Wireless Network Security and Privacy
Autumn 2023

Xiaoyu Ji

Telecom Security & Privacy

Agenda

- 2-5G and security
- Li-Fi
- Low-power wide area wireless networks

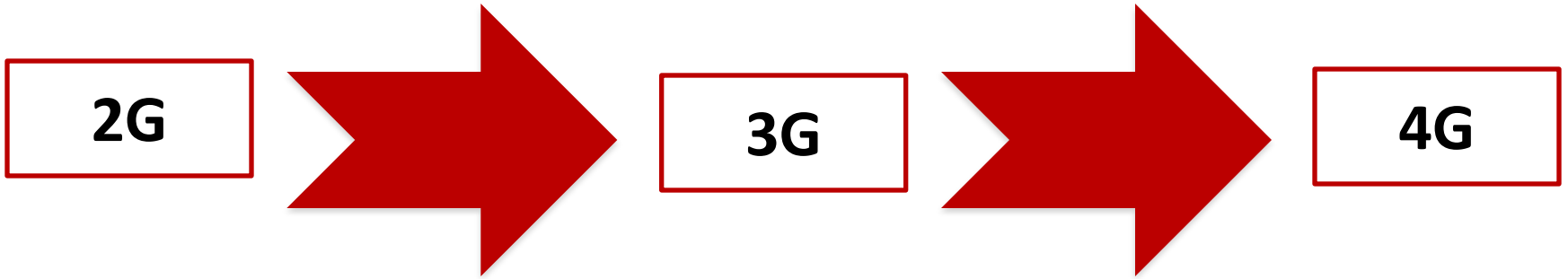
Let's talk about mobile networks

Cellular Network Standards

3GPP: The 3rd Generation Partnership Project (3GPP)

Generation	3GPP Circuit Switched	3GPP Packet Switched	3GPP2	Wimax Forum
2G	GSM		cdmaOne	
2.5G		GPRS		
2.75G		EDGE		
3G	UMTS		CDMA2000	
3.5G		HSPA/+	CDMA EV-DO	
4G		**LTE**	~~UMB~~	WiMAX

Network Architecture Evolution

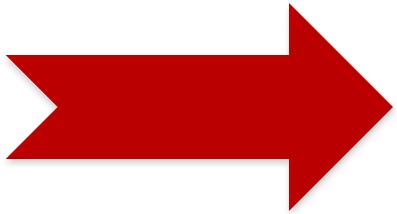


- Circuit-switching for voice

- Circuit-switching for voice
- Packet-switching for data

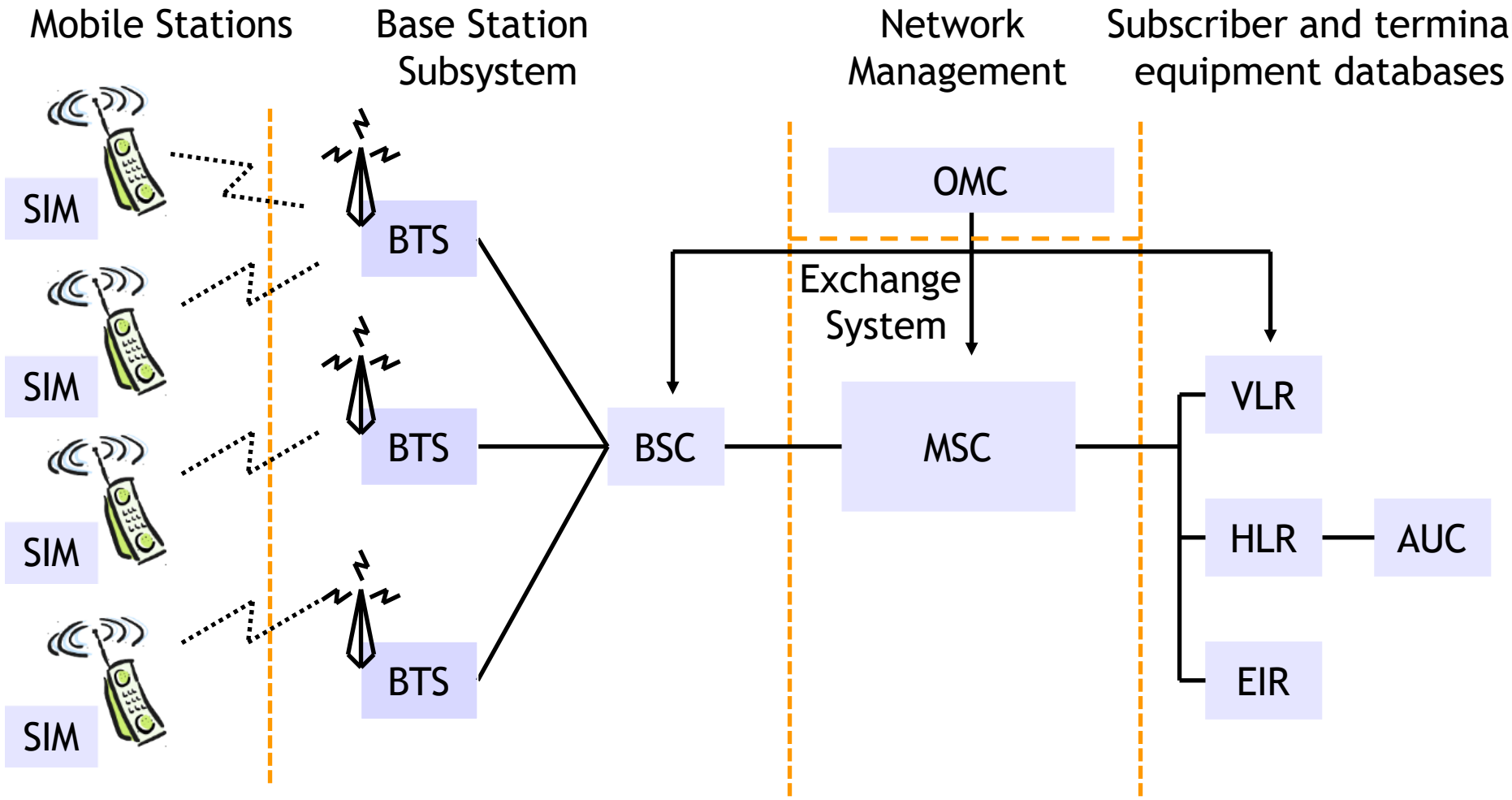
- Packet-switching for everything
- IP-based

Telecomm Infrastructure



IP-based Internet

2G GSM/CDMA Architecture



adapted from [M. Stepanov; http://www.gsm-security.net/]

2G GSM Security

- Secure access
  - User authentication for billing and fraud prevention
  - Uses a challenge/response protocol based on a subscriber-specific authentication key (at HLR)
- Control and data signal confidentiality
  - Protect voice, data, and control (e.g., dialed telephone numbers) from eavesdropping via radio link encryption (key establishment is part of auth)
- Anonymity
  - Uses temporary identifiers (TMSI) instead of subscriber ID (IMSI) to prevent tracking users or identifying calls

