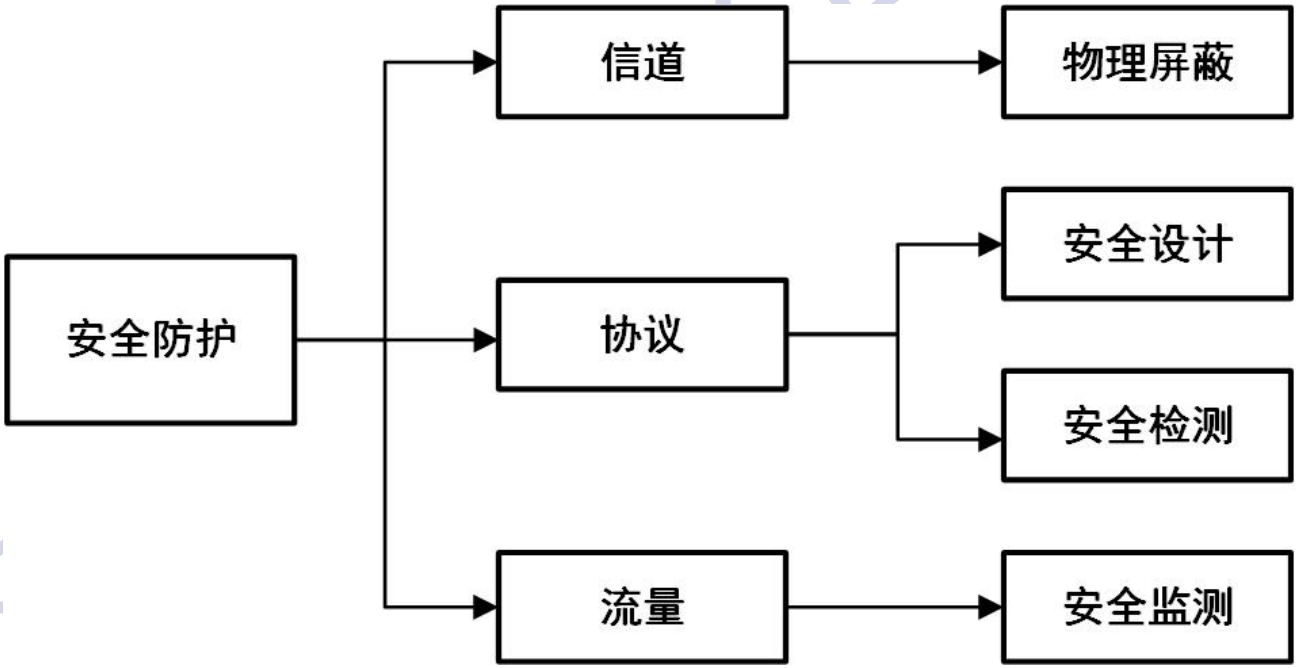
- 回顾下物联网通信安全的常见攻击类型：

	攻击作用点			攻击手段		攻击方式		攻击目的			攻击后果			
	流量	协议	信道	主动攻击	被动攻击	本地攻击	远程攻击	侦察	访问	阻塞网络	信息泄露	权限提升	拒绝服务	输出错误
嗅探攻击	■				■	■		■			■			
中间人攻击	■			■		■	■		■		■	■	■	■
暴力破解		■		■		■	■		■		■	■		
欺骗攻击		■		■		■	■		■		■	■		
重放攻击	■			■		■	■		■		■	■		■
DOS攻击	■			■		■	■			■			■	
DDOS攻击	■			■		■	■			■			■	
干扰攻击			■	■		■				■			■	
侧信道攻击	■		■		■	■		■			■			

AB版权

8.3 物联网管道安全防护

- **信道**：物理屏蔽等
- **协议**：属于软件安全范畴，防护包括安全设计与安全检测
- **流量**：流量安全监测等



物联网管道防护方法体系图

CLAB版权

8.3.1 面向协议的安全设计

- 国际电信联盟(ITU)在1991年颁布“数据通信网：开放系统互连(OSI)；安全、结构和应用”规范规范（X.800），规定了系统协议层提供安全服务，包括：
  - 访问控制（Access control）
  - 加密机制（Encipherment）
  - 数字签名（Digital Signature）
  - 数据完整性（Data integrity）
  - 认证交换（Authentication exchange）
  - 流量填充（Traffic padding）
  - 路由控制（Routing control）
  - 公证（Notarization）

内部使用，USSLAB版权

https://www.itu.int/rec/T-REC-X.800/en

8.3.1 面向协议的安全设计

- X.800提供的安全服务
  - **认证服务（Authentication）**
    - 对等实体认证与数据源认证
  - **访问控制（Access Control）**
  - **数据机密性（Confidentiality）**
    - 连接机密性、无连接机密性、选择字段机密性以及流量机密性
  - **数据完整性（Integrity）**
    - 可恢复连接完整性、无恢复连接完整性、选择字段连接完整性以及无连接完整性
  - **不可否认性（Non-Repudiation）**
    - 数据源抗否认与投递抗否认
  - **可用性（Availability）**

内部使用，USSLAB版权

8.3.1 面向协议的安全设计

- 安全服务和安全机制关系表

服务	机制							
	加密机制	访问控制	数字签名	数据完整性	认证交换	流量填充	路由控制	公证
对等实体认证	■		■		■			
数据源认证	■		■					
访问控制服务		■						
连接机密性	■						■	
无连接机密性	■						■	
选择字段机密性	■							
流量机密性	■					■	■	
可恢复连接完整性	■			■				
无恢复连接完整性	■			■				
选择字段连接完整性	■		■	■				
无连接完整性	■		■	■				
数据源抗否认			■	■				■
投递抗否认			■	■				■

