无线与物联网安全基础（WYH Version）

概述安全目标(Security Objectives):**NIST CIA**三角

●**Confidentiality** 保密性 (not leaked to unauthorized parties)○Data confidentiality - 只有 authorized parties 可以访问 sensitive info ○Privacy - Individuals 可以控制他们的哪些信息可以被收集和储存，以及会向谁提供这些信息

●**Integrity** 完整性 (not modified) ○Data integrity - 信息和软件只会以预先决定和授权的方式被更改 ○System integrity - 系统以预期方式完成预期功能，并防止以未授权的方式被manipulate

●**Availability** 可用性 (keep online, available when needed) ○系统 work promptly且不会拒绝给 authorized users 服务

其他目标●**Authenticity**真实性，真实且能够被verified和受信任的属性○Entity authentication | 实体身份验证 - 验证实体就是它声称的实体○Data authentication | 数据身份验证 - 数据来自受信任的来源●**Access control**管理用户 / 进程对 resources 的访问权限●**Non-repudiability**不可否认性 不能否认对话或行为●**Accountability**可审计性，能够追踪所有 action 对应的entity:覆盖了 non-repudiability, intrusion detection (入侵检测), fault isolation (故障隔离) 等

实现:按具体要求选择防御机制，如密码学、访问控制、软件检查工具、垃圾spam过滤等

Types of Adversaries●Passive不干预，只监控、收集信息●Active更改系统资源或者影响系统操作●Insider是系统的合法部分或者在安全范围内，有权限访问内部数据●Outsider

Policies & Mechanisms●Policy 定义系统安全规则○policies组合非平凡，冲突可能成为漏洞●Mechanisms enforce policies●Security goals 与 policies 相关，prevention / detection / recovery

Building a System: -**Trust and Assumptions**是 安全所有方面的基础—假设policies正确说明所有安全需求—假设mechanisms实现policies

-**Specification**根据需求分析定义系统的功能-**Design**声明系统如何满足 specifications

-**Implementation**应当正确执行design

Security Design Principles: Economy of Mechanism, Open Design, Modularity, Layering, Complete Mediation, Fail-safe Defaults, Separation of Privilege, Least Privilege, Least Common Mechanism, Psychological Acceptability, Least Astonishment, Isolation, Encapsulation

无线网简介 **Network/Radio Challenges**-Gbps data rates with no errors-Energy efficiency-Scarce/bifurcated spectrum -Reliability and coverage -Heterogeneous networks -Seamless internetwork handoff **Device/SoC Challenges(New:SD Radio):**性能, 复杂度, 大小, Power, Cost, 高频/mmWave, 多天线, Multiradio Integration, Coexistance

Current/Next-Gen Wireless Systems

Current:4G Cellular Systems (LTE-Advanced), 4G Wireless LANs/WiFi (802.11ac), mmWave massive MIMO systems, Satellite Systems , Bluetooth, Zigbee, **Emerging**: 5G Cellular and Advanced WiFi Systems, Ad/hoc and Cognitive Radio Networks, Energy-Harvesting Systems, Chemical/Molecular

Cellular Systems: Reuse channels to maximize capacity• Geographic region divided into cells

• Freq/time slots/codes/space reused in different cells(reuse 1 common).• Interference between cells using same channel: interference mitigation key• Base stations coordinate handoff and control functions• Shrinking cell size increases capacity, as well as complexity, handoff, …

5G Cellular • Much higher data rates than 4G/LTE (peak 1.3 Gbps)• 4G systems has 100 Mbps peak rates• Greater spectral efficiency (bits/s/Hz)

• Massive MIMO, Device to Device, Internet of Things• Introducing new spectrum for communication• mmWave band for faster communication• Low packet latency (<1ms)

• Cloud and edge computing for networking based on SDN/NFV• Feasible to support real-time and live-streaming applications

Wi-Fi : 802.11b (Old – 1990s)

• Standard for 2.4GHz ISM band (80 MHz)

• Direct sequence spread spectrum (DSSS)

• Speeds of 11 Mbps, approx. 500 ft range

802.11a/g (Middle Age– mid-late 1990s)

• Standard for 5GHz band (300 MHz)/also 2.4GHz • OFDM in 20 MHz with adaptive rate/codes • Speeds of 54 Mbps, approx. 100-200 ft range

802.11n/ac [WiFi4/5] (Current)

• Standard in 2.4 GHz and 5 GHz band

• Adaptive OFDM /MIMO in 20/40/80/160 MHz

• Antennas: 2-4, up to 8

• Speeds up to 600Mbps/6.9 Gbps, approx. 200 ft range • Other advances in packetization, antenna use, MU-MIMO

802.11ax [WiFi 6] (Latest)

• Standard in 2.4 GHz and 5 GHz band • Most characteristics are similar to WiFi 5 • Speeds up to 9.6 Gbps, approx. 200 ft range • Other advances: MU-MIMO in both upload and download links, OFDM

wifi表现差- Carrier Sense Multiple Access:if another WiFi signal detected, random backoff

- Collision Detection: if collision detected, resend

WiFi标准缺乏良好的机制来减轻干扰，尤其是在密集的AP部署中•20世纪70年代的多址协议（CSMA/CD）•静态信道分配、功率水平，和载波感知阈值•在这种部署中，WiFi系统表现出较差的频谱重用以及AP和客户端之间的严重竞争•结果是吞吐量低，用户体验差•MU-MIMO将帮助每个AP，但不会干扰AP

毫米波mmWave Massive大规模MIMO

毫米波具有较大的非单调路径损耗•信道模型理解不足•毫米波天线较小：非常适合大规模MIMO•瓶颈：信道估计和系统复杂性•非相干设计具有重要前景

satellite system 卫星系统

覆盖非常大的区域•不同的轨道高度•GEO（39000公里）与LEO（2000公里）•针对单向传输进行了优化•无线电（XM、Sirius）和电影（SatTV、DVB/S）广播•大多数双向系统破产•全球定位系统（GPS）无处不在•用于精确确定位的卫星信号•在手机、PDA和导航设备中很受欢迎•最近，卫星通信智能手机。

蓝牙Bluetooth

蓝牙•电缆更换射频技术（低成本）•短距离（10米，可扩展至100米）•2.4 GHz频带（拥挤）•1个数据（700 Kbps）和3个语音通道，最高可达3 Mbps•电信、PC和消费电子公司广泛支持•除电缆更换外，几乎没有其他应用

IEEE 802.15.4/ZigBee Radios

低速率低功耗低成本安全无线电•与WiFi和蓝牙互补•频带：784、868、915 MHz、2.4 GHz •低频，低功耗：20Kbps、40Kbps、250 Kbps•近距离，短时延：10-100m line-of-sight•支持大型网状网络或星形集群•支持低延迟设备•CSMA-CA信道接入•应用：电灯开关、电表、交通管理，以及其他低功率传感器。