3G Evolution

- The move from 2G to 3G primarily included:
  - Support for mobile data at (near-)broadband rates
    - UMTS, TD-CDMA, WCDMA, CDMA-3xRTT, TD-SCDMA, HSDPA, HSUPA, HSPA, HSPA+
  - Improved security protocols
    - Because everything in 2G was broken several ways

3G Security Enhancement

- 3G security model builds on GSM
- Protection against active attacks
  - Integrity mechanisms to protect critical signaling
  - Enhanced (mutual) authentication w/ key freshness
- Enhanced encryption
  - Stronger (public) algorithm, longer keys
  - Encryption deeper into the network
- Core security – signaling protection
- Potential for secure global roaming (3GPP auth)

Toward 4G

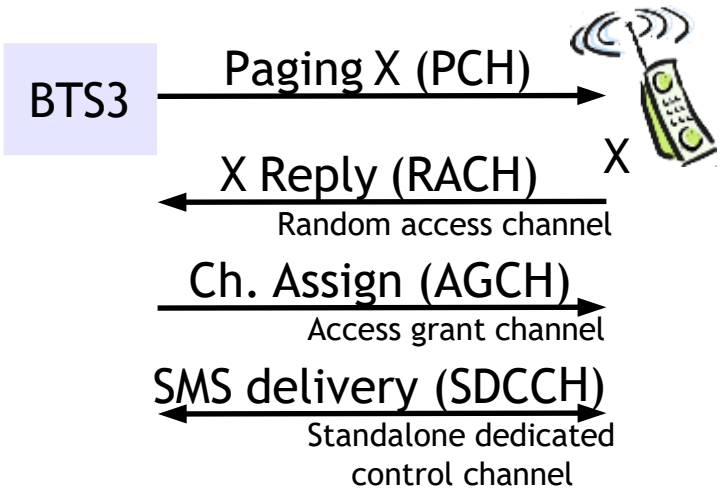
- 4G represents the next generation in cellular communication
  - ITU-R standard: 1Gbps fixed, 100Mbps @ 100kph
  - WiMAX Release 2, LTE-Advanced
    - WiMAX and LTE are not really 4G
    - Verizon, Sprint, AT&T use LTE; T-Mobile, AT&T use HSPA+
    - Most provide ~20Mbps fixed

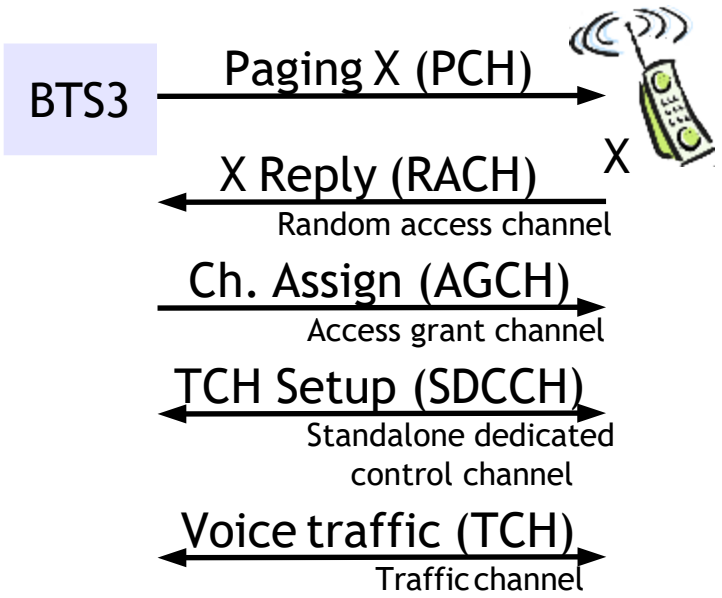
4G Security Issues

- All-IP network ==> all IP-based threats apply
- Verification of users
- Heterogeneous network access
  - User-preferred connection methods
  - Multiple available connections:
    - Attacker has more opportunity for exploit/attack
    - Device is exposed to attacks on each connection
      - Exploits based on driver code, comm protocols, transport / signaling, file-sharing, update, etc.
  - Complex management systems are required
- ?

Some other attacks on mobile networks

SMS Flooding ==> Voice DoS





- Voice & SMS Resources
  - TCH is not used for SMS
  - Both SMS and voice init. use RACH, AGCH, and SDCCH

SMS flooding also works as DoS against voice calls!

Rogue BTS

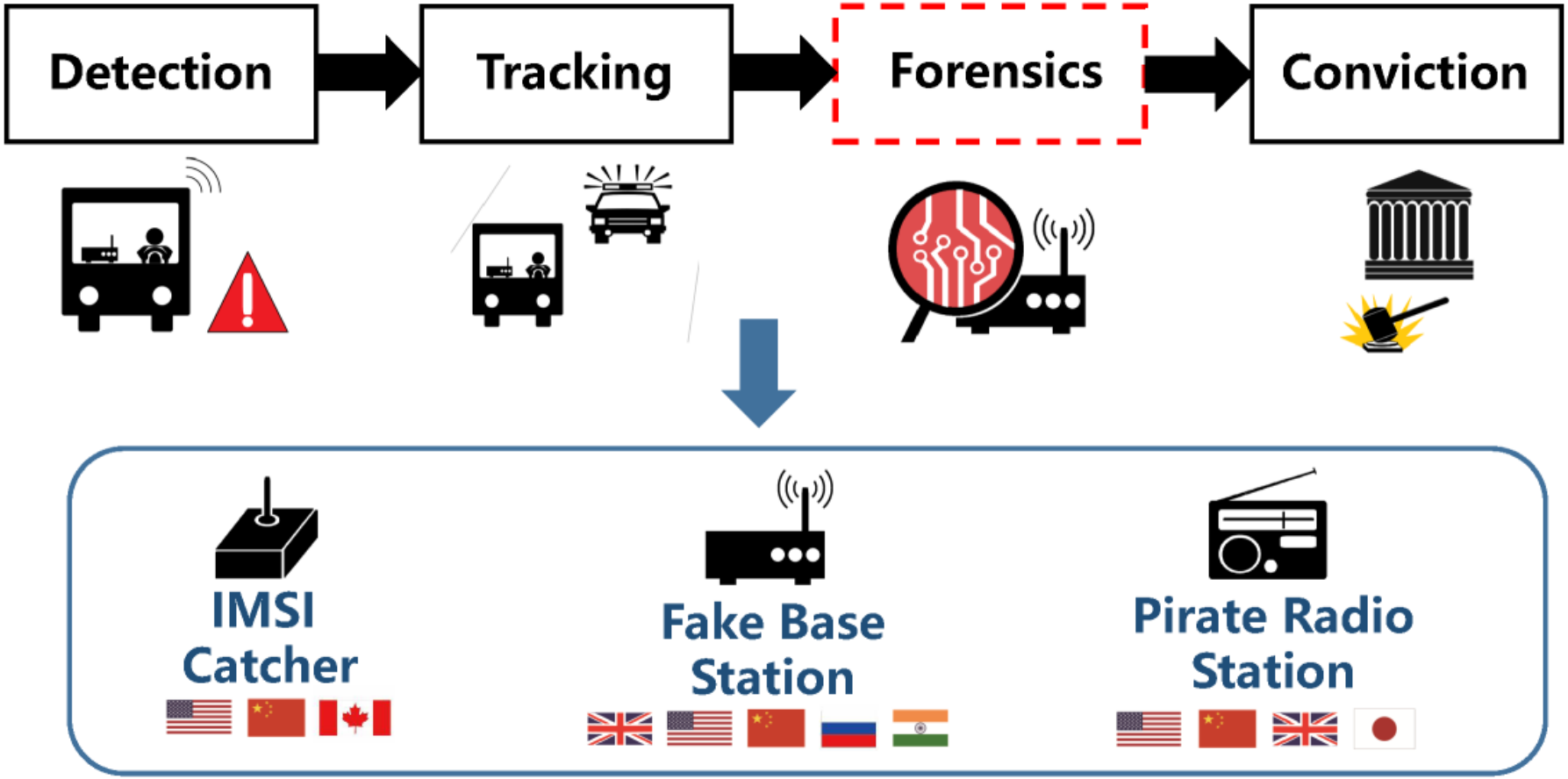
- An adversary can deploy a rogue BTS that spoofs / mimics a service provider to attract users
- Possible to launch a MitM attack on 2G/3G mobile connections
- Applies to GPRS, EDGE, UMTS, and HSPAcapable devices (far easier for GPRS/EDGE devices)
- Cheap
- Difficult to detect, if done well