版权

安全机制在通信协议中的应用案例

- 物联网通信安全，可以设计或特定的**安全协议**或者现有协议中增加安全机制：
  - IPSec
  - SSL/TLS
  - HTTPS

内部使用，USSLAB版权

IPSec

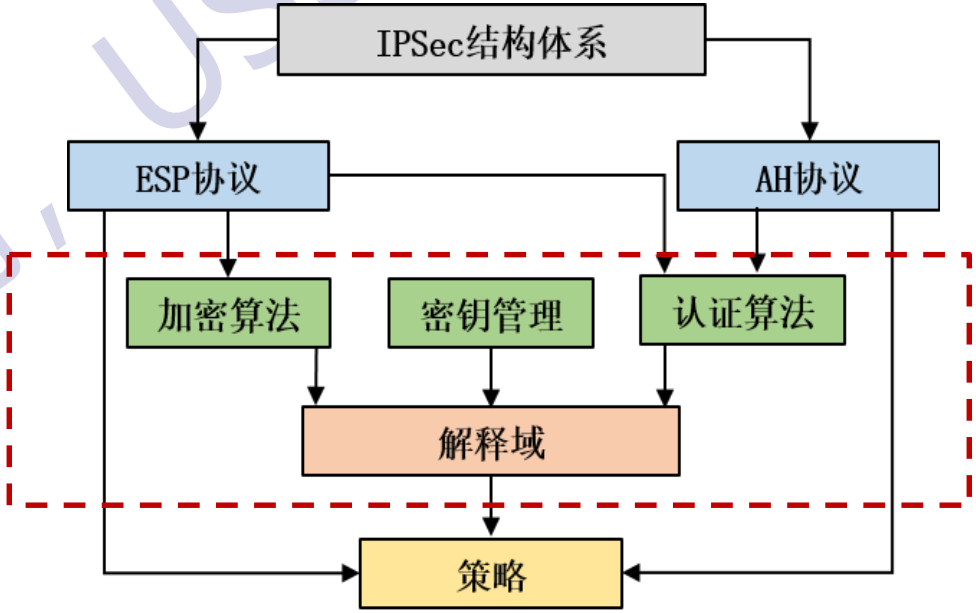
- **定义**：Internet Protocol Security（IPSec）是IETF制定的为保证在Internet上传送的数据进行分组加密和认证从而保护IP协议的网络传输协议族，是一些相互关联的协议的集合
- **目标**：为网络层流量提供灵活的安全服务，包括数据机密性、完整性、身份认证和防止重放攻击等
- 注意：IPSec不是具体一个协议，而是一个开放的协议族
- IPSec框架主要包括：
  - 认证头协议(AH: Authentication Header)
  - 封装安全载荷协议(ESP：Encapsulating Security Payload)
  - 安全关联协议(SA)：定义使用的加密和认证算法及其他参数

内部使用，USTC版权

IPSec架构

- **认证头(AH)协议**：在数据包中插入一个认证头，用于验证数据的来源和完整性，但不提供数据加密及防报文重放功能
- **封装安全载荷(ESP)协议**：将需要保护的用户数据进行加密后再封装到IP包中，保证数据完整性、真实性和私有性

解释域：规定了每个算法的参数要求和计算规则，及初始向量的计算规则等



IPSec结构体系示意图

内部使用，USST版权

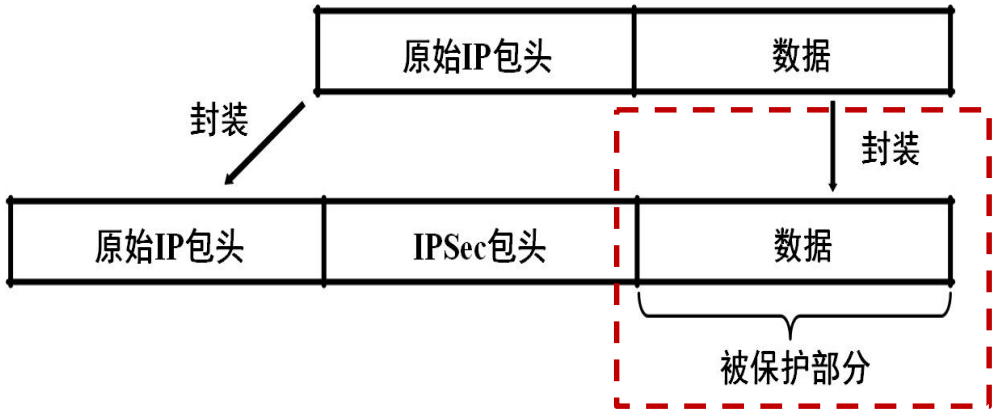
IPSec安全服务

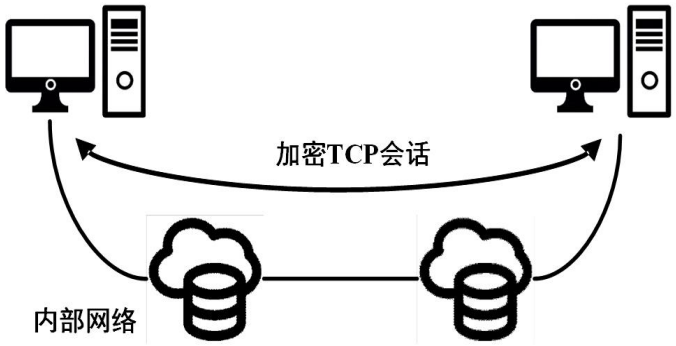
- **安全服务**
  - **数据机密性**：IPSec发送方在网络传输包前对包进行加密
  - **数据完整性**：IPSec接收方对发送方发送来的包检查，以确保数据在传输过程中没有被篡改
  - **数据源认证**：IPSec接收方对IPSec包的源地址进行认证，这项服务基于数据完整性服务
  - **反重放(Anti-Replay)**：IPSec接收方可检测并拒绝接收过时或重复的报文