Spectrum Regulation • Spectrum a scarce public resource, hence allocated• Spectral allocation in US controlled by FCC (commercial) or OSM (defense) • FCC auctions spectral blocks for set applications. • Some spectrum set aside for universal use • Worldwide spectrum controlled by ITU-R • Regulation is a necessary evil. Innovations in regulation being considered worldwide in multiple cognitive radio paradigms

Emerging Systems • Ad hoc/mesh wireless networks • Cognitive radio networks • Wireless sensor networks • Energy-constrained radios • Distributed control networks • Applications of Communications in Health, Bio-medicine, and Neuroscience

Ad-Hoc Networks • Peer-to-peer communications • No backbone infrastructure or centralized control • Routing can be multihop • Topology is dynamic • Fully connected with different link SINRs • Open questions -Fundamental capacity region -Resource allocation (power, rate, spectrum, etc.) -Routing

Cognitive Radios • Cognitive radios support new users in existing crowded spectrum without degrading licensed users -Utilize advanced communication and DSP techniques -Coupled with novel spectrum allocation policies

• Multiple paradigms- (MIMO) Underlay (interference below a threshold) -Interweave finds/uses unused time/freq/space slots -Overlay (overhears/relays primary message while cancelling interference it causes to cognitive receiver)

Wireless Sensor Networks

§ Energy (transmit and processing) is the driving constraint

§ Data flows to centralized location (joint compression)

§ Low per-node rates but tens to thousands of nodes

§ Intelligence is in the network rather than in the devices

Where should energy come from? • Batteries and traditional charging mechanisms• Well-understood devices and systems • **Wireless-power transfer** • Poorly understood, especially at large distances and with high efficiency • Communication with Energy Harvesting Radios • Intermittent and random energy arrivals • **Communication becomes energy-dependent** • Can combine information and energy transmission • New principles for radio and network design needed

IoT the Internet of Things

定义：original Auto-ID Center founded in 1999 MIT提出，A network of objects, often a self-configuring无线网.三个核心特点object equalization, ad-hoc terminal interconnection, pervasive(普遍的) service intellectualization

Layers:●Sensing Layer(collection,基础,触手tentacle) ○Fuse physical & cyber worlds

○大量的 information generating devices，如 RFID, wireless sensors, 智能电子产品 ○IoT 重要特征：Diversification of information generation methods ●**Network Layer**(transmission) ○Strong linking function, efficiently, stably, timely, securely 在上下层中传输信息 有Mobile Network(3G,4G), Low speed access(Bluetooth, Zigbee), Wireless broadband(Wi-Fi, WiMAX), Emerging wireless(visible light NB-IoT)

●**Management Layer**(processing)

○The source of the wisdom of IoT ○Integrate & utilize数据 ○Storage, search and retrieval (检索), utilization, safety and privacy, Abuse prevention

●**Application Layer**(diversification, large-scale, and industrialization) ○Traditional Internet: data-centric -> human-centric, IoT applications are based on "things" of the physical world

○Value in IoT data processing is cloud

Main Components●Networking●Operating Systems●Hardware

○**Sensor:根据** processor 和 sensor 的 interaction mode即 analog signals 还是 digital signals选择是否需要 external analog-to-digital converter 以及 additional calibration (校准) technology

○**Microprocessor** ■负责计算的核心

■Feature: deeply integrated 集成mem, flash mem, analog-to-digital converter, digital IO 等

■关键性能：能耗, wake-up time, power supply voltage(long-time work),计算速度, mem size

○**Communication Chip** ■通常耗能最多，发送接收消耗能量差不多■重要指标Transmission distance,power大接收敏感度和传输距离大■CC1000, CC2420(IEEE 820.15.4)

○**Energy Supply Service** ■Battery: easy to deploy, capacity cannot be fully utilized(电压变化和环境导致)■Renewable energy (e.g. solar energy)

●Rechargeble batteries，less self-discharge => higher power utilization,充电效率低且次数有限

●Super capacitor 超级电容，higher charging efficiency, stable, 充电次数多,不易受外部影响

Main Characteristic

●Large-scale networking terminal ●Pervasive (普遍的) sensing●Interconnection of heterogeneous equipment 异构设备互联 ●Intelligent management and processing智能处理大规模数据 ●Application service chaining 全环节覆盖

Development Trend●Broader connectivity

●More thorough sensing●Deeper intelligence

Danger Rankings:●DISASTROUS(Security Systems,Energy Meters): Cause irreversible damage ●DISRUPTIVE(Smart Video Conferencing Systems,Connected Printers,VoIP Phones):Disrupt corporate and operational processes ●DAMAGING(Smart Fridges,Smart Lightbulbs):Enable information stealing

IP-Connected Security Systems ●Many use proprietary radio frequency technology that lack authentication and encryption. ●Attackers can form radio signals to send false triggers and access system controls.●User compute capability to exfiltrate large amounts of data.●Disable camera to allow physical break in.●Hijack camera to spy on employees usage of computers, passwords, applications ●Use as a launching point for DDoS attacks.

IP-Connected Infrastructure: Climate Control & Energy Meters – HVAC systems provide an avenue for hackers to gain network access ●Attackers can force critical rooms (for example, server rooms) to overheat and cause physical damage. ●IP-connected infrastructure uses wireless technology that is often accessible to anyone within range.

Smart Video Conference Systems – These often only require the click of a button for users to share screens – and for hackers to commandeer it. ●Attackers have full access to all software, memory and hardware, exposing the microphone, camera and stored credentials.●Smart TVs connect to the local network over IP and also serve as a pivot point for hackers to gain full network access.

Connected Printers – Nearly all printers are networked over IP - a welcome mat to hackers to infiltrate the enterprise ●Without physical access, hackers can comprise printers to siphon private documents printed through them.●Many exploitable issues are not resolvable without updates to firmware or an intrusion detection system.

VoIP Phones– VoIP phones leverage the network for many sophisticated features that makes communication easy, not only for employees – but also malicious hackers.●Hackers can exploit configuration settings to evade authentication and then update the phone, allowing them to listen to phone conversations or make calls.

Smart Lightbulbs– Smart lightbulbs operate on Wi-Fi and proprietary mesh networks which can be hacked.●Mesh network communication channel can be sniffed by attackers. ●Password-protected Wi-Fi credentials without being on the network, allowing them to gain access to other systems and devices in the network.