Setting up a Rogue BTS

[Perez & Pico, BlackHat 2011]

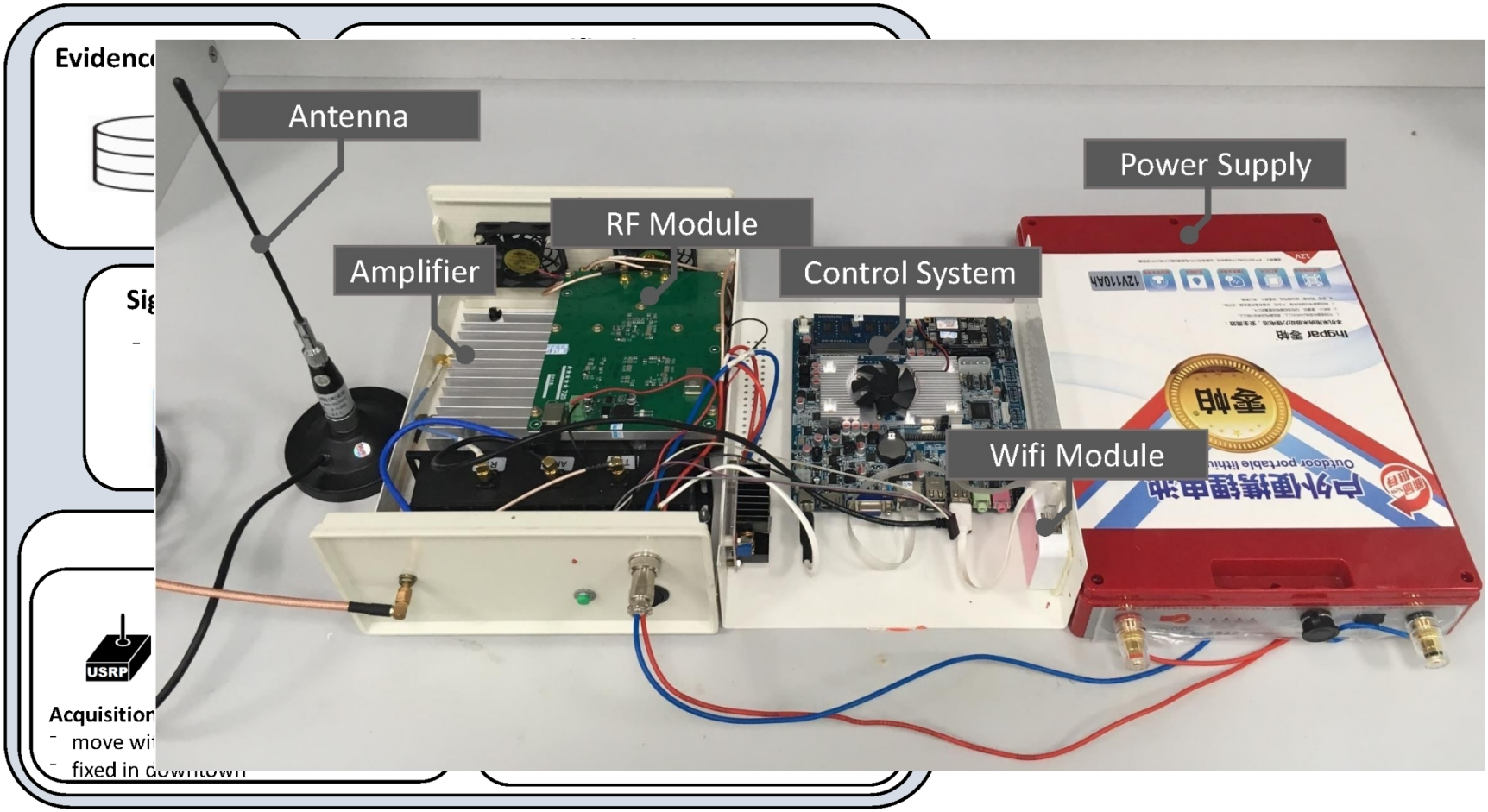
How to detect a RTS

Crime Forensics is important



How to detect a RTS

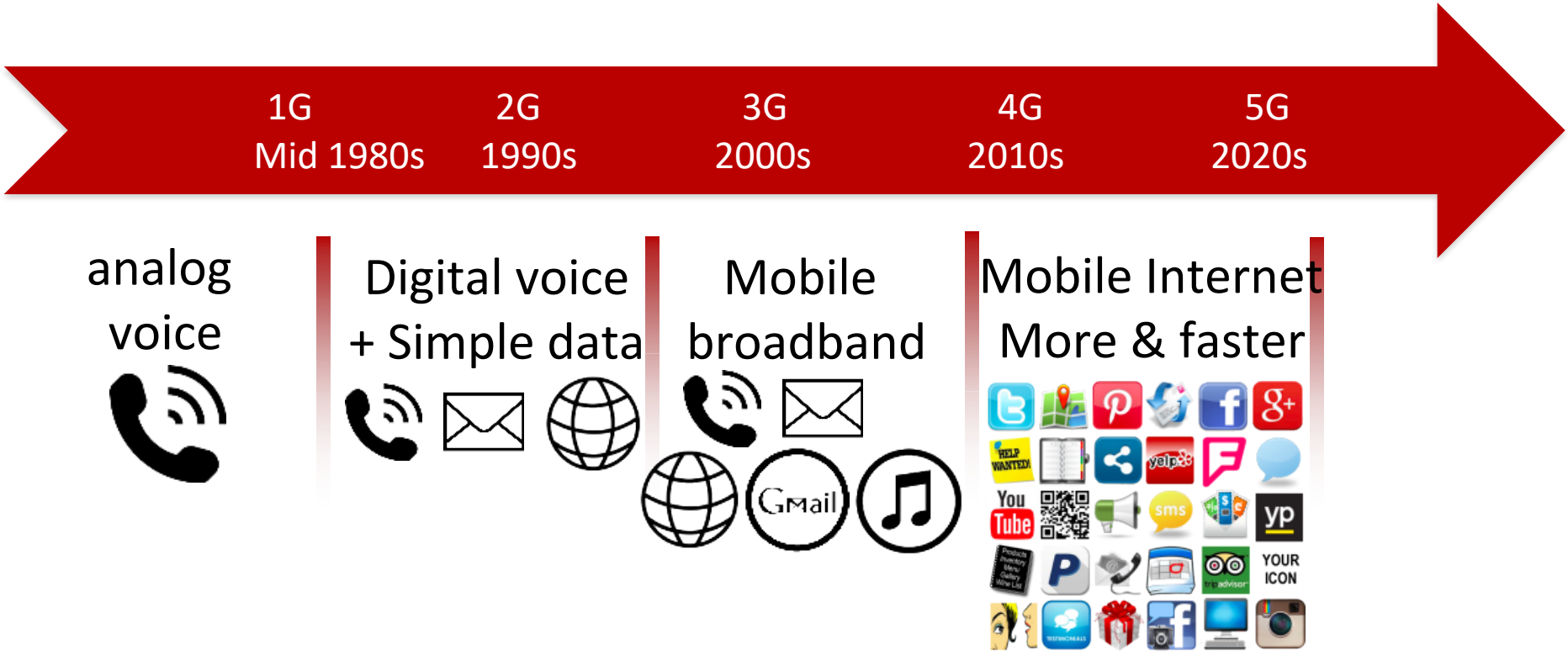
RTS hardware fingerprinting



What is 5G?

Next generation mobile network

Current generation: 4G LTE



Pull from User Demands: Mobile Internet Anytime, Anywhere

In-building

Outdoor

Walking

Driving

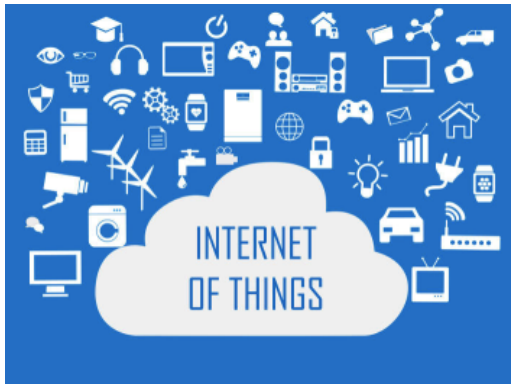
Subway

High-speed train

No. 1 disruptive technology in the past decade