内部使用，USSLAB版权

IPSec：传输模式（Transport mode）

- **定义**：传输模式下，IPSec协议会在IP报头和数据载荷之间插入一个**IPSec包头**。IPSec包头通过特定封装方式得到，如对原IP包头哈希得到，规定了IPSec协议号等信息
- **特点**：传输模式仅保护**数据包载荷**，数据负载部分被加密和/或认证；但是原始IP包头不加密
- 应用场景：常用于主机和主机之间端到端通信的数据保护

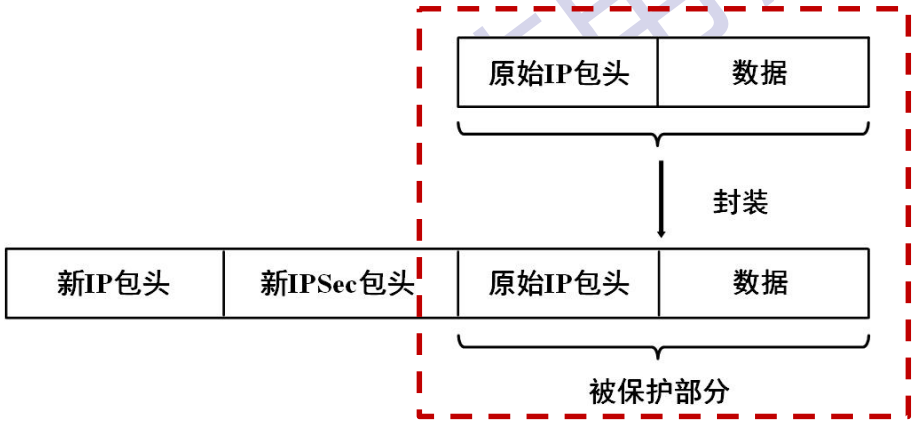




版权

IPSec：隧道模式（Tunnel mode）

- **定义**：在隧道模式下，原始IP分组被封装成一个**新的IP报文**，在原始IP包头以及新IP包头之间插入一个IPSec包头
- **特点**：原IP包头和负载同时被保护。原始IP地址被隐藏，利于保护端到端通信中**IP地址、数据、协议类型**等的安全性
- 应用场景：经常用于私网与私网之间通过公网进行通信，建立安全VPN通道；但是通信负载相对传输模式较高



仅用于UCSIA版权

SSL

SSL and TLS protocols

Protocol	Published	Status
SSL 1.0	Unpublished	Unpublished
SSL 2.0	1995	Deprecated in 2011 (RFC 6176)
SSL 3.0	1996	Deprecated in 2015 (RFC 7568)
TLS 1.0	1999	Deprecation planned in 2020[11]
TLS 1.1	2006	Deprecation planned in 2020[11]
TLS 1.2	2008	
TLS 1.3	2018	

- **定义**
  - SSL(Secure Sockets Layer)：安全套接字层
  - **目标**：SSL协议位于TCP/IP协议与各种应用层协议如FTP、Telnet等之间，为客户端和服务器之间建立安全的TCP连接，提供双向安全认证和数据机密性、完整性
  - 优点：协议本身和应用层协议相互独立
- **SSL后继者：TLS**
  - TLS：Transport Layer Security，即传输层安全性协议
  - TLS的框架与SSL基本相同，但其在OSI模型的应用层和TCP/IP模型的传输层上运行，与高层的应用层协议相互独立无耦合