Security Analysis of IoT

• 1. Information leakage caused by IoT tag scanning

• 2. Malicious attacks on the radio frequency of the IoT

• 3. Tag users may be tracked and located

• 4. Insecure factors of the IoT may spread through the Internet

• 5. The encryption mechanism of the IoT needs to be improved

• 6. The security risks of the IoT will aggravate the security threats of industrial control networks

Security Characteristics of IoT

(1) Some existing security solutions for sensor networks, the Internet,mobile networks, secure multi-party computing, cloud computing, etc. can be partially used in the IoT environment, but other parts may no longer be applicable

• First, the number of sensor networks corresponding to the IoT and the scale of terminal objects are much larger than those of a single sensor network

• Second, the processing capabilities of the terminal equipment or devices connected to the IoT will be very different, and they need to interact with each other

• Third, the amount of data processed by the IoT will be much larger than the current Internet and mobile networks

(2) Even if the security of the perception control layer, the data transmission layer, and the intelligent processing layer are separately guaranteed, the security of the IoT cannot be guaranteed

• This is because the IoT is a large-scale system integrating several layers, and many security problems from system integration; • The data sharing of the IoT puts forward higher requirements for security; • The application of the IoT will put forward new requirements for security. For example, privacy protection is not a single-level security requirement, but it is an indispensable security requirement for IoT application systems.

• In view of the above reasons, the development of the IoT needs to re-plan and formulate a sustainable development security architecture, so that the security protection measures of the IoT can be continuously improved during the development and application of the IoT.

Security Demands of IoT

•Regardless of the diversification of the sources and channels of security threats and the generalization of sources, we can summarize the security requirements of the IoT into the following aspects: IoT access security, IoT communication security, IoT data privacy security and IoT computing system security and other aspects.

• **IoT access security**: In access security, the access security of the sensing layer is the key point. First, a sensing node cannot be accessed by a node or system that has not been authenticated and authorized, which involves the security requirements of the sensing node's trust management, identity authentication, and access control. Therefore, in addition to being subject to the same security threats as existing networks, sensor networks may also be subject to security threats such as attacks from malicious nodes, monitoring or destruction of transmitted data, and poor data consistency

• **IoT communication security**

• Due to the exponential growth of communication terminals in the IoT and the limited carrying capacity of existing communication networks, when a large number of network terminal nodes access the existing network, it will bring more security threats to the communication network.

- First, the access of a large number of terminal nodes will definitely bring about network congestion, and network congestion will give attackers an opportunity to take advantage of, thereby causing a denial of service attack on the server;

- Second, due to the small amount of data transmitted by devices in the IoT, complex encryption algorithms are generally not used to protect data, which may cause data to be attacked and destroyed during transmission;

- Finally, the integration of the sensing layer and the network layer will also bring some security problems.

-In addition, in practical applications, a large number of wireless transmission technologies are used, and most of the equipment is in an unattended state, making information security not guaranteed and easy to be stolen and maliciously tracked. The leakage of private information and malicious tracking have brought great security risks to users

• **IoT data privacy security**

• With the development and popularization of the IoT, data has exploded. Individuals and companies are pursuing higher computing performance, and software and hardware maintenance costs are increasing, making the equipment of individuals and companies no longer able to meet their needs. Therefore, cloud computing, grid computing, pervasive computing, cloud computing, etc. have emerged. Although these new computing models solve the equipment needs of individuals and businesses, they also risk losing direct control over their data.

• Therefore, the security and privacy protection technology for outsourced data in data processing is particularly important. Since traditional encryption algorithms perform poorly in the calculation and retrieval of ciphertexts, it is very necessary to study encryption algorithms that can be retrieved and operated in the ciphertext state.

IoT computing system security

• The application field of the IoT is very wide, and it has penetrated into all walks of life in real life. Due to the particularity of the IoT itself, its application security problems exist in addition to the common security threats in existing network applications, and there are more special problems of application security.

• In IoT applications, in addition to the security requirements of traditional networks (such as authentication, authorization, auditing, etc.), it also includes the privacy and security requirements and service quality requirements of IoT application data, and the security requirements of application deployment.

IoT Security Architecture

1. IoT sensing security

• The sensing node access and user access of the IoT are inseparable from information security technologies such as identity authentication and access control.

2. IoT data security

• The confidentiality of the IoT requires information to be used only by authorized users and not to be leaked.

• Commonly used security technologies include anti-detection, anti-radiation, information encryption, and physical secrecy.

3. IoT security control

• The security control of the IoT requires information to be non-repudiation, that is, it is impossible for all participants in the information interaction process to deny the characteristics of the operations and promises that have been completed.

4. IoT security audit

• The security audit of IoT requires the confidentiality and integrity of the IoT. Confidentiality requires that information cannot be leaked to unauthorized users; integrity requires that information not be damaged by various reasons.

5. The privacy and security of the IoT

• In addition to the above security indicators, privacy issues need to be considered in the IoT

无线基础 通信系统:①移动语音电话②接入点覆盖范围大(几百-几万)③中/低传输速率(几十kbps-几十mbps)④GSM/UMTS/LTE/5G;无线局域网(WLAN):①扩展无线以太网②几十米到几百米③几十mbps-几百.④IEEE 802.11b, a, g, n, ac;短距离无线通信:②数十米⑤低功耗;④Bluetooth/ZigBee/NFC卫星系统;广播系统;固定无线接入系统

标准**:**①3GPP:GSM/UMTS/LTE②IEEE:WiFi/ZigB /Bluetooth/WiMAX③IETF:MobileIP/TCP/AODV模拟：连续时间连续值 数字：离散时间离散值(有限) 模拟信号结构复杂，抗干扰能力差，而数字信号结构简单，抗干扰能力强，所以模拟通信必然被数字通信所取代

模拟信号-采样-量化-编码-数字信号

电磁波所有可能的频率(无限个)的集合称为电磁频谱 • 从3 kHz到300 GHz的频率子集称为无线频谱或射频(RF)(更高是光) • 有效带宽(或带宽)：包含信号主要能量的频率的宽度

无线电频段分配• 授权频段：由政府机构(FCC)授权（移动蜂窝网络）-特定频道，每个区域仅一个用户-“窄带”-信道宽度为6.25、12.5或25KHz • 免授权频段: 工业，科学和医疗ISM（WLAN，lecture1 2的）-必须是宽带 (5MHz)

- 限制对其他用户的干扰

基带**(**基本频带**):**零频附近(直流到几百KHz)的带宽;基带信号是最“基础”的信号,生活中更多指手机基带芯片/电路/基站的基带处理单元(BBU)

射频 无线电频率 低于100kHz的电磁波会被地表吸收,不能形成有效的传输.高于100kHz的电磁波可以在空气中传播，并经大气层外缘的电离层反射，形成远距离传输能力。

• 调制技术:线性调制/恒包络调制/混合调制

• 模拟调制:将基带信号的中心频率调制至无线电载波;①方法:调幅(AM)/调频/调相(连续)