Smartphones (not PCs): primary access points to Internet

Pull from User Demands in 5G



Internet of Things

Tactile Internet

Autonomous Driving

AR/VR

Remote Healthcare

Drone-based Delivery

… … … …

Well-Connected Everything

Pull from User Demands in 5G

4G 2010s → 5G 2020s

Much Faster
10Gps peak rate
< 1ms latency

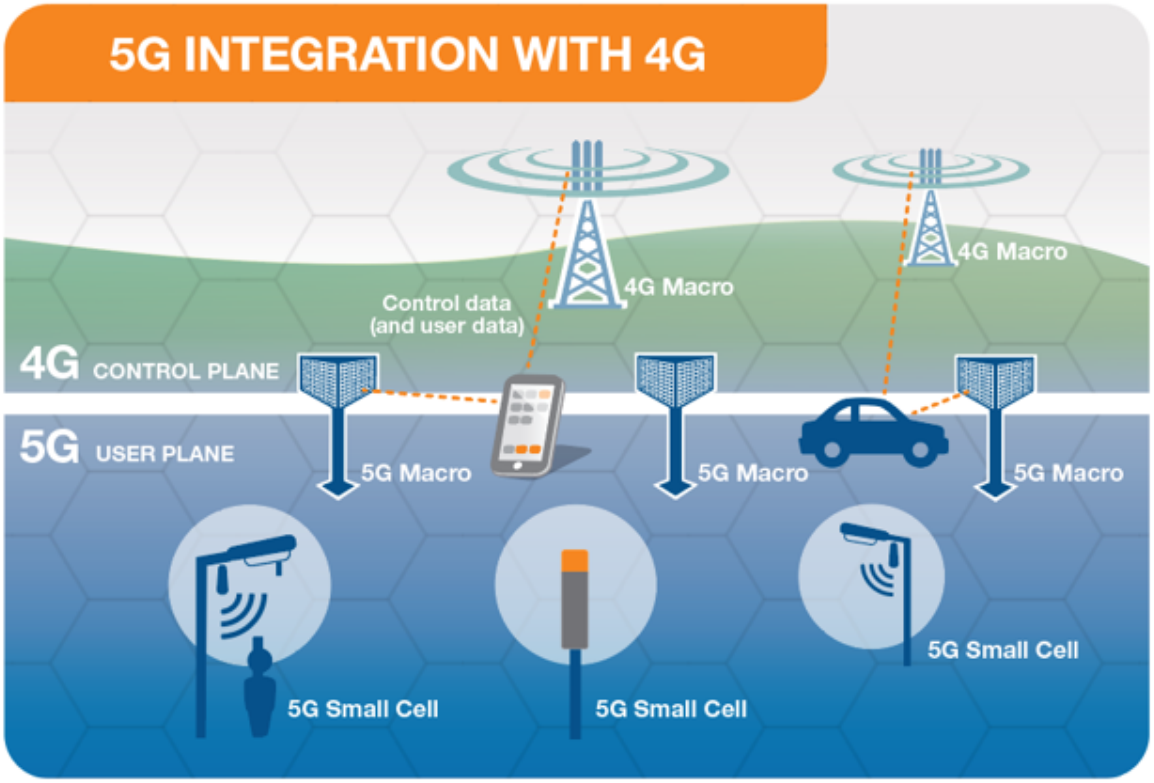
Super-connected
10000x traffic
1000x bandwidth
10-100x devices

Higher mobility
300+ Kmh

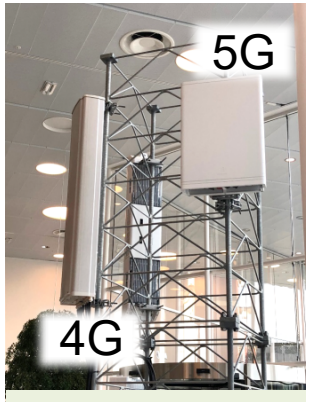
Ultra-reliable
99.999%

Energy-efficient
...