内部使用，USSLAB

SSL

- **加密机制（回顾下密码学的知识）**

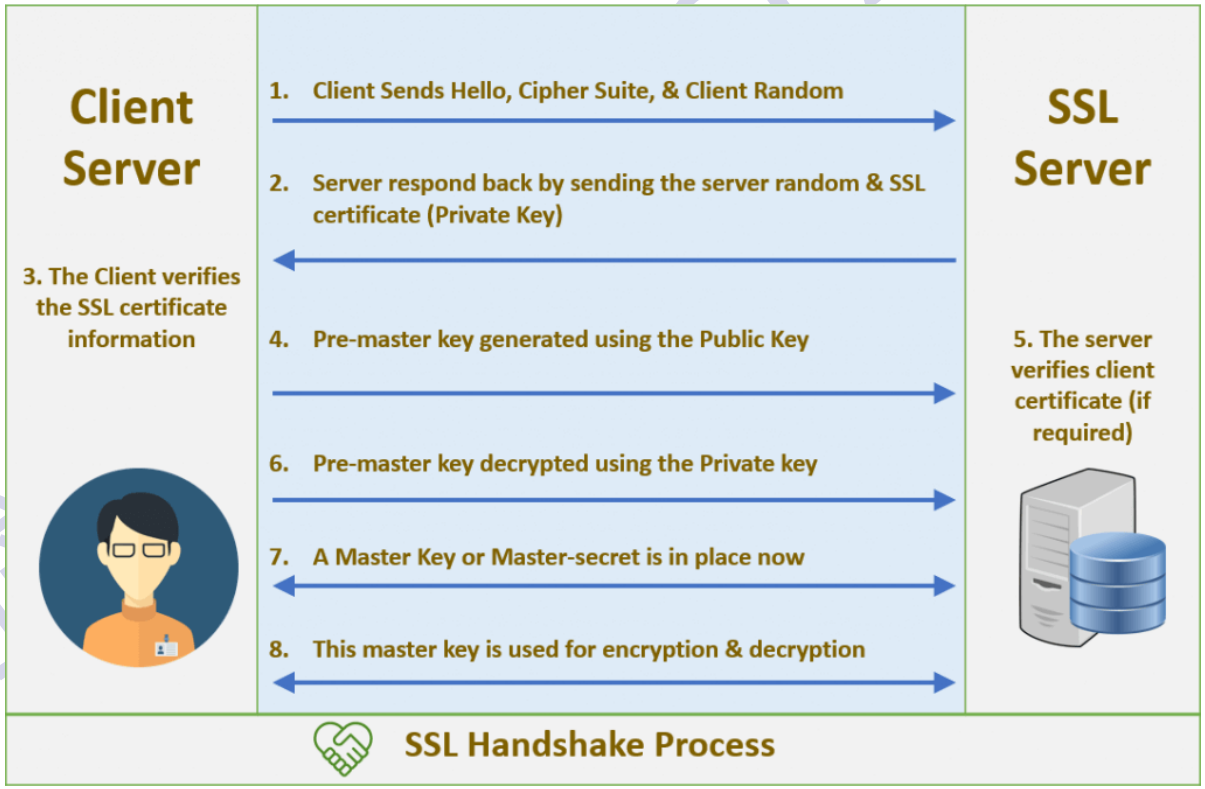
  SSL通信主要采用加密套件来保障安全，主要由四个部分组成：

  - **密钥交换**：用于客户端与服务器之间在握手的过程中认证。SSL通常使用非对称加密算法来生成会话密钥，常用算法如RSA
  - **加密算法**：对传输的数据进行加密传输，常用算法有DES 64, AES 128/256等
  - **会话校验(MAC)算法**：为了防止握手消息本身被窜改，常用算法包括MD5、SHA等

内部使用，USSLAB版权

SSL握手协议

- 握手协议是客户端和服务器用SSL连接通信时用的第一个子协议
- SSL允许服务器和客户端**相互验证，协商加密和MAC算法以及密钥**，用来保护在SSL记录中发送的数据机密性



握手协议流程图

内部资料 版权所有

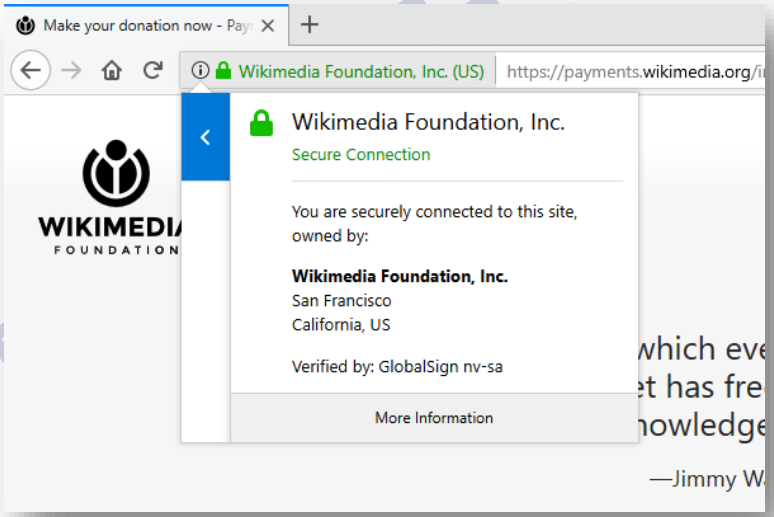
SSL握手过程

- **Step1: 客户端招手**
  - 支持的协议版本、加密方法、客户端生成的随机数
- **Step2: 服务器招手**
  - 回复使用的加密通信协议版本、加密方法以及服务器证书
- **Step3: 客户端验证服务器证书**
  - 客户端认证服务器发来的证书
- **Step4: 客户端发送证书与预先主密钥**
  - 客户端用服务器公钥生成预先主密钥，并与自身证书一起发给服务器
- **Step5-6: 服务器验证客户端证书**
  - 服务器验证客户端证书，并用自身私钥解密预先主密钥
- **Step7-8: 加密密钥确立并切换到加密模式**
  - 确立加密主密钥，并且双方使用相同的对称密钥进行加密的通信

内部使用，USSLAB版权

HTTPS

- **定义：**超文本安全传输协议(Hyper Text Transfer Protocol over Secure Socket Layer)，以SSL/TLS建立安全通道，加密数据
- HTTPS使用的主要目的是提供对网站服务器的身份认证，同时保护交换数据的隐私与完整性
  - 回顾：HTTP超文本传输协议，是一个基于请求与响应、无状态的应用层的协议，常基于TCP/IP协议传输数据



物联网管道安全防护机制

内部使用，USSLAB版权

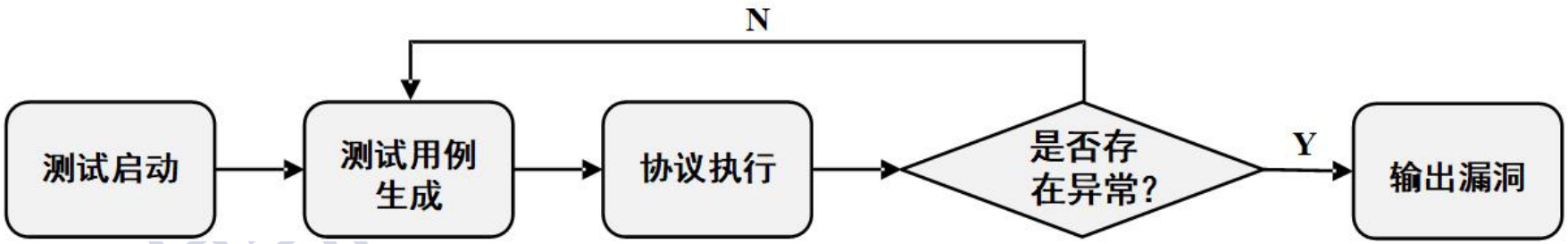
8.3.2 面向协议的安全检测

- **通信协议安全检测**
  - **协议差异性**:
    - 协议不存在统一标准
    - 各个服务提供商在不同的应用场景中会选择不同的通信协议
    - 通信协议的实际部署中采用不同的细节设计
  - **协议模糊性**:
    - 私有协议
    - 协议设计与实现的细节无法获取
- 因此，通信协议安全检测面临困难