• 数字调制**(**移动键控**)**:数字数据转换为模拟信号(基带);①幅移ASK:简单,带宽要求低/容易受干扰,通过光纤传输数据②频移FSK:不容易出错/需要更大的带宽/用于高频3-30MHz 数字FSK简单,抗噪声衰减,中低速③相移PSK:更复杂/抗干扰④BPSK二进制相移键控:0是正弦/1是倒正弦波/鲁棒/用于卫星⑤QPSK正交相移键控:2位编码一个码元->确定正弦波的偏移/在衰落信道中也好/抗干扰/中高速传输⑥QAM正交幅度调制:幅度+相位调制/ QAM星座图容纳更多星座点/更高频带利用率 2^n个离散级,n=2即QPSK

编码和解码**:**①信源编码:数据压缩②信道编码:↑链路性能/抗干扰和衰落/纠错/误码判断

信道编码**:**①按纠错检错能力:检错码/纠错码/纠删码②按检验关系:线性码/非线性码③按约束关系:分组码/卷积码(纠错能力强/可纠随机差错|突发差错)/Turbo编码(伪随机/性能好)

容量:传输数据的最大速率bps(802.11首要目标)

主要取决于分配的带宽,可通过用户数量及数据速率粗略衡量,特定服务的带宽固定,但用户数量和数据传输率不固定

无噪声信道下的容量：**Nyquist** 公式：

具有多级信号/编码 $C = 2B\log_2 M$, M = 离散信号或电压电平的数量。

信噪比**SNR**，接收测量,高信噪比高质量信号

$$(SNR)_{dB} = 10\log_{10}\frac{\text{信号功率}}{\text{噪声功率}}$$

信噪比决定了可达到理论数据传输速率上限

$$C = B\log\left(1 + \frac{S}{N}\right)$$

应对环境干扰:物理层设计(调制(扩频/OFDM) /多路复用/天线阵列(MIMO/波束成形))/纠错码FEC/载波频率/信号功率

信号传播模式:①地波传播:频率最高为2 MHz ,沿地球轮廓传播,如:AM广播②天波传播:电离层和地球表面反射的信号,可以传播数千公里,频率: 2-30MHz,业余无线电/军事通信③视线传播:发射和接收天线必须在视线范围内，频率: 30MHz以上，电视/卫星/光学通讯

影响无线信号传播的四大效应:①多径效应(瑞利分布,时空频快衰落)②阴影效应(对数正态,慢衰落)③远近效应(CDMA网络明显,功率控制技术平衡)④多普勒效应(接收者v 波长λ波的到达角度有关)无线信号的三大损耗:多径损耗/传播损耗/穿透损耗:频率越高,损耗越大

快衰落:短距离移动导致的小规模衰落,移动半波长发生,相位随机噪声;慢衰落:大规模衰落,移动距离>波长;

抗衰落技术**:**①分集技术(将在接收端分散接收到的几个衰落情况不同（相互统计独立）的合成信号，再以一定的方式将它们合 并集中，使总接收信号的信噪比得到改善，衰落的影响减小):显分集(采用了多种设备在不同空间、不同频率和不同极化方向接收合并而来实现的分集)隐分集(利用信号设计技术将分集作用隐含在被传输的信号之中，称为隐分集)(信道交织:误码离散化/跳频/扩频)②信道编码技术(检错纠错)③均衡技术(消除码间干扰)

多路复用:①频分FDM:优点:无需动态协调/也适用于模拟信号;缺点:流量分布不均会浪费带宽/不灵活/需要保护间隔②时分TDM:优点:任何时候介质中只有一个载波/大用户条件下保证高吞吐量;缺点:需要精准同步③时分频分复用GSM:优点:放置频率选择性干扰/更好的防窃听保护;缺点:需要精确的协调④码分CDM:用于蜂窝电话系统的某些部分以及某些卫星通信;每个发送者被分配唯一二进制代码;优点:带宽高效/无需协调同步/良好的抗干扰和防窃听;缺点:更复杂的信号再生 码分多址CDMA

正交频分复用**OFDM**:①难点:频率选择性衰落/码间串扰②解决方案:多载波调制③允许重叠载波的原因:子载波是正交的④优点:降低码间串扰ISI/干扰抑制 扩频:特殊编码扩展宽带①优点:不受噪音干扰/带宽共享/防窃听

跳频扩频**FHSS**:①信号以固定的间隔从以恶搞频率跳到另一个频率②每个连续间隔选择新的载波频率③优点:对窄带干扰具有很高的抵抗力;对窄带窃听者来说信号表现为背景噪音④缺点:同步问题 直接序列扩频**DSSS**: ①使用扩展码将信号扩展到更宽频带(异或)②优点:减少频率选择性衰弱;蜂窝网络中基站可选择相同频率范围③缺点:精准功率控制,抗干扰弱

FHSS vs. DSSS

吞吐量：直接序列扩频(DSSS)系统可以连续传输 (PSK)，跳频扩频(FHSS)系统花一些时间来重新同步和跳频 (FSK)

抗干扰：直接序列扩频(DSSS)系统会受到使用相同频段的其他直接序列扩频(DSSS)系统产生的高水平干扰的影响，如果干扰高于一定的限制，DS将停止工作; 而FS可以使用不受影响的频率并继续工作

多径容忍度：直接序列扩频(DSSS)系统使用非常高的传输速率 => 非常短的码元，因此对回声和延迟特别敏感

单双工方式:①单工:单方向传输,广播②半双工:同一时间单方向,对讲机③全双工:同时双向,手机④时分双工TDD，频分双工FDD

天线：把传输线上的导行波变成电磁波或相反;波束有主瓣和旁瓣

基站:①O型站点:全向性小区/全向天线②S型站点:扇区性小区/3扇区型/定向天线③宏基站/微基站50-200/皮基站20-50/飞基站10-20m

MAC层 多址**(**多用户**)**接入信道:① 每个节点通过共享的通道与AP/BS进行通信②一个节点的传输可以被其他节点所接收 多址接入协议:①决定节点如何共享信道的分布式算法②关于信道共享的协商本身要求对信道的使用

信道分割协议:①频分多址FDMA:多频段②时分多址TDMA:轮流访问/固定时间槽/在低负载时效率低下③码分多址CDMA:独立地址码,主要用于无线广播信道(蜂窝网络/卫星)共享频段

信道分割的控制:①中心化:IEEE802.1 1架构/蜂窝网络/电缆调制解调器②分布式共识协议:节点广播要使用的时间频率，在一个单独的控制信道，通常用于ad-hoc的网络/MANET