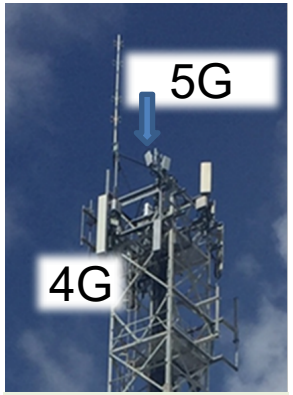
How does 5G work?



5G works together with 4G
4G acts as control plane
5G acts as data/user plane
5G will operate stand alone in later releases

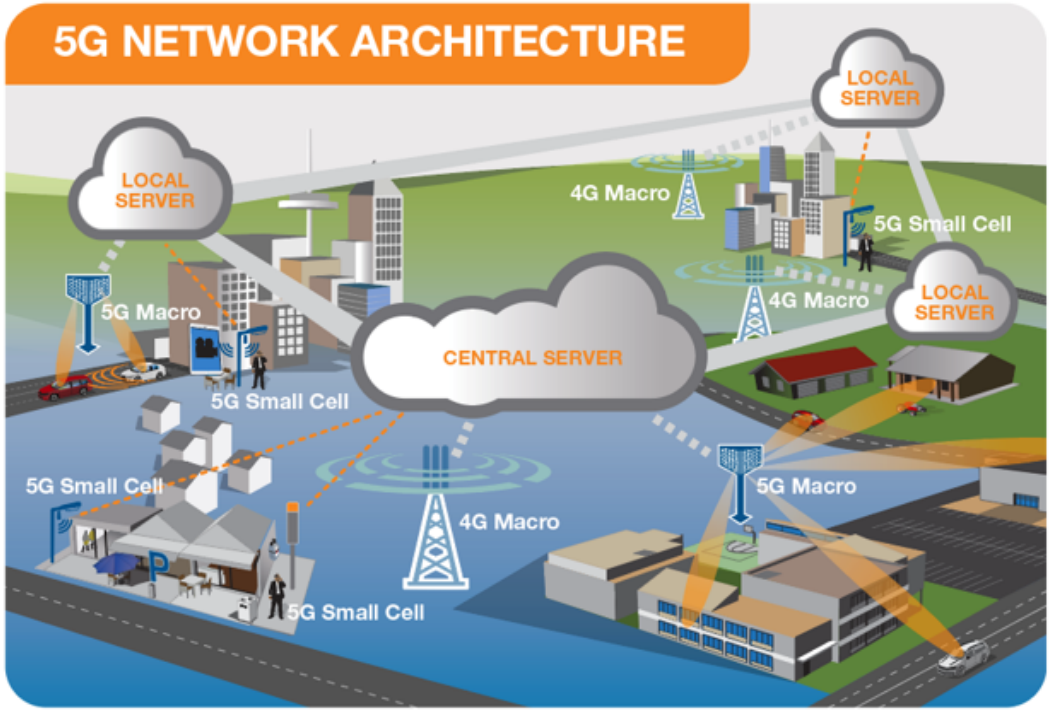


5G - 3.5GHz



5G – mmWave 27GHz

How does 5G work-network architecture



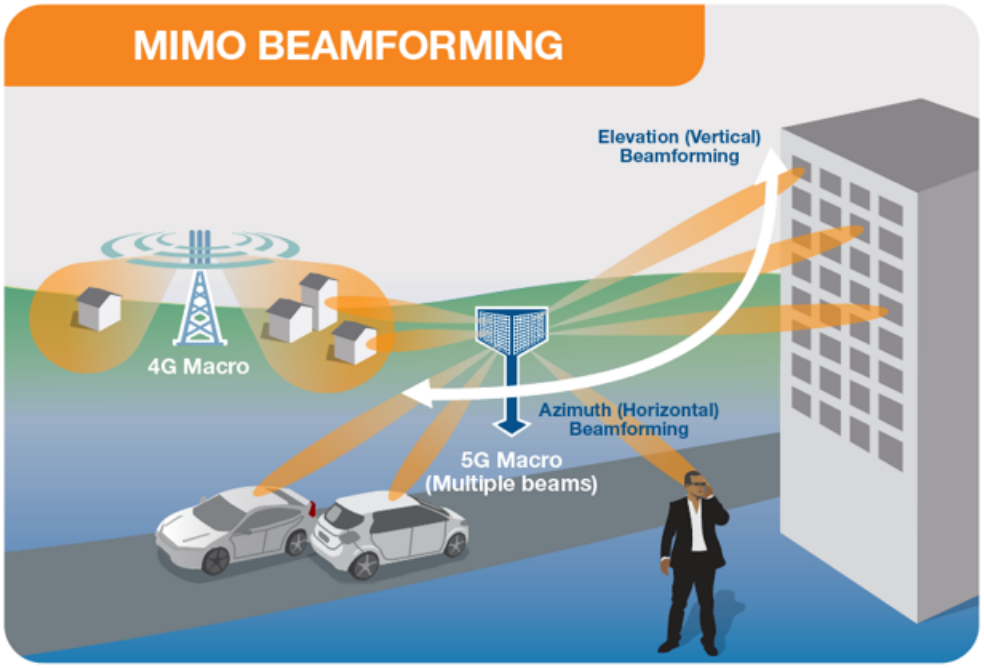
5G network architecture - illustrating 5G and 4G working together, with central and local servers providing faster content to users and low latency applications

Radio Access Network - small cells, towers, masts dedicated in-building and home systems that connect mobile users and wireless devices to the core network

Core Network - mobile exchange and data network, manages mobile voice, data and internet connections. Redesigned to integrate with the internet and cloud based services, distributed servers across the network.

Network Slicing - smart way to segment network for separate applications – e.g. emergency services

5G Technology - Beamforming



Dedicated radio signal towards the user

A 4G signal is typically spread across a wide area

Enabled by Massive MIMO technology

Identifies most efficient signal path

Improves connection reliability

Reduces interference (unwanted signals)