内部使用，LISSLAB版权

8.3.2 面向协议的安全检测

- **基于模糊测试（Fuzzing）的协议安全检测技术**
  - **定义**：通过提供大量的随机输入或是可能导致协议出现问题的错误数据，观察被测目标的输出中是否存在异常结果来发现漏洞，类似于软件安全的模糊测试
  - **核心**：不同模糊测试的主要区别在于他们**测试用例构造**和**自动迭代的算法**不同



基于模糊测试的协议漏洞检测流程示意图

USSLAB版权

8.3.2 面向协议的安全检测

- **基于模糊测试（Fuzzing）的协议安全检测技术**
  - **执行步骤**：
    - 步骤一： 确定**测试目标**并启动模糊测试
    - 步骤二： 依据**用例自动化生成规则**去生成测试用例
    - 步骤三： 输入测试用例后，让其依据协议流程执行
    - 步骤四： **监视**协议执行过程中是否存在流程或输出等**异常**，若无异常则重新生成测试用例，若有，则进入下一步
    - 步骤五： 分析异常行为，**输出协议漏洞**

内部使用，USSLAB版权

“管”中窥“豹”

基于流量的安全监测

内部使用，USSLAB版权

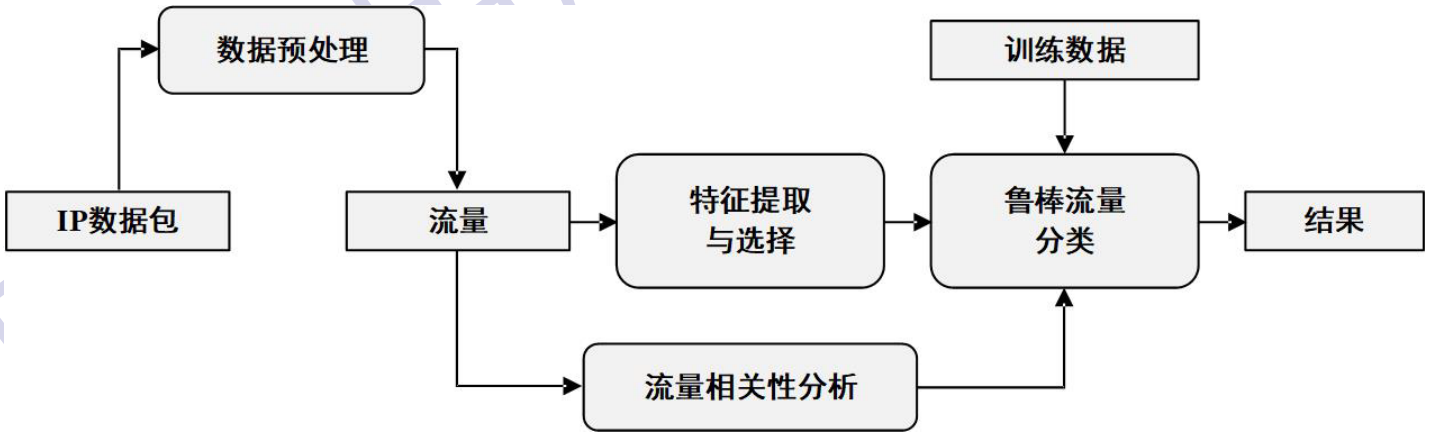
8.3.3 基于流量的安全监测

- **流量安全监测原理**
- **基于流量的恶意设备入侵检测**
- **流量监测在物联网中的应用案例**
  - 基于流量的说话者语种推断
  - 基于流量的隐藏无线摄像头检测
  - 基于流量的无人机入侵检测

内部使用/USSLAB版权

流量安全监测原理

- **定义**：通过对传输流量进行实时监测以实现网络安全管理的技术。其核心是流量分类，即根据通信管道中流量的特征对流量进行分类
- **目的**：设备辨识、入侵检测、服务质量(QoS)控制、合法拦截等
- **原理**：各类协议会对网络流量产生shaping（塑形）的作用，因此流量特性反映了协议类型甚至是物联网设备类别
- **过程**：
  - 数据捕获→构造流量→提取特征→流量表征→流量分类→安全分析