随机访问协议:①ALOHA:18%②时隙ALOHA:优点:单个活动结点能以信道全部速率连续传输/高度去中心化:只有结点的时间槽需要保持同步

③载波监听多路访问CSMA：改进: 在传输数据包前监听信道。仅当没有传输的情况下才开始传输

CSMA 碰撞：由非零的传播延迟导致，即使发生了碰撞，节点仍继续传输，导致信道容量的完全浪费，碰撞的概率随着传播延迟而增加

④CSMA/CD:改进: 如果检测到碰撞，停止正在进行的传输

碰撞检测（CD: Collision Detection）

检测碰撞的发生：每个帧的时间应至少是检测碰撞时间的两倍 (2 ·最大传播延迟) 如果发生碰撞，所有的节点都会退后，等待一个随机的时间

问题: 碰撞检测（"边听边说"）在无线网络中不起作用，碰撞的成本很高（只有在发送了整个数据包而没有收到ack后才会被发现 ）

CSMA/CA避免:改进: 当检测到介质空闲时，在传输之前，通过启动（随机）回退（backoff）定时器，将碰撞的机会降到最低。

核心思路:使用空闲信道评估（**Clear Channel Assessment, CCA**）进行载波监听载波存在 ==> 不传输 (延迟或回退)

没有载波 ==> 或许可以传输（等待DIFS: Distributed Inter-frame Spacing）碰撞避免（**Collision avoidance, CA**）

使用帧间间隙（Inter-Frame Spaces, IFS)随机回退的机制

有可能实施不同的固定优先级别（用于QoS）

当检测到介质空闲时,在传输之前,通过启动随机回退计时器,将碰撞的机会降到最低;核心思路:①使用空闲信道评估CCA进行载波监听:若载波存在,不传输(延迟或回退);没有载波;等待DIFS时间后传输;②使用碰撞避免CA③算法流程:(发送方)如果程序DIFS时间检测到信道空闲,发送整个数据帧;如果检测到信道繁忙:开始随机回退一段时间,定时器到点后发送数据;如果没有ACK,增加回退时间(接收方)如果成功收到数据帧,SIFS后返回ACK

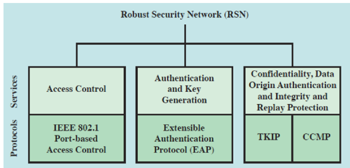
带有**RTS/CTS**的**CSMA/CA**:1. 发送方发送一个请求发送RTS，表明它想使用多长时间的介质 2. 接收方以 CTS作为回复，呼应预期的传输时间(一定程度上有助于解决隐藏的终端问题) 3. 任何听到CTS的节点都知道它在接收方附近，应该在该时间段内不进行传输(听到RTS但没有听到CTS的节点仍然可以发送,一定程度上有助于解决显露的终端问题)4. 接收方在成功接收一个帧后向发送方发送ACK(所有节点都必须等待接收方的ACK，然后再尝试发送)

[假设布局:A|B|C]①避免隐藏终端问题:A和C项发给B;A率先

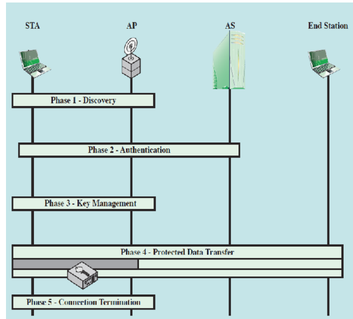
发送RTS;B发送CTS;C收到CTS后等待②避免暴露终端问题:B想发送给A,C想发送给另一个终端;C不需要等待,因为它收不到A的CTS③算法流程:发送方发送RTS,表明想占用多长时间;接收方以CTS作为回复,呼应预期传输时间;任何听到CTS的节点在该时间段内不进行传输;接收方在成功接收到一个帧后向发送方发送ACK
轮流协议:①轮询polling:主节点,问题:开销/延迟/单点故障②令牌Token passing:问题:同轮询
蜂窝网络 **4G LTE(Long Term Evolution)**
LTE帧结构:1帧(10ms)=10子帧=10*2时隙=10*2*7 OFDM Symbols
信号捕捉效应(Capture Effect): 当空中同时存在多个无线信号时, 功率最强的那个信号会被接收方解调出来。
信号遮蔽攻击Signal Overshadowing Attack:攻击者发送信号对目标子帧进行精准遮蔽 若攻击信号无实际意义:Jamming 若攻击信号是攻击者伪造的子帧:攻击者能够向受害者注入伪造的(广播)信息
SigOver的优势 功率优势 不需要与基站建立连接 受害者UE与合法基站保持通信
ReVoLTE 攻击流程
1. 目标通话 (第一次通话): 攻击者嗅探目标通话的密文(c)
2. 密钥通话 (第二次通话): 攻击者在发现上一个通话结束后，立即进行发起第二次通话, 攻击者收集通话过程中的明文(m')和密文(c')。结合第一步的密文(c)，即可推导出目标通话的明文
Radio-Frequency Identification IC chip + 天线
Components: Transceiver (Tag Reader), Transponder (RFID Tag), Antenna (天线)
Identification Assign IDs to objects;Link the ID to additional information about the object;Link the ID to complementary info;Find similar objects.
条形码Line-of-sight,Specifies object type **RFID** Radio contact(Fast, automated scanning), Uniquely specifies object(pointer to database entry for every object, unique, detailed history)
RFID Hardware Magnetic / Inductive Coupling电感耦合或Propagation Coupling电磁反向散射
RFID Tag Characteristics●passive device - power from reader
●range of up to several meters
●"smart label" - unique name and/or static data
Capabilities●little memory (64~128 bit static, cheap) Hundreds of bits soon;Maybe writeable under good conditions●little computational power (A few thousand gates,static keys for r/w permission, no real crypto functions)
Types of Tags●Read Only-factory programmed -usually chipless●Read / Write-on-board memory
-can save data -can change ID -higher cost
Data Transfer: Modulation Techniques Amplitude Modulation (AM)Frequency Shift Keying (FSK) Phase Shift Keying (PSK):-One frequency
Change the phase on the transition between a 0 to 1 or 1 to 0
-Faster data rate than FSK -Noise immunity -Slightly more difficult to build a reader than FSK **Data Encoding**:Miller
防冲突算法:阅读器之间TDMA, FDMA, CAMS 标签冲突自助阅读器:TDMA
TDMA①ALOHA回退,纯(18.4)/时隙S(时间同步,36.8)/帧的时隙ALOHA(FSA)(逻辑简单,常用,效率和帧长相关-动态自适应设置帧长)Q算法(动态调整帧长):一帧冲突过多,提前结束,发送更大帧; 一帧空隙多, 提前结束, 重启更小帧. ALOHA优缺点:算法简单, 标签识别性能良好, 结果可统计分析;标签饿死, 最坏情况时延无穷大②基于二进制树的防冲突:递归将冲突标签划分为两个子集, 直到只剩一个标签, 无饿死。查询二进制树(无状态, 维持广播二进制前缀), 用于无可写存储区的标签:随机二进制树, 标签维持计数器,0发送id,冲突加0/1,中序遍历.
优:算法简单, 不需要存储中间状态变量;缺:标签识别时延受标签ID分布及长度影响
RFID: Security and Privacy for "Five-Cent Computers" RFID特点●highly mobile●contain personal info●subject to surreptitious (秘密的) scanning●no crypto●Access control difficult to achieve●Data privacy difficult to protect
Proposed Solutions to the Privacy Problem
consumer privacy problem / tracking problem (被跟踪) / authentication problem (-Privacy:
Misbehaving readers harvesting information from well-behaving tags -Authentication:Well-behaving readers harvesting information from misbehaving tags, particularly counterfeit ones) Corporate espionage (商业间谍) efficient mugging(抢劫) Tag counterfeiting(伪造) 国防部要求
Solutions:●"Kill" RFID Tags:EPC tags "kill" 功能收到密码自毁永久失效,在物品卖出后保护消费者隐私●Re-naming Tags:tag可能会被跟踪:随时间变化relable new identifier仍能按原信息识别●Distance Measurement:识别距离越远给的信息越少●Policy and Legislation | 政策和立法
HB Protocol Goal:authenticate RFID tag to the reader 内积challenge(一定概率正确即可,HB+互相challenge更安全)安全性基于LPN NP-hard
LPN:带噪声学习奇偶校验Learning Parity with Noise(1一奇数个1, 0一偶数个1)噪音会以ε概率随机反转 方程组难解
Summary●Advantages○Passive 被动的(wireless) ○Store data on a tag ○Can be hidden ○Work in harsh environments (能在恶劣环境下工作) ○Low cost ●Disadvantages ○Lack of standards