Efficient use of spectrum and power

Allows more simultaneous data streams

Key Point – Beamforming is more efficient and reduces average RF exposure levels

5G Technology - Beamforming live example

Li-Fi communication

可见光通信（Light Fidelity，Li-Fi）

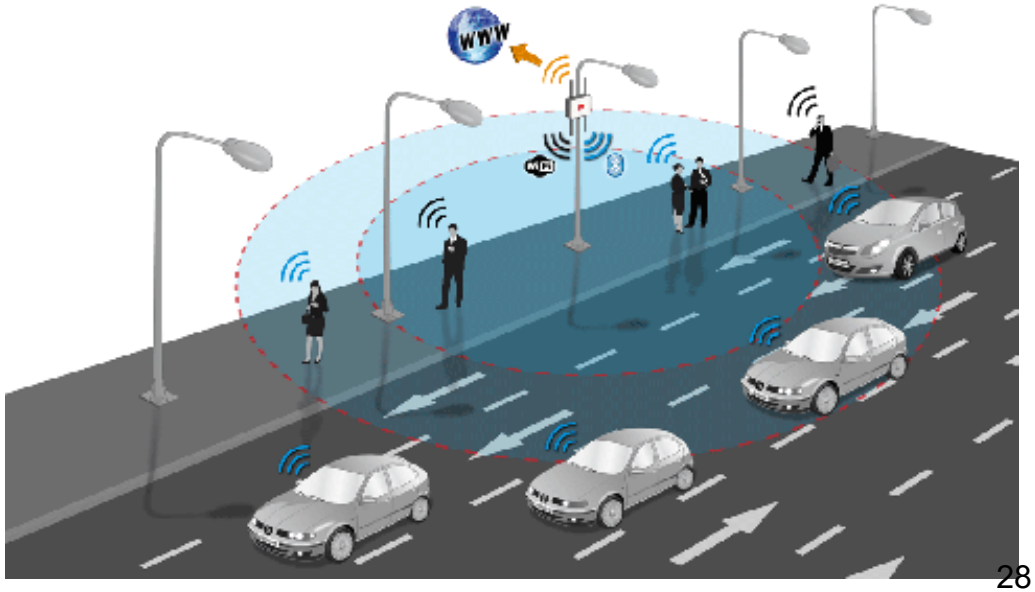
英国爱丁堡大学的哈斯教授研发出一种利用可见光波谱（如灯泡发出的光）进行数据传输的全新无线传输技术——Li-Fi，可作为Wi-Fi的有效补充手段。

可见光通信是一项前沿技术，其泛在性和频谱丰富性使其具有广泛的发展空间。

作为一种新的无线通信技术，可见光通信仍旧处在发展初期，还需要科研工作者更多的研究，才能催生出更为成熟的技术和产品。

Li-Fi的工作原理

LED灯具有高速电调制性能，可通过高速明暗闪烁信号传输信息（例如LED开表示1，关表示0）。这些闪烁肉眼不可见，但是却能被电子接收器或移动设备读取。
LED灯一旦被改造为Li-Fi热点，其照亮区域内的终端设备就能够随时接入网络。



Li-Fi的优点

- 丰富的频谱资源

  可见光的频谱宽度可达到射频频谱的1万倍，丰富的频谱资源使Li-Fi能够利用更宽的频谱实现更高的数据传输率。

- 低成本

  LED灯相较专用的Wi-Fi热点是非常廉价的，并且是人类生产生活的必需品，具有泛在性，几乎不需要额外的基础设施建设，部署、使用成本非常低。

- 安全性

  由于可见光具有可遮挡性，无法穿透墙壁，Li-Fi便于将信号限定在一定区域内，产生物理隔离，具有安全性。

- 无电磁辐射

  由于没有电磁辐射，Li-Fi的发射功率可以很高，且不会对人体产生电磁辐射影响。

- 无电磁干扰

  许多精密仪器对电磁干扰敏感，而Li-Fi并不使用无线电波，所以不会受到电磁干扰的限制，可以广泛应用于不适合射频无线通信的场合。

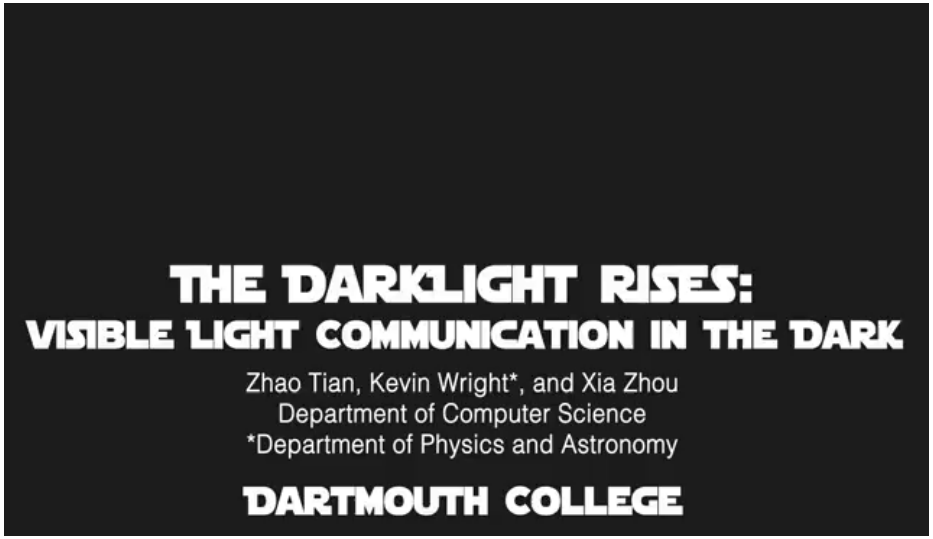
Li-Fi的缺点

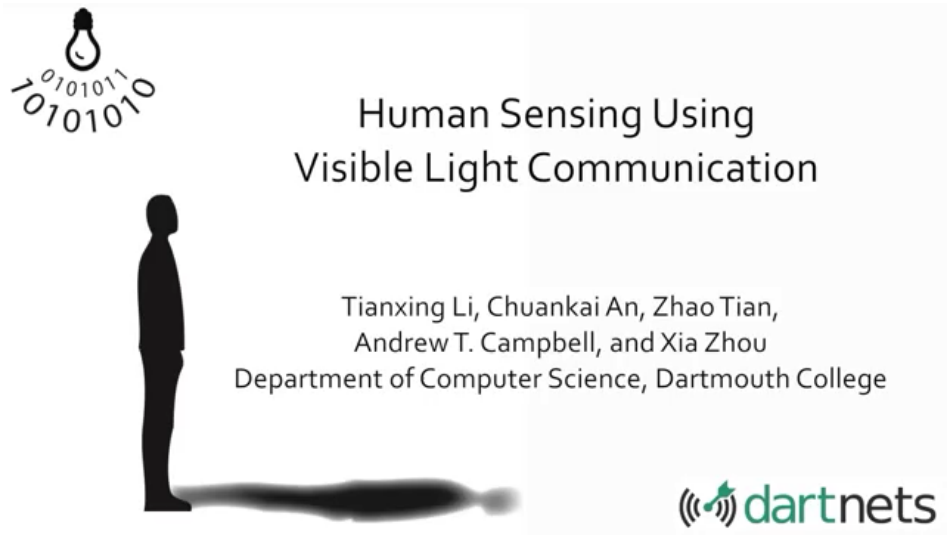
- 易被遮挡
  可见光通信非常容易被遮挡，进而导致信号中断，可靠性有待提升。
- 光源间断问题
  虽然电灯在人类生产生活空间普遍存在，但是当有自然光存在时，电灯并不会打开，通信无法进行。
- 频繁切换
  单一LED设备覆盖范围有限，当终端设备不停地移动时，需要频繁切换Li-Fi热点，容易导致连接丢失。
- 环境干扰
  环境光源有可能工作在同样的光谱频段，对Li-Fi造成干扰，后者会因为信噪比过差而无法可靠通信。
- 用户友好的反向通信
  从Li-Fi热点到终端设备使用可见光是非常自然的。但是用户如何友好地让终端设备与热点通信是值得深思的难题。相信没有人愿意在使用手机时还要忍受手机LED灯光照射自己的眼睛。

Demo

Research group: Xia Zhou, Dartmouth: https://home.cs.dartmouth.edu/~xia/

https://www.youtube.com/watch?v=qwxLYC2z1C0
https://www.youtube.com/channel/UCQhj_t5VL-SnOAj24EJcwaw/videos





Low-power wide area networks(LP-WAN)

低功耗广域网技术的发展

物联网出现之后，远距离、低功耗、低带宽的协议迸发出了新的生机。

物联网的典型场景：智能环境监控

- 从通信带宽角度看，智能监控的部分场景需要很低的数据量，比如智能电表。
- 从通信距离角度看，这类数据通常分布在各家各户，传输距离较远。
- 从通信能耗角度看，这类设备一般部署规模大且采用电池供电，由于需要长期工作，而且为了避免大规模更换电池带来的开销，这类设备对能耗有较高的要求。

低功耗广域网技术的发展（续）

- 对于这类远距离、低功耗、低带宽的协议，我们统一称之为低功耗广域网（Low Power Wide Area Network）技术。

- 该类协议有两个主要代表，远距离通信（Long Range Communication，LoRa）和窄带物联网（Narrow Band Internet of Things，NB-IoT）。

LoRa协议

- 2013年，Semtech公司发布了SX127x系列芯片，LoRa协议自此登上了无线通信的历史舞台。之后，Semtech公司发起成立的LoRa联盟负责协议的推广和应用等工作，为LoRa的后续发展提供了有效的保障和强大的助推力。
- 2016年，荷兰电信运营公司KPN宣布，荷兰已经成为世界上第一个推出全国性LoRa物联网应用网络的国家。
- 包括中兴在内的多家相关企业加入LoRa联盟，进一步推动LoRa协议、芯片和应用平台的发展。

LoRa芯片与ZigBee芯片的对比

协议	ZigBee	LoRa
芯片	CC2420（TI）	SX127x（SemTech）
发射功率	0dBm（1mW）	20dBm（100mW）
传输距离	100～300m	最高3km
调制方式	DSSS	CSS
带宽	250kbps	0.3～22kbps
单个包长	128字节	256字节
MAC协议	无特定MAC协议，可实现ZigBee不同模式	LoRaWAN三种不同模式
接收敏感度	+3dB高于噪声平面	19.5dB低于噪声平面

LoRa协议的三种集中工作方式

- 双向终端设备模式
  - 在这一模式中，节点只能在有数据上传时下载数据。这一模式可以减小大量能量开销。
- 有接收时隙的双向终端设备模式
  - 在这一模式中，节点可以在固定的时隙内下载数据。
- 最大化接收时隙的终端设备模式
  - 在这一模式中，节点有几乎连续的接收时隙。

NB-IoT协议

- 国内更为熟悉的一种低功耗广域网协议。
- NB-IoT支持蜂窝连接。相比GSM，NB-IoT将覆盖能力提升了20～30dB，支持每平方千米10万台设备连接，终端电池寿命长达5～10年，芯片成本低至1美元。
- NB-IoT极大地延伸了蜂窝网络的应用边界，适应了物联网时代的链接需求。

NB-IoT协议（续）

- 最初以沃达丰和华为提出的NB M2M为基础；
- 在高通加入后，发展为NB-CIOT；
- 随后，NB-CIOT与爱立信的NB LTE合并，最终形成了NB-IoT；
- 目前，NB-IoT已经进入了3GPP标准化工作的阶段

NB-IoT协议（续）

- 根据目前公开的资料，NB-IoT和LoRa的技术指标区别并不大，这是由低功耗广域网应用环境需求决定的。
- 然而，NB-IoT技术能够与现有的移动通信基站相结合，易部署于现有的无线基站上。
- 此外，NB-IoT目前得到了一级运营商（如沃达丰）以及设备制造商（如华为）的支持。这对于NB-IoT技术的推广和应用将起到至关重要的作用。
- 目前市场上不断出现商用的NB-IoT芯片，其具体性能和在应用中可能存在的问题尚不可知。

NB-IoT业务的主要特点

- **连接海量化**：Gartner预测，到2020年全球将有260亿物联网设备，市场价值超过3000亿美元，DHL和思科则预测连接数将达到500亿。中国移动预测2020年蜂窝物联网连接规模超过5亿。
- **业务碎片化**：NB-IoT与个人及家庭生活、工业生产深度融合，应用场景多，产业链中的终端、网络、芯片、操作系统、平台、业务等的具体实现各不相同，各类应用场景的业务规模、终端功能、数据种类也存在差异，“碎片化”现象严重
- **服务开放化**：NB-IoT业务平台既有运营商平台，也有互联网或用户自建的平台，可满足各种业务需求；同时，部分业务需要运营商开放云计算、位置查询、设备状态查询、认证等必要能力，使得运营商网络更加开放。因此，NB-IoT服务模式与传统的通信服务模式有较大不同，产业链将更长且不断产生各类新兴的商业模式。

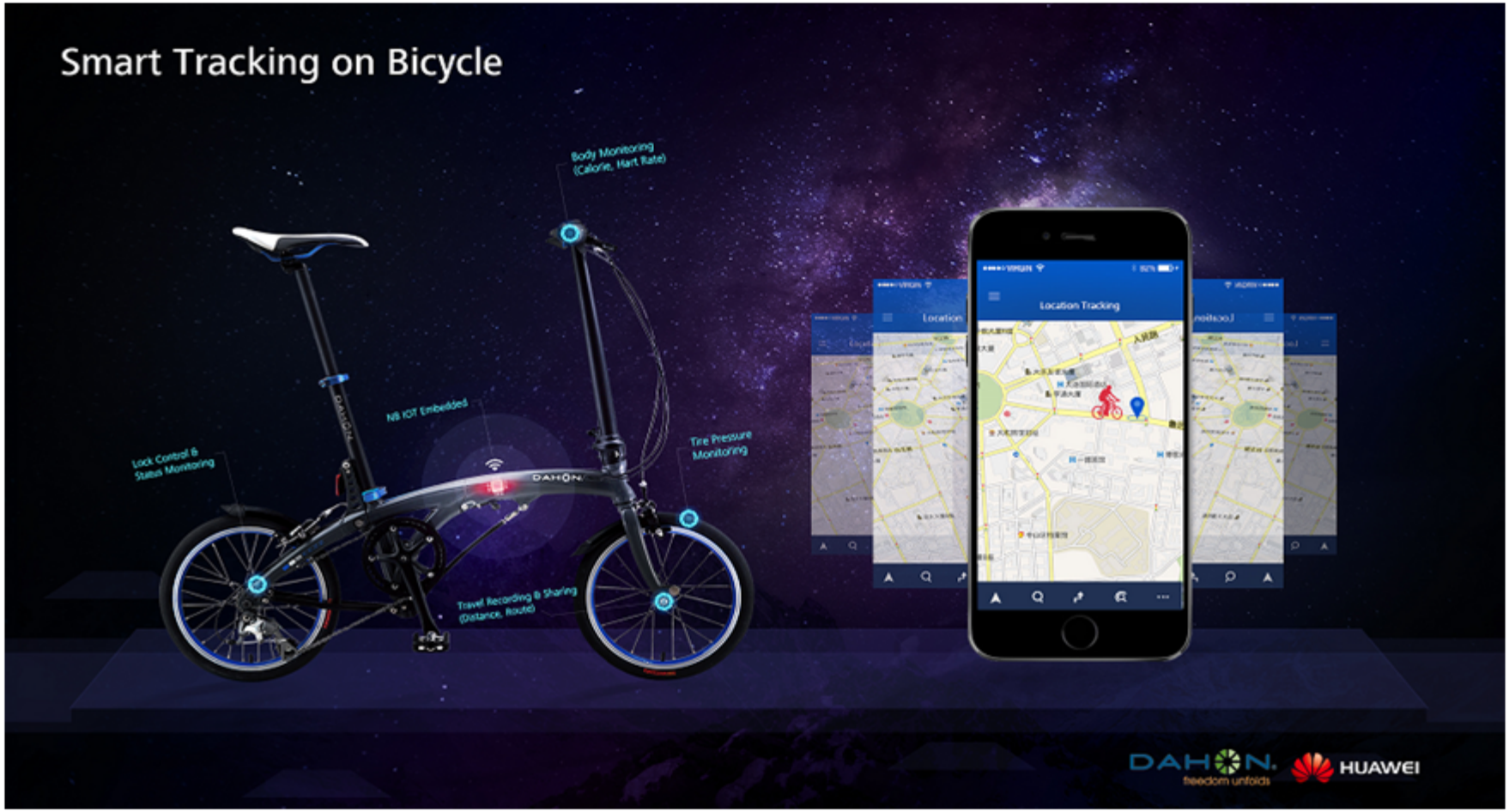
芯片厂商

- 华为海思
- 高通
- 中兴微电子
- RDA
- 英特尔
- …

NB-IoT的应用


SMART TRAVEL COMPANION WITH NB IOT
Minifly Module
With NB-IOT
LOCATION TRACKING
PROXIMITY ALERT
DIGITAL LOCK
BATTERY MONITORING
WIRELESS CHARGING
Smart Suitcase
LOCKED
FIREFLY
HUAWEI

NB-IoT的应用


Smart Tracking on Bicycle
Body Monitoring
(Calorie, Hart Rate)
NB IOT Embedded
Lock Control &
Status Monitoring
Tire Pressure
Monitoring
Travel Recording & Sharing
(Distance, Route)
Location Tracking
DAHON
freedom unfolds
HUAWEI

NB-IoT安全问题

数据安全及隐私:公网传输导致重要数据泄露风险
通信安全:通信网络面临复杂攻击的风险
设备安全:设备规模巨大易引发大规模网络攻击
参考: Mirai botnet DDoS attack

Ref: 中国移动NB-IoT白皮书
http://iot.10086.cn:81/Uploads/file/20171222/20171222084728_77259.pdf

IoT Security: Mirai Botnet Example

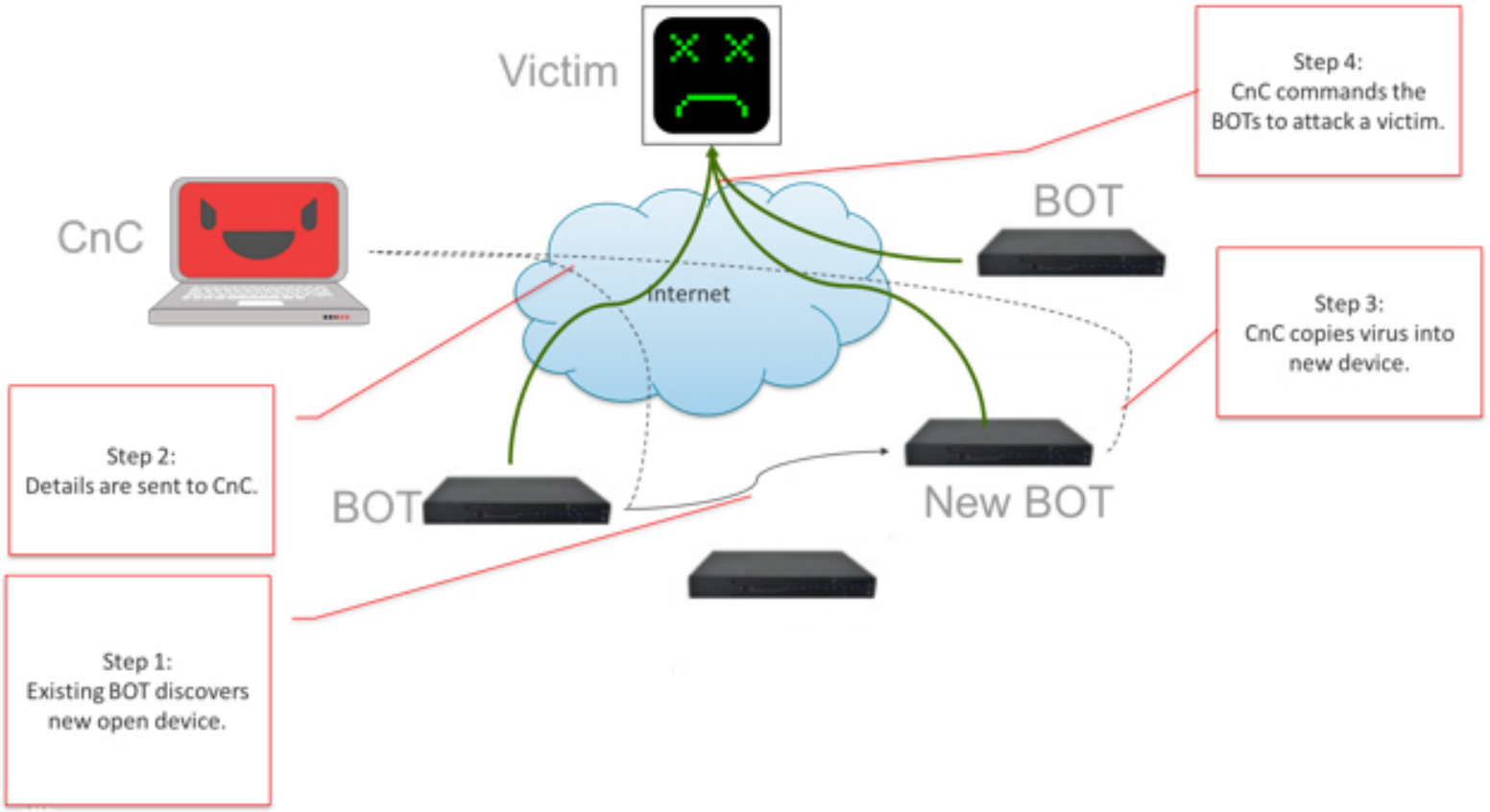


Figure 1 Mirai System