流量分类方法示意图

版权

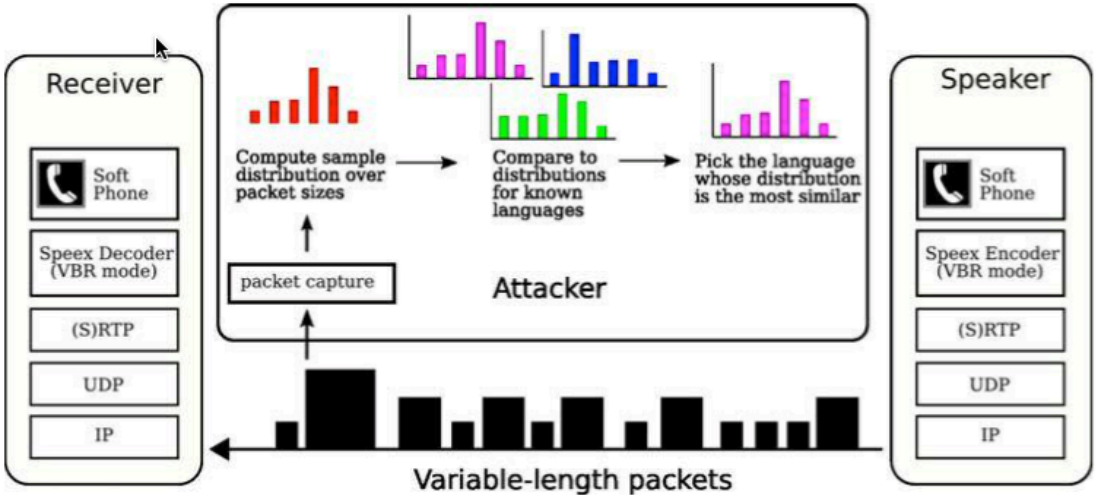
基于流量的入侵检测

- **定义**：通过监视与分析网络流量以实现对网络中异常或可疑行为检测的技术。一旦系统检测到网络流量特征出现异常或者较大变化时，会采取进一步的防护手段，如报警或丢弃特定流量包
- **核心**：基于流量分类区分正常流量与异常流量，包括
  - 基于已知特征的入侵检测技术
    - 技术点：检测目标流量签名是否属于已知漏洞利用
    - 适用范围：已知安全威胁与漏洞
  - 基于异常检测技术
    - 技术点：检测目标流量是否符合正常基准流量
    - 适用范围：未知安全威胁与漏洞

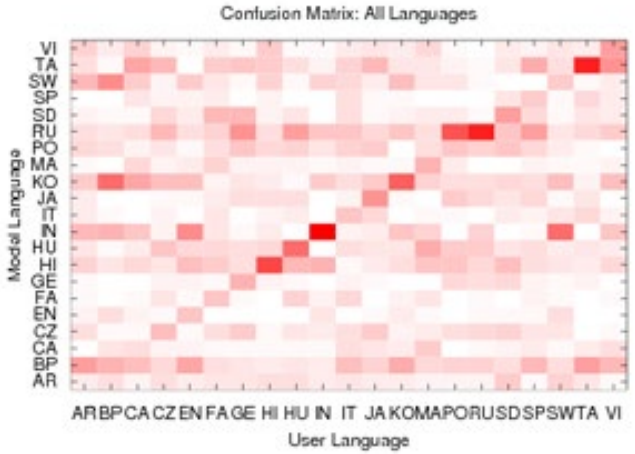
内部使用，USSLAB版权

应用案例一：说话人语种推测

- **VoIP电话语种推断**
  - VoIP通信中常用的两种协议SIP与RTP编码后的语音消息会和说话者的语种存在一定的相关性，因此攻击者可通过分析VoIP通信中流量（即使已经加密）的长度信息去推断说话者的语种



基于流量的说话者语种推断流程示意图

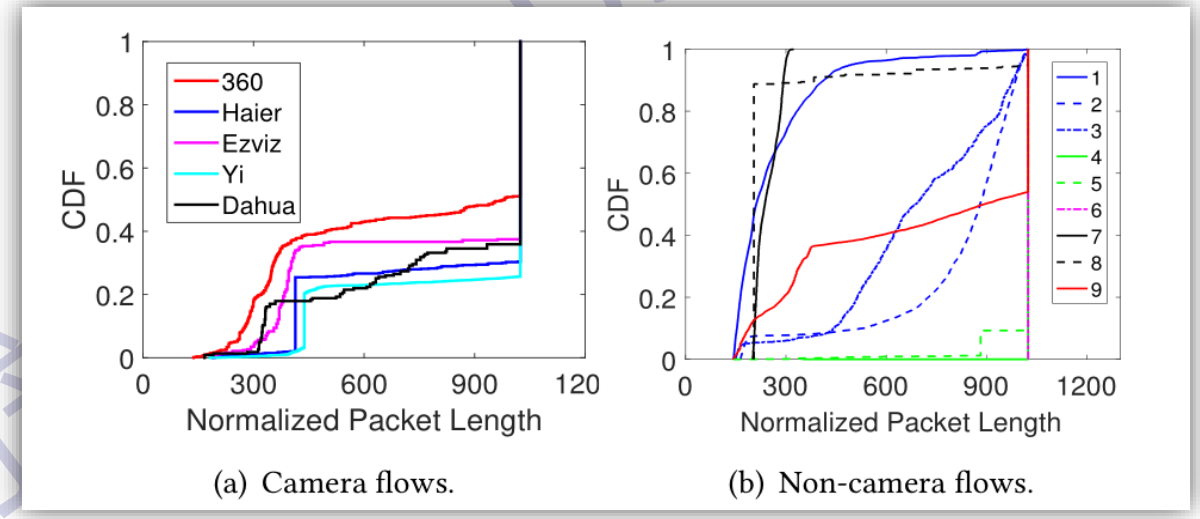


攻击效果

参考文献： Wright C V, Ballard L, Monrose F, et al. Language identification of encrypted VoIP traffic: Alejandra Roberto or Alice and Bob?[C]. USENIX Security, 2007.