○Short range ○Security **Reality**: 几乎不能工作:水旁难识别,可以偷偷让别人帮你付钱
安全例子:提取硬件特征(协方差)和防重放机制
蓝牙安全与隐私用于短距离交换数据的无线技术标准.ISM 频段从2.4到2.485 GHz。个人局域网(体域网)。爱立信1994年首次提出•最初设想为RS-232数据电缆的无线替代品。
Bluetooth Special Interest Group 1998 802.15.1SIG监督规范的制定，管理资格认证程序，并保护商标
Characteristics -Unlicensed 2.4 GHz ISM 工业、科学、医疗 -总数据速率为1 Mbit/s(EDR:3Mbit/s, HS:24Mbit/s) –放大器:10米范围扩展到100米–TDMA TDD慢速跳频扩频 - 一个piconet中最多支持8个设备(1个主设备和7个从设备) ,piconet可以组合形成散射网scatternets- Mixed voice/data connections possible- 加密-Ubiquitous无处不在 radio link
OSI物理链路应用层, L2CAP WPAN
通信拓扑:**蓝牙Piconet ad-hoc**
●可以是 master 或者 slave, 最多可以 1 master & 7 slaves (255 inactive slaves), sync to a common clock
●master 可以确定每个 slave 的 bit rate
●unique frequency hopping pattern / ID
●slave 只能与 master 通信
Bluetooth Scatternet 两个piconet有交集
●设备可以时分复用TDM 参加多个 piconet
●可以同时作为 master 和 slave, 但是不能同时做两个 master
物理层:跳频 由设备地址和master时钟中的字段决定.基本模式:ISM频带79个频率伪随机排序.自适应频率跳变AFH存在干扰情况下提高物理链路性能, 减少物理链路对ISM频带内其他设备的干扰,使用的频率少于79
时间槽物理信道划分为 625μs time slot 时分双工time divison duplex, master 和 slave 通信alternatively transmit交替传输, 包出发必须对齐slot,可以拓展到五个time slots
●Bluetooth Low Energy(Smart Bluetooth)相对传统 classic bluetooth 在发送时间和能耗有显著提高, 传感器网络中使用. 双模芯片组Dual Mode Chipsets支持传统和BLE
Security authentication–验证通道中正在通信的设备的标识 Confidentiality—只允许授权用户访问数据来保护数据不受攻击者的攻击。
Authorization-只有授权用户才能使用控制资源
Security Modes
Mode 1 Non-Secure Mode无安全
蓝牙自带跳频(1600次)短距(<10m), 窃听有限 2.45GHz FHSS微波炉等
Mode 2 - Service Level Enforced Security
链路建立后、逻辑通道建立前启动安全过程。
●Depend on service:见下0x2●All services on a device are given the same security policy, other than application layer add-ons.
Services can have one of 3 **security levels:**
●Level 3: Requires Authentication and Authorization. PIN number must be entered.
●Level 2: Authentication only, fixed PIN ok.
●Level 1: Open to all devices, the default level. Security for legacy applications, for example。
Mode 3 - Link-level Enforced Security
在链路建立前启动安全过程。
一用对称密钥实现in a challenge-response system.一目前所有蓝牙安全机制都是相同且公开的一关键:PIN, BD_ADDR, RAND(), Link and Encryption Keys
蓝牙安全运作流程
• 0x2 蓝牙的信任模式– 受信任:设备已与另一设备建立固定关系, 且对所有服务的访问不受限制。– 不受信任:虽然已成功通过身份验证, 但设备只能访问一组受限制的服务。
• 0x3 设备的可发现性– BD_ADDR
• 0x4 蓝牙安全服务– 基于挑战/应答(Challenge/Response)方式执行身份验证。
– PIN码/SSP
• 0x5 其他安全功能– 自适应跳频– E0加密算法– 不可见性– 配对
Security Issues ●Strength of the Random Number Generator (RNG) is unknown.●Short PINs are allowed.●Encryption key length is negotiable (可协商的). ●No user authentication exists.●Stream cipher is weak and key length is negotiable.●Privacy can be compromised损害 if the BD_ADDR is captured and associated with a particular user.●Device authentication is simple shared key challenge response. (单线身份验证会受到Man-in-middle攻击; mutual auth is good)
Security Threats●DoS, 设备不可用, 电池耗尽●Fuzzing attacks发错误格式的信息●Blue jacking (用IMEI标识所有来电)●Blue snarfing 用户向外发消息时干坏事●重放攻击, sniff嗅探 guard:阻塞+专有链接
定位系统 位置●地理位置 空间坐标● 处在时刻 时间坐标 ● 对象 身份信息
各国的卫星定位系统:美GPS, 俄GLONASS, 欧盟 伽利略, 中北斗一号(区域)北斗二号(全球)GPS是目前最常用卫星导航系统,1973开始计划,1994投入使用,2000取消军用民用精度差别. 系统结构:宇宙24颗工作卫星, 地面监控1主控 4天线 6监视站, 用户GPS接收机
优点:精度高,全球覆盖 ;缺点:启动时间长,室内信号差,需要接收(定位3颗卫星足够)
A-GPS(Assisted):GPS和蜂窝基站定位结合体, 利用基站定位确定大致范围, 连接网络查询当前位置可见卫星, 大大缩短搜索卫星的时间。