应用案例二：恶意设备探测

- **隐藏无线摄像头检测**
  - DeWiCam：通过分析无线网络流量，检测无线网络摄像头，并判断无线网络摄像头是否处于当前房间
  - 工作原理：基于无线摄像头与其他网络应用具有不同**网络流量特征**，如数据包长度分布等



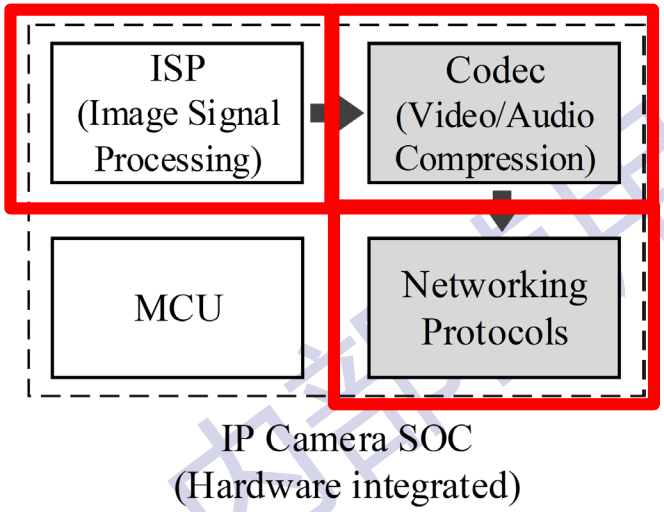
包长统计特征：摄像头数据流 vs. 非摄像头数据流

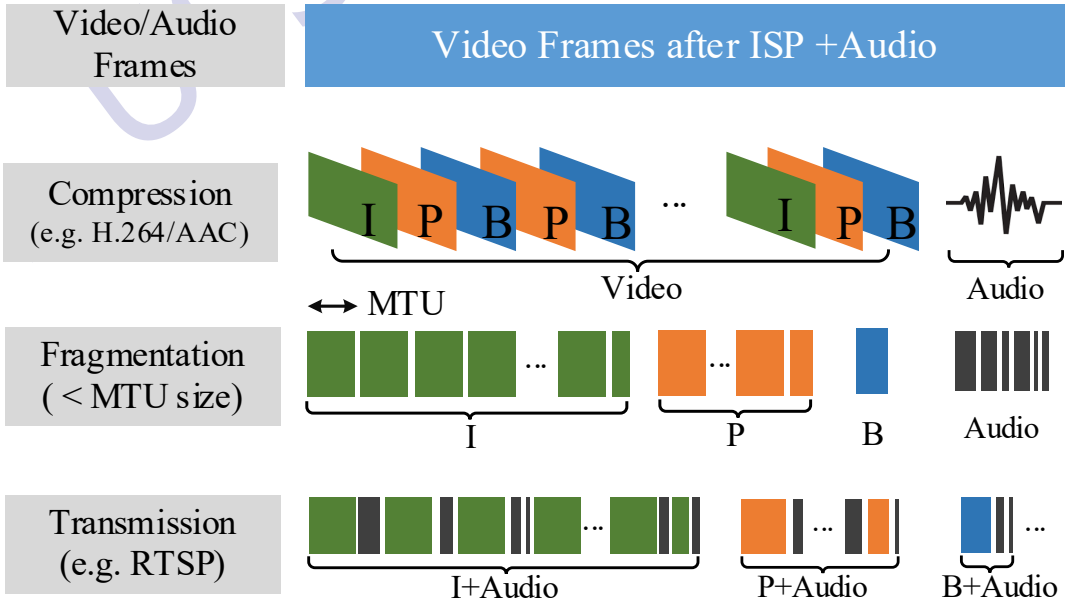
内部资料 USTC AD版权

参考文献： Xiaoyu Ji, etc., DeWiCam: Detecting Wireless Cameras via Smartphones, in ACM AsiaCCS 2018, Best Paper Award.

隐藏无线摄像头检测

- 为什么无线摄像头的流量不一样?
- 无线摄像头的SoC中ISP、编解码、传输协议等，会对其通信流量产生塑性，导致流量呈现特定特征

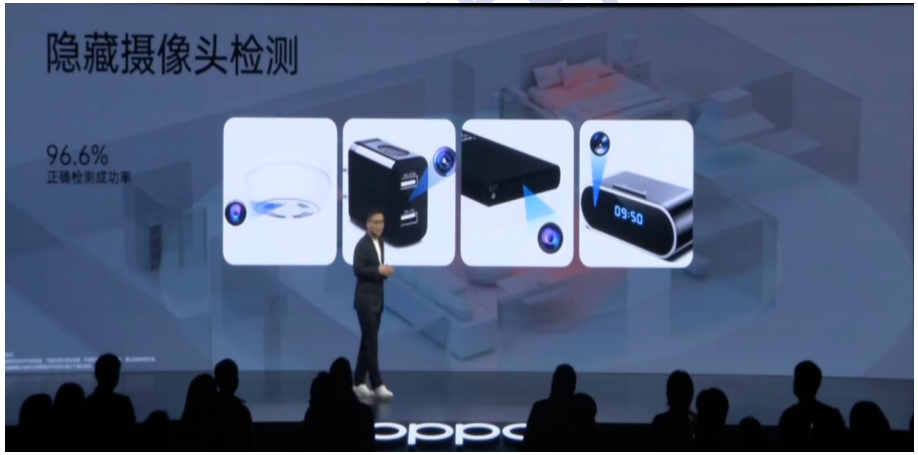


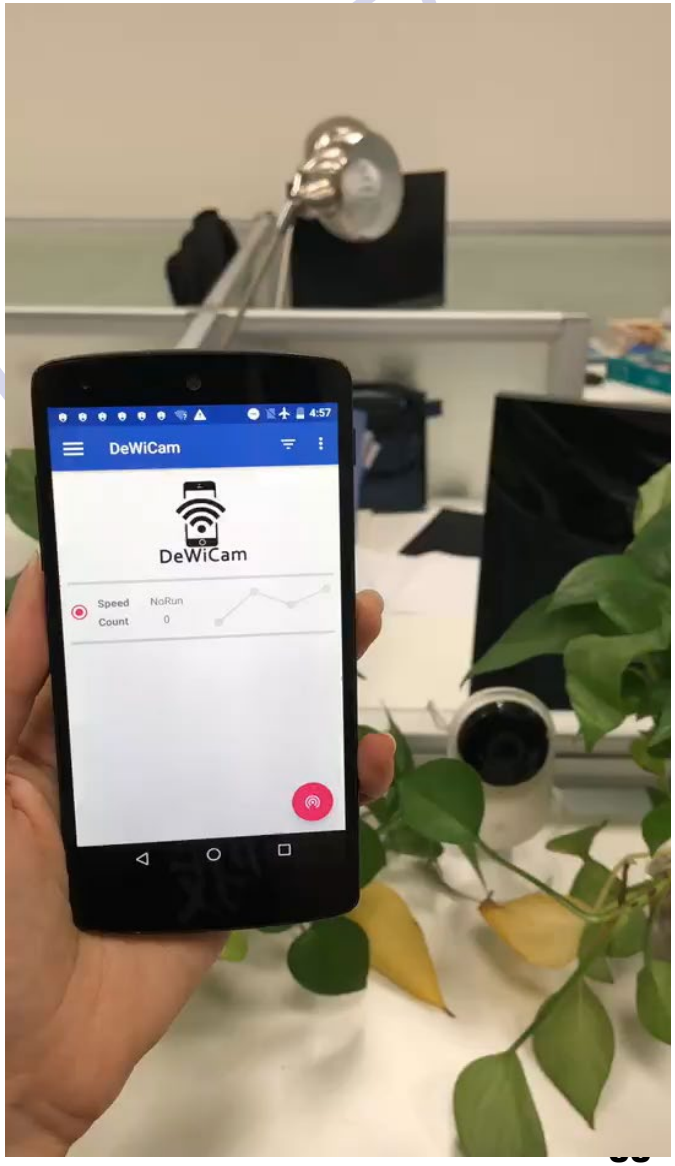


内部使用 CSSLAB版权

隐藏无线摄像头检测

- 视频演示





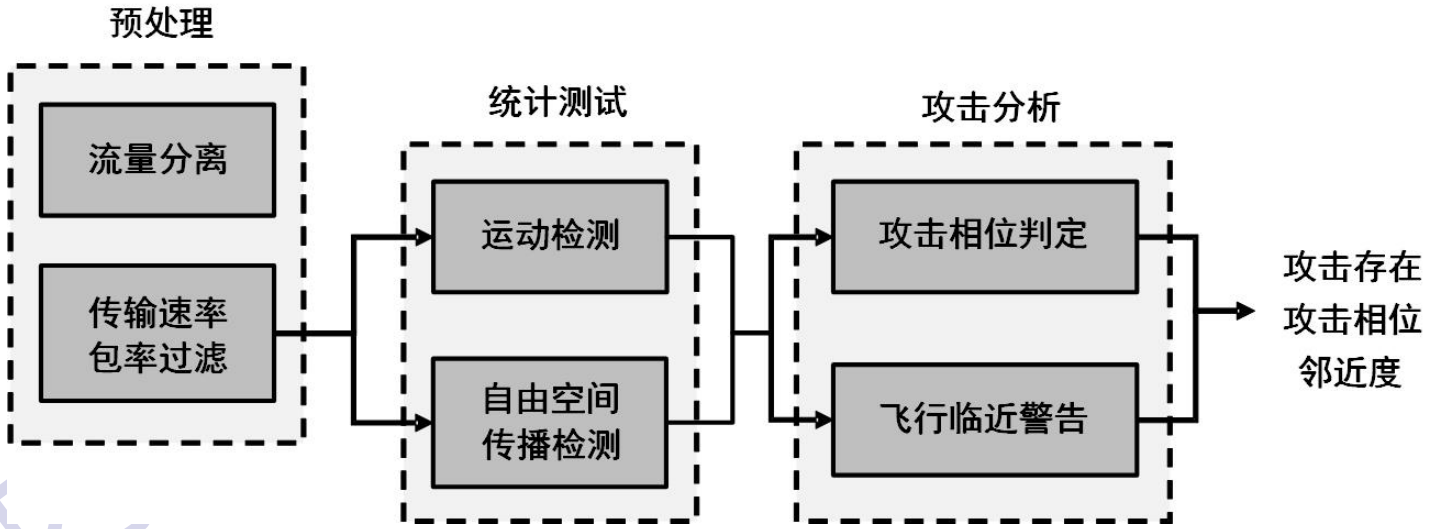
还可以做什么?

- **基于家庭物联网设备的用户隐私探测**
  - 摄像头、智能语音助手等、智能门锁等
- **How?**

内部使用，USSLAB版权

应用案例三：无人机探测

- **无人机入侵检测**
  - 通过无人机飞行时与控制器之间通讯的信号特征和流量信息，分析无人机的飞行动作与临近度，从而实现无人机的入侵检测。
  - 原理：无人机逼近、下降等过程流量以及RSSI特征不同。
  - 还可以结合DeWiCam的方法主动激发流量，如何？



基于流量的无人机入侵检测流程示意图

ISSLAB版权

参考文献： Birnbach S, Baker R, Martinovic I, et al. Wi-Fly?: Detecting Privacy Invasion Attacks by Consumer Drones.[C]. network and distributed system security symposium, 2017.

总结

- 了解物联网管道的定义
- 了解物联网管道物理链路层和应用层的代表通信协议，如5G、NB-IoT、MQTT、COAP及特点
- 掌握物联网管道在不同维度面临的安全威胁及其原因，可以对一类安全威胁进行分析
- 了解物联网协议安全的机制、代表性安全机制的应用及其工作机理
- 了解基于流量安全监测方法学术界的典型代表工作和应用场景

内部使用，USSLAB版权