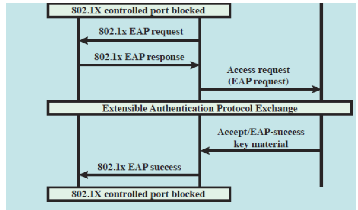
蜂窝基站定位 **GSM**蜂窝网络, 通讯区域分割成蜂窝小区, 每小区对应一个基站(利用基站位置已知)
-单基站定位法-**COO**定位**Cell of Origin**将所属基站位置视为移动设备位置,精度取决于基站覆盖范围,大则误差大,简单快速紧急。
-多基站定位法 -**ToA/TDoA**定位法, 测量无线信号传播时间, 需要三个基站才能定位, 稀疏不适用 -**AoA**定位法:测方向, 需要两个基站
蜂窝优点:启动速度快, 信号穿透能力强
缺点:精度低, 基站造价昂贵
紧急电话定位E-911:综合各类定位方法择优
室内精确定位 复杂性 多径效应,阻碍作用(长波GPS传播能力强, 穿透弱, 应选短波定位)
-已有设备:WiFi, ZigBee, 蓝牙, 部署方便, 成本低, 精度有限
-专门设备:红外线, 超声波, RFID, 超宽带UWB, 精度高, 成本高
Wi-Fi定位:无线AP定位 精确 智能手机成熟
Skyhook: AP位置数据库 精度10米 响应1秒
定位方法 关键• 一个或多个已知坐标参考点• 测量待定物体与已知参考点的空间关系• 两个步骤:测量物理量→根据物理量确定目标位置
常见定位方法:• 基于距离(时间)ToA • 基于距离(时间)差TDoA• 基于信号特征 RSS
ToA 时间:电磁波和声波波速差/波往返时间 位置:三点画圆交点 超过三个点最小二乘
局限 要参考点和测量目标时钟同步, TDoA不需要, 但参考点间仍要同步
TDoA距离差→双曲线 至少两组联立
基于信号强度测距 前述都需要接收端特殊装置 这个直接利用无线通信的射频信号定位
• 原理:信号强度随传播距离二次衰减
• 问题:理想公式难以实际应用
基于信号特征 将信号强度特征看做"指纹",N个参考节点信号的强度N维向量比对数据库
缺点:不能应对动态变化
例子• LANDMARC:RFID • LiFS:智能手机运动传感器捕捉用户运动信息, 关联独立RSS
新挑战和发展前景:网络异构, 环境多变, 信息安全与隐私保护, 大规模应用
WEP Wired Equivalent Privacy: Link-layer encryption
802.11 **Goals** Confidentiality Access control Data integrity but fail **security more a concern reason**: no inherent physical protection(logical associations); broadcast communications(overhear,jamming); eavesdropping窃听; bogus伪造; 重放; illegitimate access; DoS
Eavesdropping:easy to perform, **most impossible to detect**; everything is transmitted in clear text; different tools available; possible kilometers away
Man-in-the-middle-attack: spoof a disassociate断连 message from victim->look for new AP->advertises his own AP on a different channel->using the real AP's MAC address->connects to the real AP using victim's MAC address
Denial-of-Service:transmission regency used(frequency jamming); MAC layer (spoofed disassociation messages, target on specific user); higher layer protocol(TCP/IP)(SYN Flooding)
Security Requirements: confidentiality, authenticity, replay detection, integrity, access control, protection against jamming
WEP flavors: RC4(stream cypher); originally 64bit (40 key+24 IV-initialization vector)- > 128->256
WEP encryption:CRC-32 polynomial(integrity; plaintext=message+CRC; keystream和plaintext等长) concat IV and key, use RC4; ciphertext: XOR plaintext with keystream; IV放密文前;解密反向并验证CRC
Major problems with WEP: keystream(IV) reuse; key management/distribution; weak msg authentication; shared key authentication不用WEP key就能和AP认证;loose authentication (Beacon, de-auth & re-auth messages not authenticated
Keystream Reuse: ①WEP seed=24bit IV+fixed key②same IV is used with the same master key, keystream same③24 bit IV not sufficient to avoid collision(assigned randomly->birthday paradox, assigned sequentially->re-initialized] **IV** carried in plaintext, only 24 bits, no restrictions on IV reuse, forms a significant portion of the seed for RC4
Weak IVs and Weak keys in RC4 Weak Message Integrity(ICV): CRC-32: 非密码; 攻击者容易重算 (replay/injection attacks)无 **Key Management,**只能手动改(often one);statically configured; key values can be directly set as hex data; key generators provided
User Auth(可选)shared key authentication protocol(challenge);keystream known, 无需key
Brute Force/Dictionary Attack:明文IV+暴力key
FMS Attack: a class of RC4 keys weak keys, first 2 bytes of key stream->rc4 key can be discovered
Chopchop Attack: not recover key, reveal msg. capture one packet,truncate the last byte guess one value for plaintext, correct the checksum
Fragmentation Attack: chopping a packet into smaller packets(802.11 16 & IP);WEP encryption on each individual fragment using the same IV
Protecting WEP:ncrease the number of bytes used for encryption; Remove the weak IV-keystream re-use vulnerabilities; prevent key re-use; extensible authentication protocol(EAP)-change often the WEP-key; deploy IDS;using modified versions
WPA Wi-Fi Protected Access
4 new algorithms:①message integrity code (MIC) – Michael②48-bit IV and IV sequencing rules③key derivation and distribution④temporal key integrity protocol(TKIP) generates per-packet keys
WPA Facts:①RC4②key size: 128 bits(每 frame改变)③密钥管理 TKIP④hash method: Michael (8bytes, placed between data and ICV)⑤802.1x 认证
MIC:①64 bit message②保护data和header③hash calculated on a per-packet basis④per-sender, per-receiver basis(IV, dst MAC, src MAC, payload)
IV Sequence Enforcement(defeating replays): 16-bit 单增计数①取old IV 1和3 bytes②rekey重置0③每个包+1④不按规矩就丢了
TKIP: WEP(per-packet,simply concat), TKIP(per-packet key 2 key mixing phases,temporal+MAC+IV)
TKIP Re-key mechanism:①process of delivering fresh encryption and integrity keys(MIC keys) to the stations and Aps②WPA key hierarchy: master key(Pairwise Master Key, PMK) – derived from either an 802.1X key exchange or from the passphrase, Session keys(Pairwise Transient Key, PTK) – derived from the master key **TKIP** appears to provide weak but genuine security, meet goal of software deployment.performance降不多,达到市场要求
Passphrase/PTK Negotiation:①Pre-shared key mode: no RADIUS server required, shared secret is used for authentication, management is handled on the AP, vulnerable to dictionary attacks②Enterprise mode: requires an authentication server, uses RADIUS protocol for authentication and key distribution, centralizes management
WPA-PSK: home/SOHO use, 4-way handshake authentication(generate PTK) , pre-shared key+TKIP(shared secret known->no security), weak against passive dictionary attack **MSK→GMK/PMK→(握手,两次challenge+两次确认)→GTK/PTK**
暴力630年,字典快一点/彩虹表(indexed hash lists, pre-hash millions of words, 2-3T容量,cracks WPA v1 and v2 with preshared key)
WPA Enterprise: authentication server distributes different keys to each user using 802.1X; enhanced security and authentication
IEEE 802.1X(supplicant,authenticator,authentication server): 基于端口的网络的访问控制,fulfills securit漏洞, authentication and key management. 第三方RADIUS server完成.
Extensible Authentication Protocol(EAP): carrier protocol to transport msgs of real authentication protocols, generic authentication protocol run over any link layer protocol(4 types: EAP request-AS to M, EAP response-M to AS, EAP success-successful authentication, EAP failure -authentication failure)
IEEE 802.1x authentication end: AS and client establish a session, AS and client possess a mutually authenticated Master key, client and AS derived PMK, AS distribute PMK to AP.
Chopchop:802.11e Qos不同channel密钥同IV不同
WPA2 Wi-Fi Protected Access II



在WPA的基础上使用基于AES的CCMP来增强。
WPA2分为个人模式和企业模式
• 个人模式使用PSK无需对用户进行单独身份验证
• 企业(Enterprise)模式要求使用Extended EAP对用户进行单独身份验证。



WPA2 操作阶段**:**Phase1:Discovery AP和client协商安全协议;
Phase2:Authentication 生成master key;
Phase3:Key-Management 生成temporary keys;
Phase4:Protected Data Transfer Phase3中生成的所有key都被用来CCMP协议, 用来提供数据机密性和完整性. Phase5:Connection Termination
Phase1:**Discover** • 功能发现 ◇AP使用称为Beacons and Probe Responses来广播发布其安全功能(在RSN Information Element(RSN IE)中发布)
◇STA使用这些信息来识别其希望与之通信的WLAN的AP ◇STA与AP通信, 用于选择通信请求中的密码套件和身份验证机制 • 开放系统认证:◇ 只为IEEE 802.11状态机向后兼容, 不提供安全性 ◇ 本质上只是两个设备(STP和AP)交换标识符 • 通讯:◇ 目的是达成一套一致的安全功能 ◇ STA发送通信请求(Association Request)帧给AP, 从AP发布的功能中指定一组匹配功能(一个身份验证和密钥管理套件、一个配对密码套件和一个group-key密码套件)



Phase2:**Authentication** 基于上阶段协商的EAP和身份认证方法 • 连接到AS ◇ STA向通信的AP发送"连接到AS"的请求 ◇ AP回复并向AS发送访问请求 • 交换EAP:STA和AS进行相互认证 1.使用EAPOL-start消息启动802.11X交换 2.身份验证器发出EAP-request/identity帧 3.恳求者用EAP-response/identity帧回复, 并将其传递给radius服务器 4.Radius确定所需身份验证类型并发送针对特定方法类型的EAP请求 5.请求方以EAP-response/method帧进行回复 - 重复步骤4和5以完成身份验证 6.radius服务器用Radius-access-accept包授予请求 • 安全密钥的传输:一旦建立认证, AS生成主会话密钥并发送给STA
Phase 3 Key Management
PMK由AS发送到验证器, 请求者和认证者现在有相同PM(整个会话中永久)Must generate a Pairwise Transient Key for encryption of data. Done using 4-way handshake
PTK加密数据, 四次握手过程生成会话密钥确保每个会话数据加密唯一, 减少密钥破解风险。
四次握手过程 • 第一次AP 向客户端发送一个随机数(ANonce)客户端用其生成 PTK • 第二次客户端回复 AP并发送自己生成的随机数(SNonce) AP用其和ANonce生成相同PTK • 第三次AP 发送消息确认PTK 生成并提供用于广播和多播数据加密的 Group Temporal Key(GTK) • 第四次客户端回复AP确认收到GTK, 可以开始加密和解密数据传输
Confirm that the client holds the PMK.
Confirm that the PMK is correct and up-to-date.
Create pairwise transient key (PTK) from the PMK.
Install the pairwise encryption and integrity keys into IEEE 802.11.
Transport the group temporal key (GTK) and GTK sequence number from Authenticator to Supplicant and install the GTK and GTK sequence number in the STA and, if not already installed, in the AP.
Confirm the cipher suite selection.
配对密钥体系 **PSK/MK(个人/企业)→PMK→PTK→KCK(confirmation)+KEK(加密)+TK(临时)**
WPA2 加密 WPA2基于WPA增加了AES加密, 128bitAES采用CCMP(Counter-Mode/CBC-MAC Protocol)机制 CTR加密,CBC完整性
CTR:随机数和计数器和key块加密后与明文异或
CBC:消息和上一步密文异或后加密,继续下一轮
AES–CCMP特点• CCMP在MAC帧的帧体和几乎整个报头上提供完整性保护(防止对手利用MAC报头) • CCMP使用48位分组号(PN)(防止重放攻击并为每个数据包构造新的nonce)
•未知密钥对手无法破坏数据的机密性和完整性
加密算法比较

	WEP	WPA	WPA2
Cipher	RC4	RC4	AES
Key Sizes	40 bits	128bits encryption 64 bits authentication	128 bits
Key Life	24 bit IV	48 bit IV	48 bit IV
Packet Key	Concatenated	Mixing Function	Not Needed
Data Integrity	CRC-32	Michael Algorithm	CCM
Header Integrity	None	Michael Algorithm	CCM
Defeat Replay Attacks	None	IV Sequence	IV Sequence
Key Management	None	EAP Based	EAP Based

WPA2 优点 •免疫中间人/伪造/重放/暴力/弱key
• 使用PMK缓存功能允许客户端重新连接到他最近连接的访问点, 而无需重新进行身份验证。
•允许客户端在保持连接到正在远离的接入点的同时令正在靠近的接入点对自己进行预身份验证。
•基于鲁棒安全网络RSN, 除WPA中功能还支持◇ 基础设施和特设网络的强大加密和身份验证;WPA只支持基础设施网络 ◇ 密钥推导过程开销减少
WPA2 缺点 • jamming/flooding/AP failure• 攻击者可通过分析未受保护的控制和管理帧获取发现大量网络信息 •易受DoS攻击 •易受MAC addresses spoofing和mass deauthentication attacks.攻击
KRACK(Key Reinstallation Attack)攻击使用4路握手漏洞。攻击者嗅探、重放四次握手过程中的第3个消息报文, 强制重置协议加密使用到的nonce值及重放计数, 重装加密密钥。
Reinstallation攻击流程: