5G Trends, Challenges, and Technology

(5G + IoT = The *Internet of Tomorrow*)

Richard D. Gitlin

Distinguished University Professor

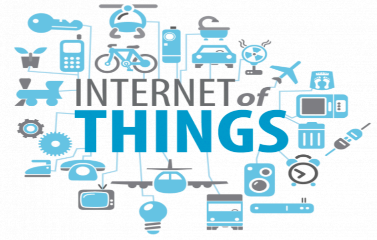
University of South Florida

April 12, 2016

Slides at iwinlab.eng.usf.edu

5G Trends, Challenges, and Technology

+



=>***Internet of Tomorrow***

- 5G Vision and Drivers
- Application Scenarios and Requirements
- Standards and Spectrum Availability
- 5G ***Revolution***
  - Network Architecture and Protocols
  - Software-based Networking
  - Enabling Technologies and Research Issues
  - Internet of Things --- IoT
- Concluding Remarks
  - Skeptics View of 5G/IoT
  - A New Era of Connectivity

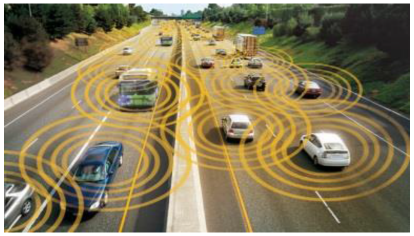
5G Vision

Heterogeneous, Revolutionary, and a Green Ecosystem

- **Physical Layer: 10Gbps** mobile data, dynamic "cell" and spectrum utilization
- **HetNet "cells":** Macro→ femto cells, many RF technologies, *OFDM*+, WiFi, BLE, **mmWave small cells** and distributed radio elements
- **Software-based network:** SDN/NFV low cost customizing of emerging services
- **Internet of Things (IoT):** wireless networking of diverse objects and applications
- **Tactile Internet:** Low-latency wireless access (e.g., autonomous cars) ~1ms

5G use cases

Gbps Mobile Data/Video
(Cellular, HetNets)



Vehicular Networks
(Autonomous cars→ **Tactile Internet**)

Content Delivery

Cloud Services

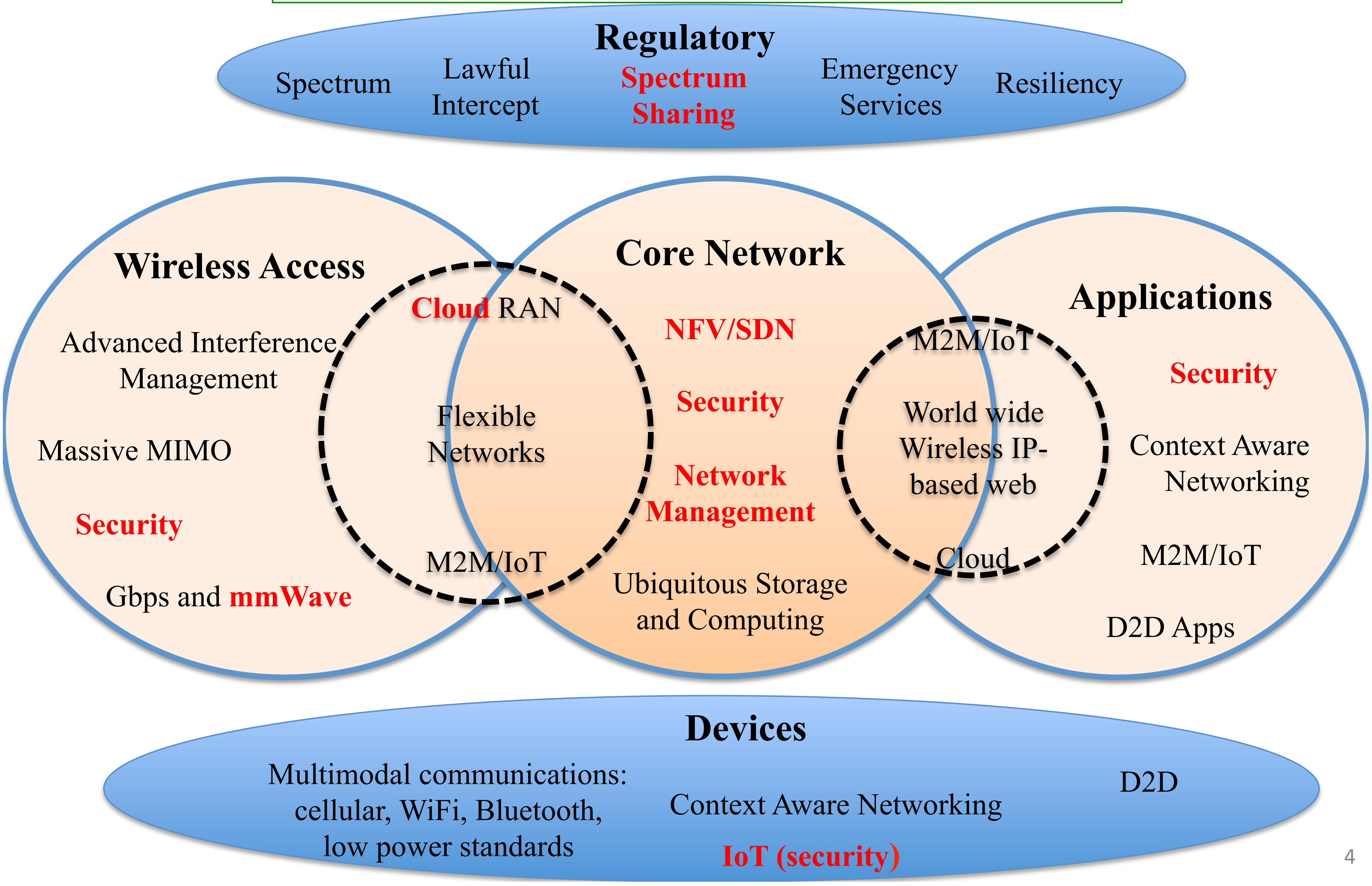
SDN =Software Defined Network
NFV = Network Function Virtualization

Emergency Networks

Internet of Things

Functional View of the 5G Ecosystem

Green philosophy: energy, spectrum, and cost efficiency



Regulatory

Spectrum

Lawful Intercept

Spectrum Sharing

Emergency Services

Resiliency

Wireless Access

Advanced Interference Management

Massive MIMO

Security

Gbps and **mmWave**

Cloud RAN

Flexible Networks

M2M/IoT

Core Network

NFV/SDN

Security

Network Management

Ubiquitous Storage and Computing

M2M/IoT

World wide Wireless IP-based web

Cloud

Applications

Security

Context Aware Networking

M2M/IoT

D2D Apps

Devices

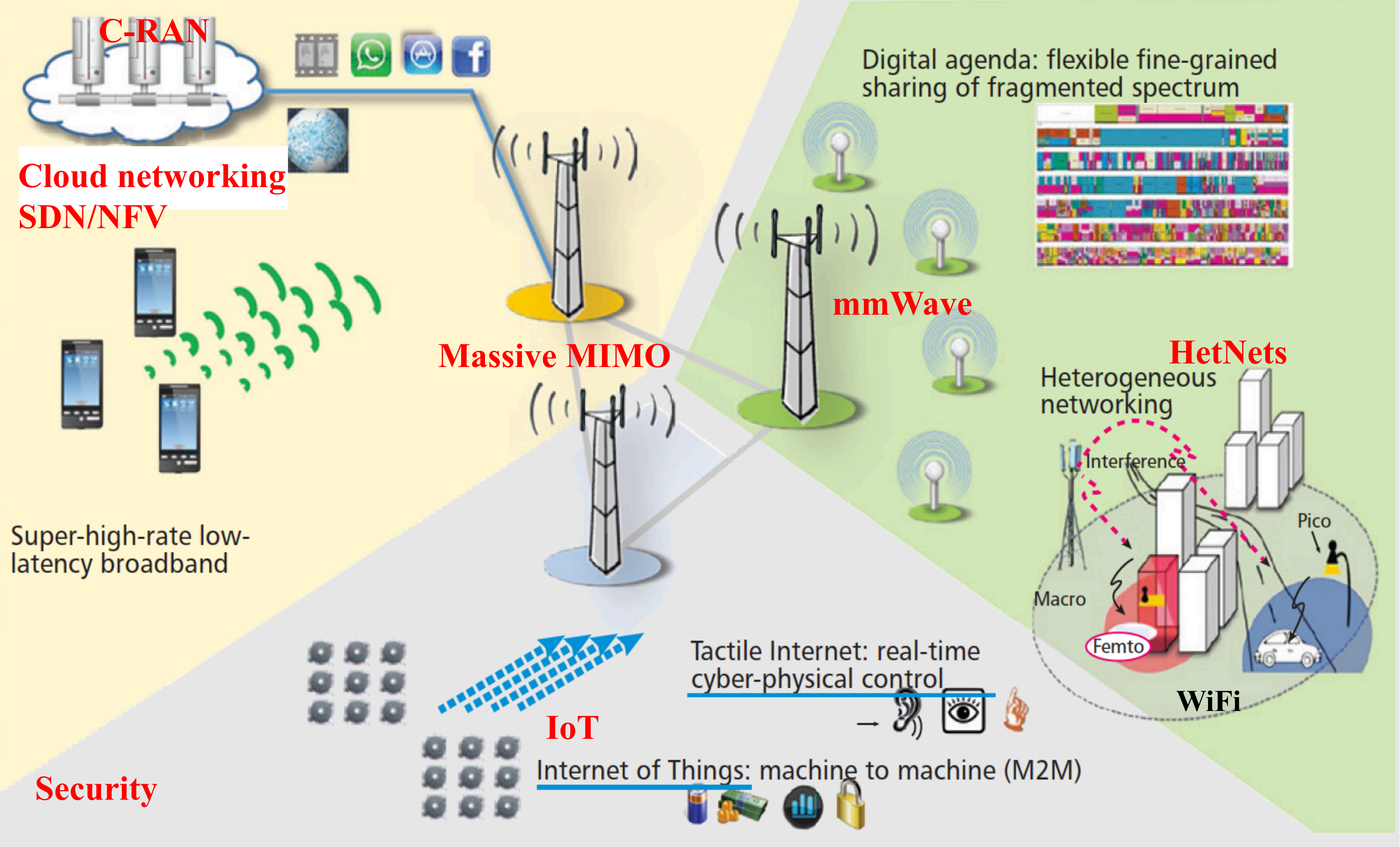
Multimodal communications: cellular, WiFi, Bluetooth, low power standards

Context Aware Networking

IoT (security)

D2D

System View of 5G Heterogeneous Network (2020?)


C-RAN
Cloud networking
SDN/NFV
Digital agenda: flexible fine-grained sharing of fragmented spectrum
mmWave
Massive MIMO
HetNets
Heterogeneous networking
Interference
Pico
Macro
Femto
WiFi
Super-high-rate low-latency broadband
Tactile Internet: real-time cyber-physical control
IoT
Internet of Things: machine to machine (M2M)
Security

- Heterogeneous broadband network – HetNet: wireless network with multiple types of access nodes (macrocells, picocells, and/or femtocells + WiFi and Bluetooth).
- Software-based core network: SDN/NFV
- Integration of **5G** and the **Internet of Things [IoT]** → **Internet of Tomorrow**

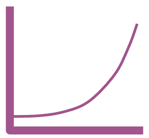
5G Drivers

5G + IoT → *Internet of Tomorrow*

Avalanche of
Traffic Volume

Dramatic expansion of mobile broadband (video)

Additional traffic due to communicating machines



1000x in ten years

Massive growth in
Connected Devices
"Communicating machines"

50 billion devices in 2020

IoT

Large diversity of
Use Cases and Requirements

Device-to-Device Communications

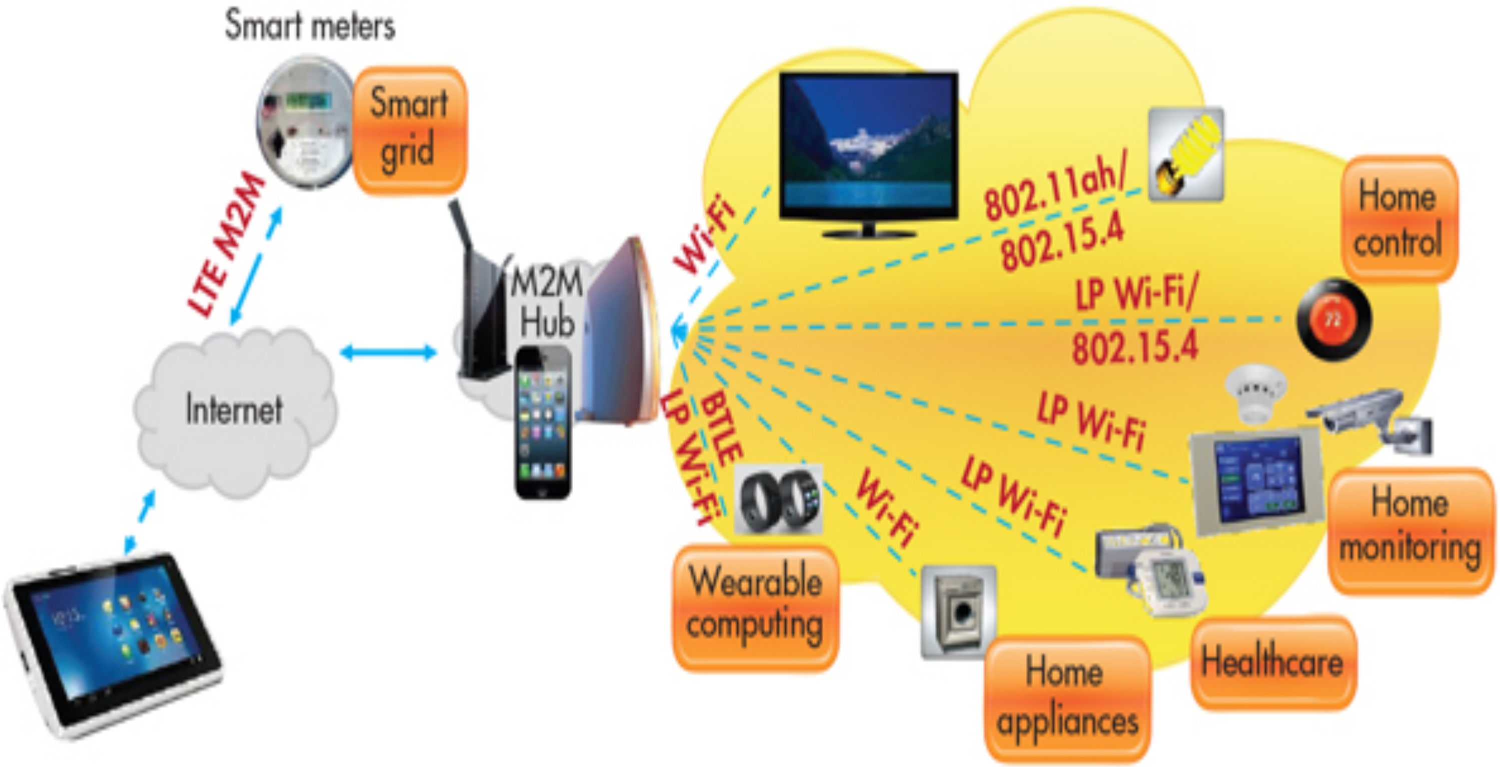
Car-to-Car Communications

(ms) Low latency---**Tactile Internet**

New requirements and characteristics due to communicating machines

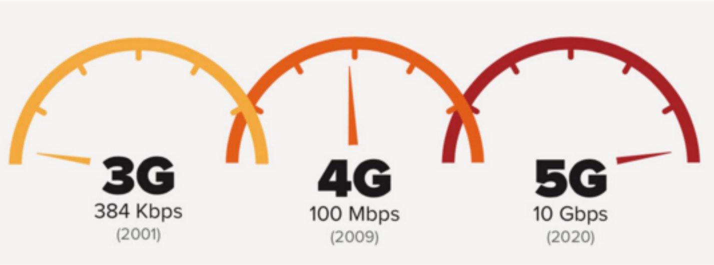
The Internet of Things (**IoT**) is the intelligent connectivity of physical devices

Internet of Things [IoT]
Connectivity for Everyone and Everything



- The **IoT** is an ecosystem of physical objects, devices, vehicles, and all kinds of objects that embed electronics, software, sensors and network connectivity.
- Content delivered everywhere, streamed from the cloud, from smartphones, smart watches, tablets, multimedia, home automation, security, and eHealth.
- Likely that several [many?] connectivity standards will coexist.
- IoT security a major issue

5G Application Requirements and Challenges



Key Application Requirements

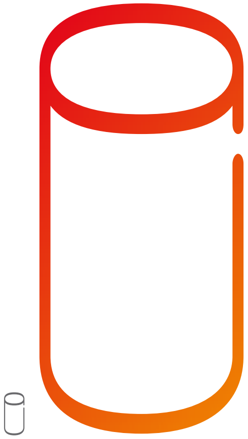
- **Gigabit wireless connectivity**: For quick downloads of 3D streaming content (e.g., from a wireless data kiosk, augmented/virtual reality) on the order of ~**10 Gb/s**.
- **Internet of Things (IoT)**: The major challenges are scalability and security with more than **100K** machine-type communication (MTC) nodes expected in a cell.
- **Tactile Internet**: Real-time applications, such as autonomous vehicles, robotics, and healthcare/surgery, with extremely low latency requirements compatible with the **1ms** tactile sensitivity of the human body.
- **Security and Authentication**: New challenges for a networked society

Research Directions: 5G demands a complete network overhaul to meet the new network requirements and associated challenges.

- **Software-driven networking**: SDN and NFV that enable adaptive and customizable networking and effective network management.
- Dynamic, dense, low latency, high capacity and heterogeneous IP-based networks.
- **Higher capacity** networks: mmWave systems, Massive MIMO, cognitive systems.
- **Security and Authentication** for Device-to-Device, IoT, and networked systems with new models of trust and service delivery in an evolved threat landscape.

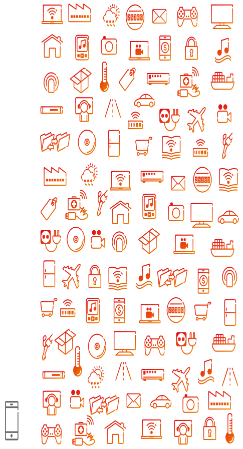
5G’s Ambitious Technical Objectives

1000x data volume



1000x
higher mobile data volumes

50/500 B devices

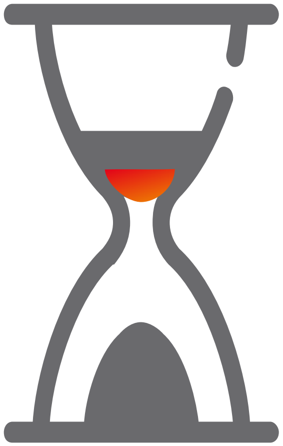


10-100x
higher number of connected devices

Up to 10Gbps

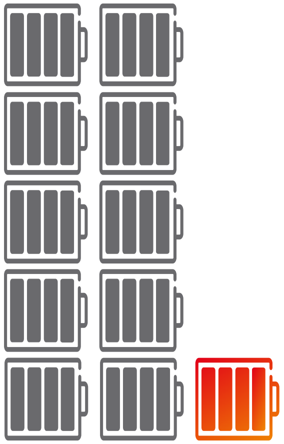
10-100x
typical end-user data rates

Few ms E2E



5x
lower latency (1ms target)

10 years



10x
longer battery life for low-power devices

Plus: Security, Network Management, IoT integration, …

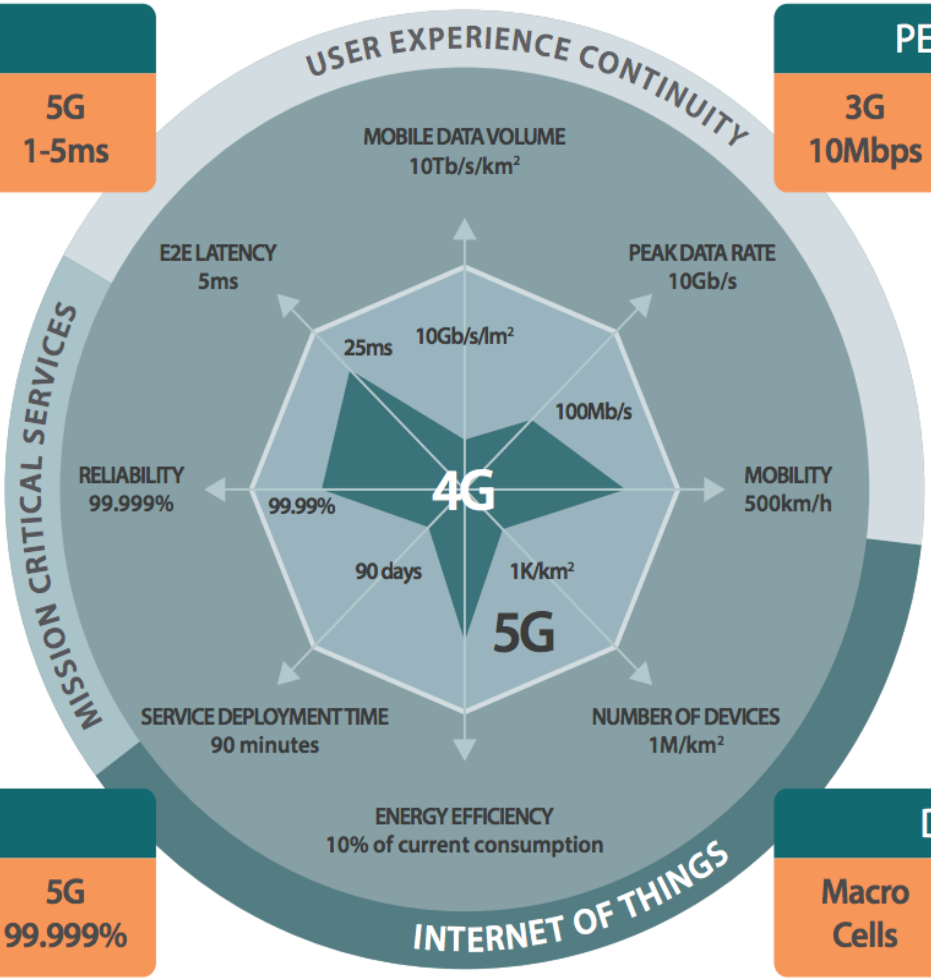
5G Network Management Challenges

- With a mixture of macrocell towers, small cells, possibly customer-installed tiny cells, WiFi hotspots, and peer-to-peer [D2D and M2M] and IoT connections, network management becomes a greater challenge.
- The service expectation is that all 5G users should always have up to their full 10 Gbps available on demand, with imperceptible latency.
- 5G nodes may be arranged fundamentally differently from today's 4G topologies --- almost at random rather than in geographic/cellular patterns and communicating with multiple "base stations" (no more cells???).
- Different nodes will support different combinations of spectral bands, and may have different levels of MIMO/beamforming capability.
- Many of the users will be moving --- some of the most critical, like automated vehicles, will move quite rapidly.
- As IoT moves from promise to reality, there will be10 to 100 times that many devices to manage [just in the business world].
- **Successful connection management and optimization algorithms remain to be demonstrated, whether for centralized or distributed control --- IoT will add a new dimension.**

5G Network Expectations/Requirements

E2E LATENCY		
3G	4G	5G
100ms	25ms	1-5ms

PEAK BANDWIDTH		
3G	4G	5G
10Mbps	100Mbps	1000Mbps



RELIABILITY		
3G	4G	5G
99.9%	99.99%	99.999%

DENSIFICATION		
Macro Cells	Small Cells	Femto WiFi

- **5G** widespread gigabit wireless connectivity [cellular, WiFi, …]
- The **Internet of Things** --- connectivity for everyone and everything
- **5G revolution re 4G: speeds, frequencies, latency, SW-based, Hetnets, …**

5G Standard(s)

5G

International Standards Initiatives + Industry Groups + Proprietary

ETSI Summit 2016

5G: from Myth to Reality

IEEE

P241 and IEEE 802.11ah

http://iot.ieee.org/

ngmn

the engine of broadband wireless innovation

IEEE

Internet of Things

atis

OPEN INTERCONNECT

CONSORTIUM

INTERNET OF THINGS

IoT-GSI

GLOBAL STANDARDS INITIATIVE

ITU-T

ITU-T Y.2060

Committees & Forums

5G

OMG®

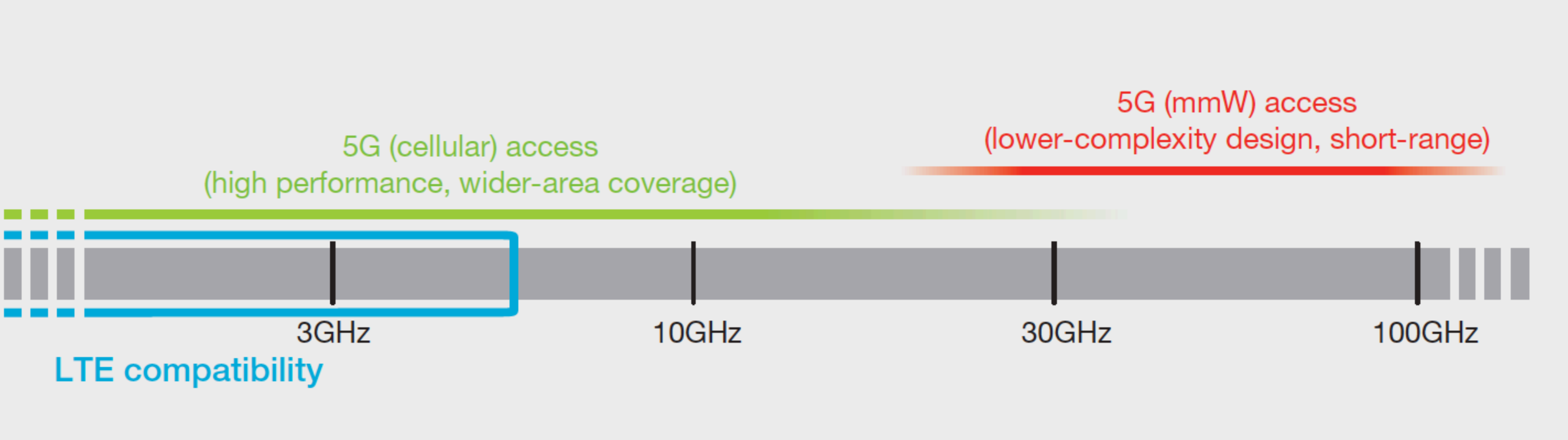
OBJECT MANAGEMENT GROUP®

ALLSEEN ALLIANCE

LINUX FOUNDATION

AllJoyn® Framework

5G Spectrum


5G (mmW) access
(lower-complexity design, short-range)
5G (cellular) access
(high performance, wider-area coverage)
3GHz
10GHz
30GHz
100GHz
LTE compatibility

- Spectrum up to 100GHz is being considered for use by 5G mobile systems.
- Propagation characteristics, implementation, and compatibility issues imply that the 5G wireless-access solution will most likely consist of multiple radio interfaces.
- OFDM-based transmission technology will still be a good baseline, although the details will probably need to be adjusted for frequencies above 10GHz.
- For higher frequency bands – a few tens of GHz and above – propagation characteristics and implementation aspects will likely dictate a more simplified radio-interface structure targeting short-range communication for ultra-dense deployments.

5G Spectrum: Flexible Access Below 6 GHz

- Flexible to support diverging requirements in the same spectrum
- Multiple operating modes (FDD/TDD, indoor/outdoor, star/mesh/D2D)

Enhanced Mobile Broadband

- Macro and small cells
- 1 ms Latency (air interface)
- Spectrum allocated at WRC-15 may lead up to 8Gbps of additional throughput
- Support for high mobility

Low Power & Complexity

- Low data rate (1~100kbps)
- High density of devices (up to 200,000/km^2)
- Latency: seconds to hours
- Low power: up to 15 years battery autonomy
- Asynchronous access

Ultra-High Reliability & Ultra-Low Latency

- Low to medium data rates (50kbps~10Mbps)
- <1 ms air interface latency
- 99.999% reliability and availability
- Low connection establishment latency
- 0-500 km/h mobility

Source: InterDigital

5G Ultra Broadband above 6 GHz (Indoors and Hotspots)

- Frequencies above 6 GHz suffer from much higher path los
- Massive antenna arrays are feasible due to shorter wavelength
  - Leads to compact antenna array structures
  - Beamforming gains overcome high path loss

Free-Space Path Loss

Distance	2.4GHz	28GHz	60GHz
d = 1m	-40 dB	-62 dB	-68 dB
d = 100m	-80 dB	-102 dB	-108 dB

28 dB

- **NO new spectrum allocated to date for 5G**. The next meeting to talk about spectrum allocation will take place at the World Radio Communication Conference (WRC-2019)
- Recommendation from WRC-15 related to 5G mmWave frequency ranges and bands:

24.25 to 27.5 GHz
37.0 to 43.5 GHz
50.4 to 52.6 GHz
81 to 86 GHz

31.8 to 33.4 GHz
45.4 to 50.2 GHz
66 to 76 GHz

Key Requirements

- 20 Gbps (peak user throughput)
- 1 ms Latency (air interface)
- Standalone and/or macro-assisted access
- Joint access/backhaul

Source: InterDigital

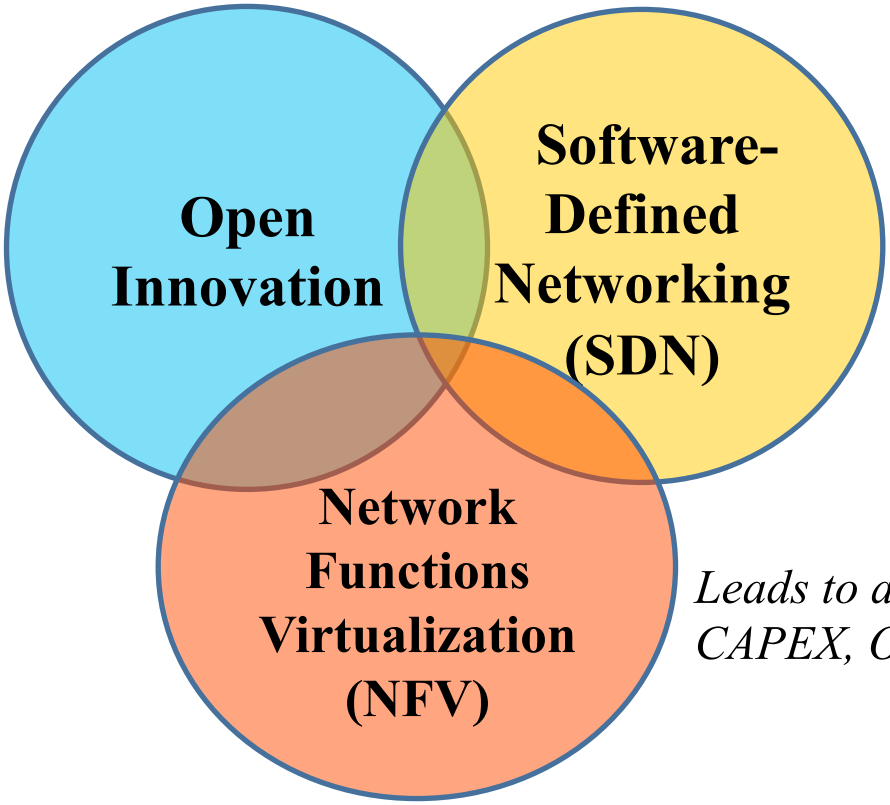
Key Enablers

- Large amounts of spectrum
- Massive antenna arrays
- Cell densification

Key Challenges

- Timely availability of globally harmonized spectrum
- Low-cost & low-complexity implementations
- Discovery & initial access
- Frequent & abrupt loss of radio link(s)

5G Strategic Networking Paradigms



Open Innovation

Software-Defined Networking (SDN)

Network Functions Virtualization (NFV)

Creates competitive supply of innovative applications by third parties

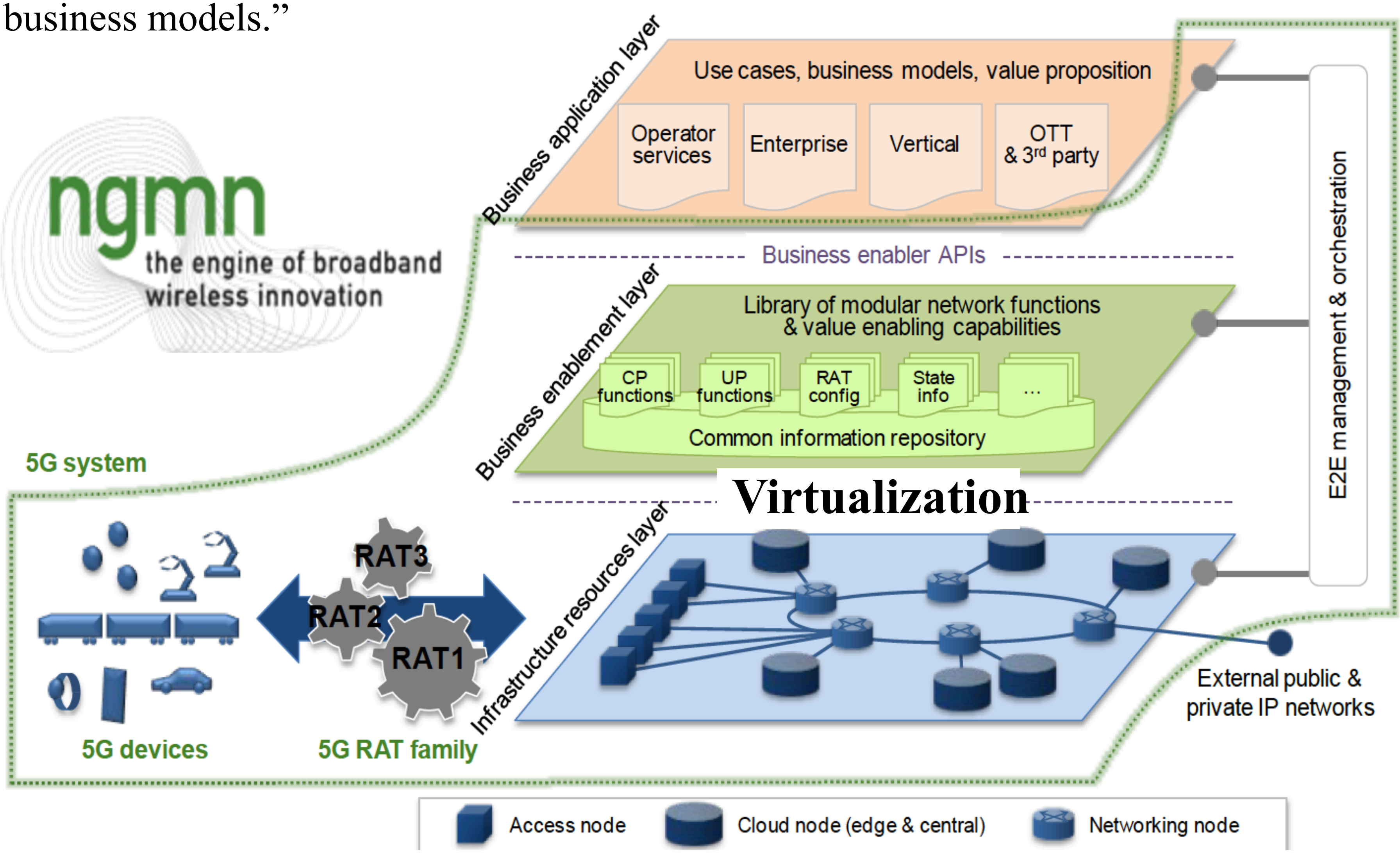
Creates network abstractions to allow application-aware behaviour, and increased flexibility

Leads to agility, Reduces CAPEX, OPEX,…

- SDN: Separate CONTROL and DATA plane
- NFV: Separate SERVICE logic from HW Platform
- NFV and SDN are highly complementary. They are mutually beneficial but not dependent on each other (NFV can be deployed without SDN and vice-versa)
- SDN can enhance NFV performance, simplify compatibility, facilitate operations
- NFV aligns closely with SDN objectives to use **software, virtualization and IT management techniques in 5G.**

NGMN Vision: A Baseline for 5G Architecture Discussion

“5G is an end-to-end ecosystem to enable a fully mobile and connected society. It empowers value creation towards customers and partners, through existing and emerging use cases, delivered with consistent experience, and enabled by sustainable business models.”

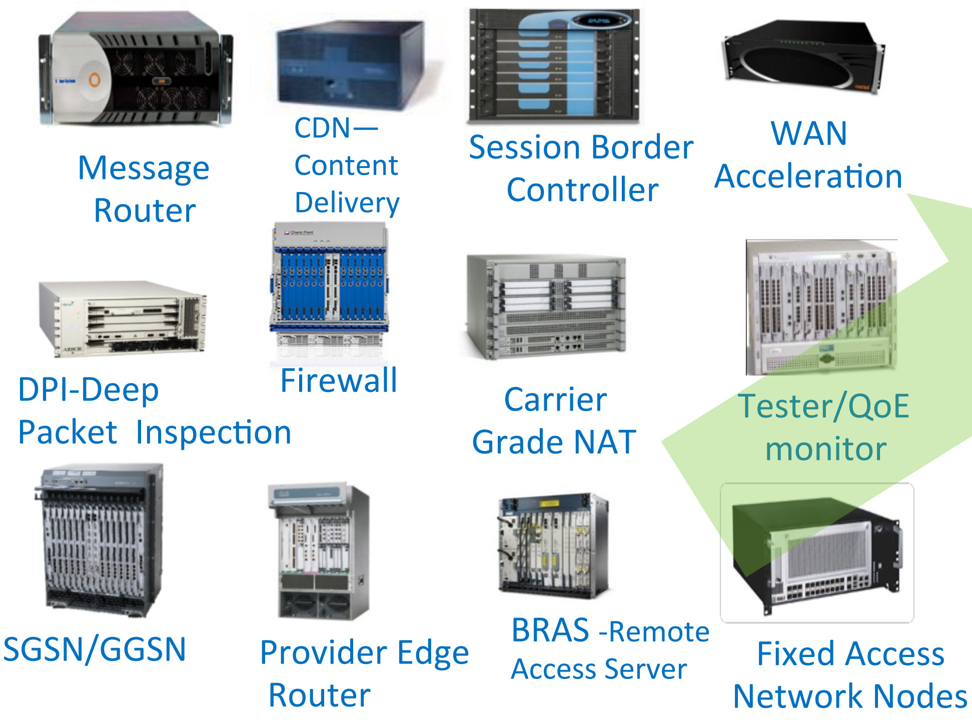


Business application layer
Use cases, business models, value proposition
Operator services
Enterprise
Vertical
OTT & 3rd party
Business enabler APIs
Business enablement layer
Library of modular network functions & value enabling capabilities
CP functions
UP functions
RAT config
State info
…
Common information repository
Virtualization
Infrastructure resources layer
E2E management & orchestration
External public & private IP networks
ngmn
the engine of broadband wireless innovation
5G system
5G devices
RAT3
RAT2
RAT1
5G RAT family
Access node
Cloud node (edge & central)
Networking node

Network Functions Virtualization [NFV]

Becoming a Software-Based Network

Classical Network Appliance Approach



Message Router

CDN—Content Delivery

Session Border Controller

WAN Acceleration

DPI-Deep Packet Inspection

Firewall

Carrier Grade NAT

Tester/QoE monitor

SGSN/GGSN

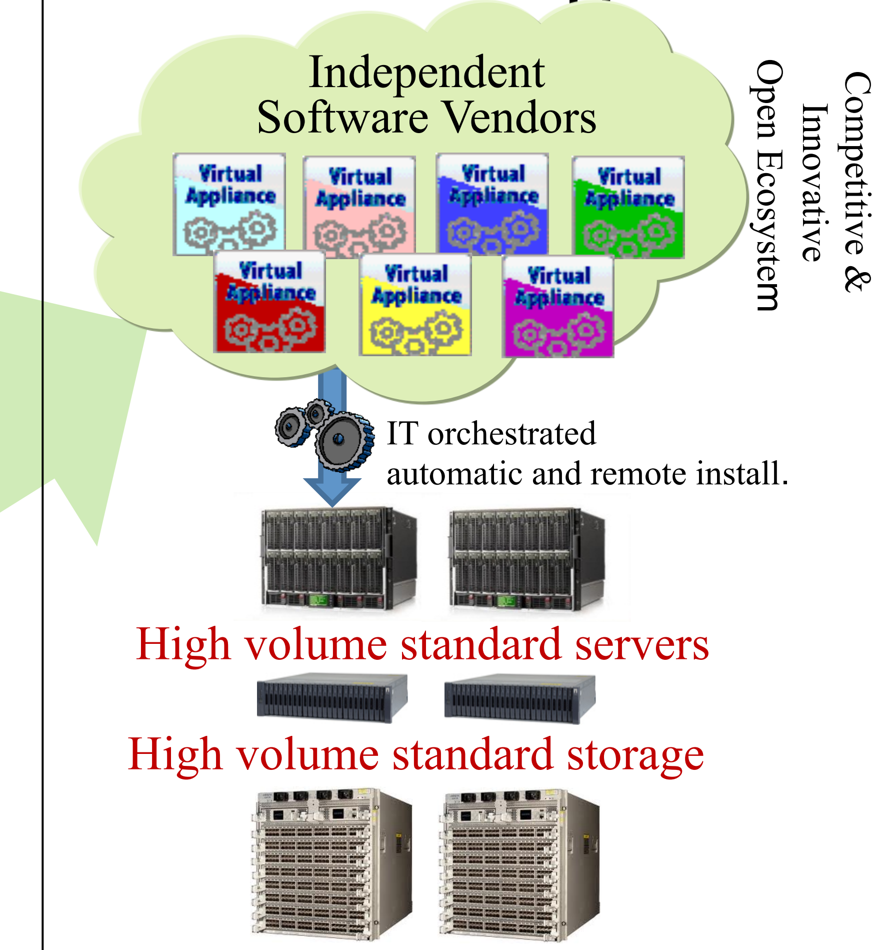
Provider Edge Router

BRAS -Remote Access Server

Fixed Access Network Nodes

- Fragmented, purpose-built hardware.
- Physical install per appliance per site.
- Hardware development large barrier to entry for new vendors, constraining innovation and competition.

Network Functions Virtualization Approach



Independent Software Vendors

Competitive & Innovative Open Ecosystem

IT orchestrated automatic and remote install.

High volume standard servers

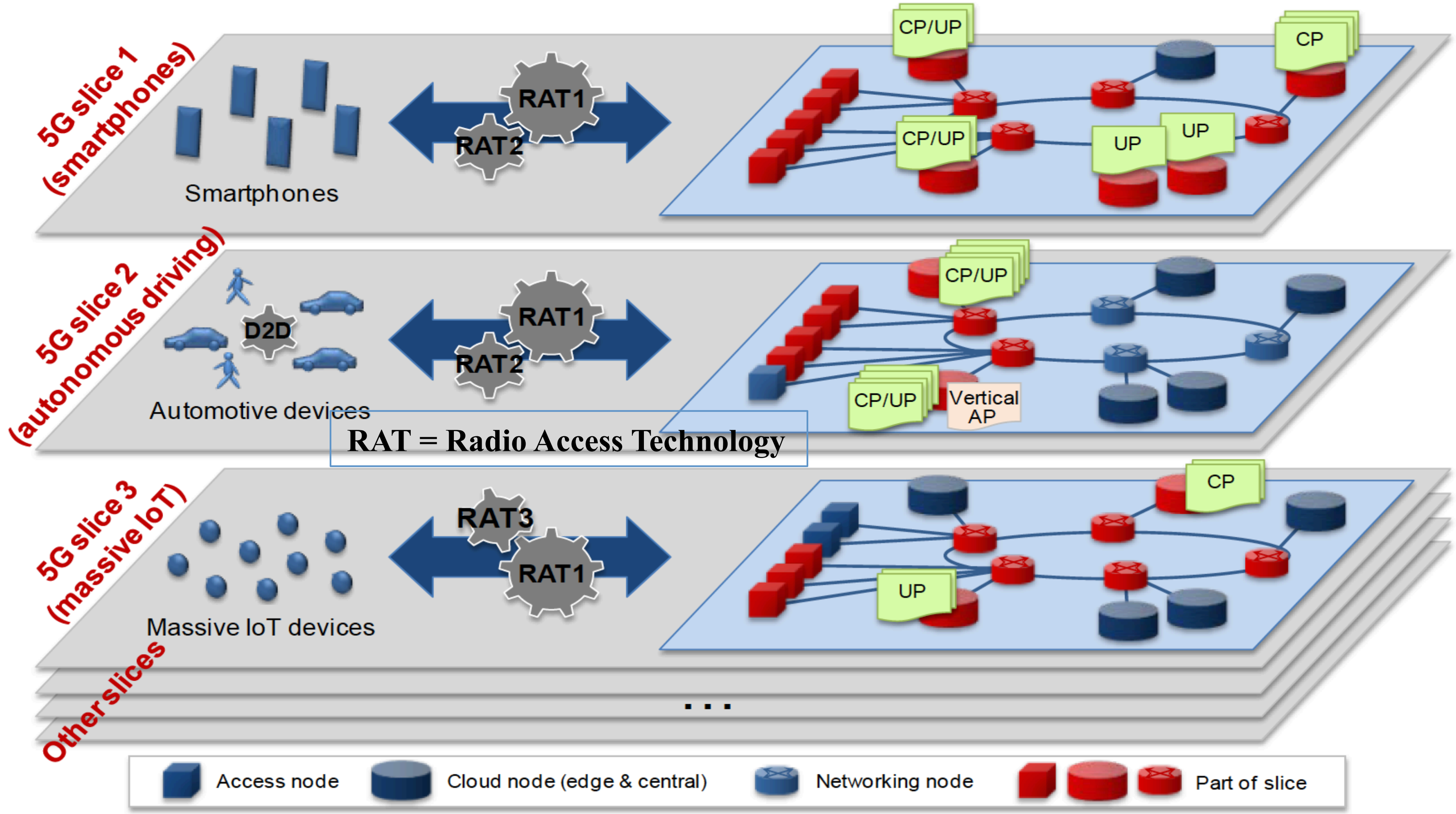
High volume standard storage

High volume Ethernet switches

NFV: network functions in SW leverage (high volume) standard servers and virtualization

5G NFV: Network Slicing

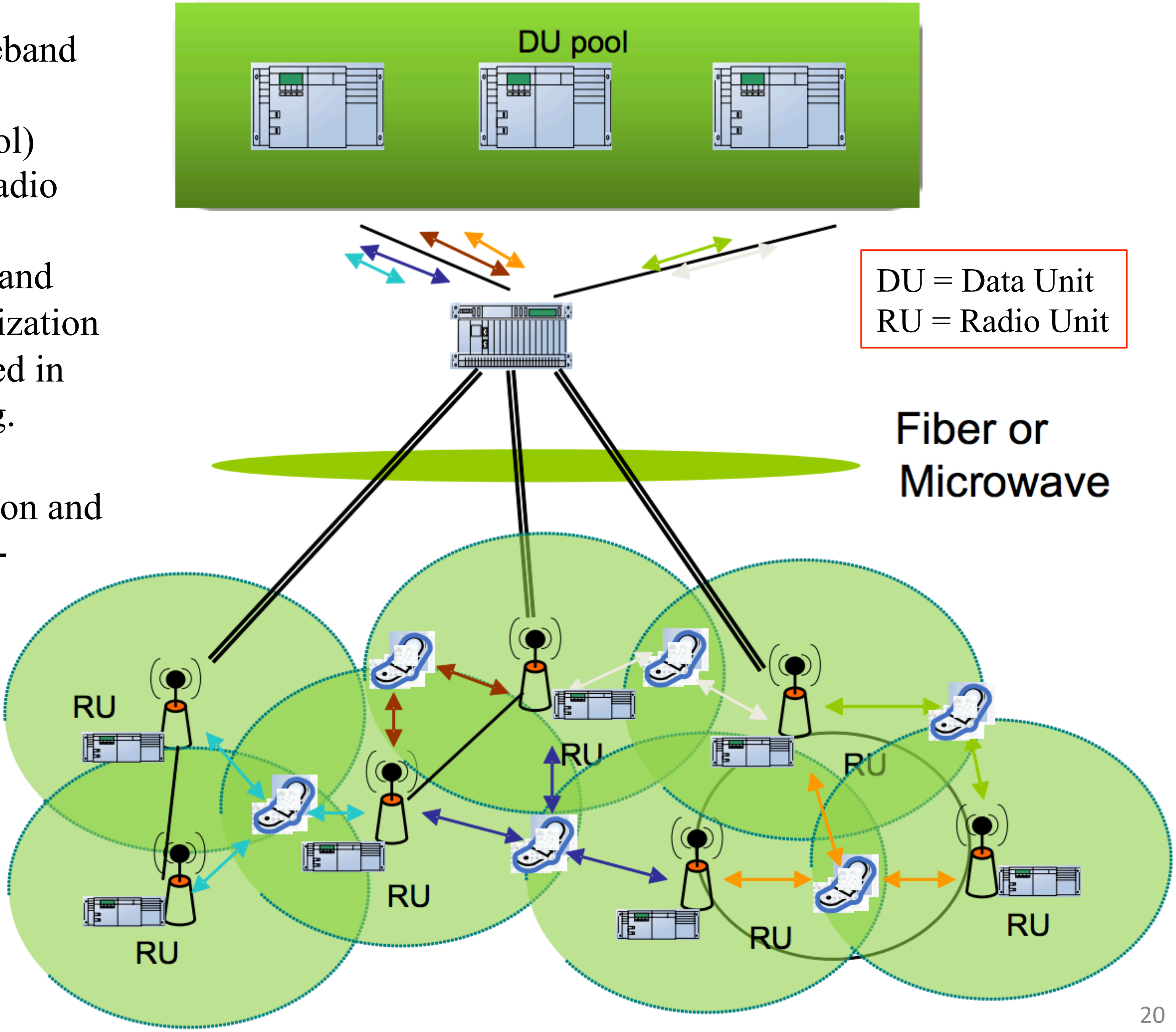
- A network slice is an end-to-end logically isolated network including devices, access, transport and (virtualized) core network functions to support diverse scenarios on a common infrastructure.
- Enables operators to launch a range of highly differentiated network services, each aimed at a distinct vertical market but relying on the same infrastructure.



RAT = Radio Access Technology

5G Centralized/Virtualized RAN: C-RAN

- Centralized baseband processing pool (Digital Unit pool) separate from Radio Unit (RU).
- Open platforms and real-time virtualization technology rooted in cloud computing.
- Dynamic shared resource allocation and support of multi-vendor, multi-technology environments.
- Mesh network architecture



DU = Data Unit
RU = Radio Unit

5G Emerging Technologies in the Wireless Access Network

Advanced waveforms

Alternatives to pure OFDM such as RBF-OFDM, FBMC, GFDM, and UFMC, are motivated for better spectrum containment and asynchronous (non-orthogonal) sharing scenarios in 5G.

Advanced MIMO

The use of a very large number of antennas is proposed as a means to achieve very high throughput and spectral efficiency per area. Both co-located and distributed architectures are envisaged, with co-located massive MIMO particularly appealing to high frequency bands (thanks to the narrow beams and small form factor).

Millimeter Wave

Millimeter Wave spectrum (up to 100 GHz) offers large chunks (up to 2GHz) of contiguous bandwidth, which makes it suitable for ultra-high throughput and low latency scenarios.

5G Emerging Air Interface [PHY] and Multiple Access Technologies

PHY Goals: Alternative to or enhancements of OFDM to improve spectral efficiency, reduce peak-to-average power ratio [PAR], work well in higher frequency bands.

Multiple Access Goals: 5G multiple access technologies should provide higher network spectral efficiency; the performance gap between cell-center and edge users should be reduced, and the number of simultaneous (access) users could be increased.

Advanced waveforms and multiple access

- More flexible waveforms than pure OFDM (e.g., RBF-OFDM; FBMC; etc.)
- Non-orthogonal multiple access (NOMA)
- Broader set of modulation and coding schemes

Advanced antenna and multi-site technologies

- 3D-beamforming and MU-MIMO
- Massive MIMO
- Network MIMO (Advanced Coordinated Multipoint --CoMP)

Novel duplexing schemes

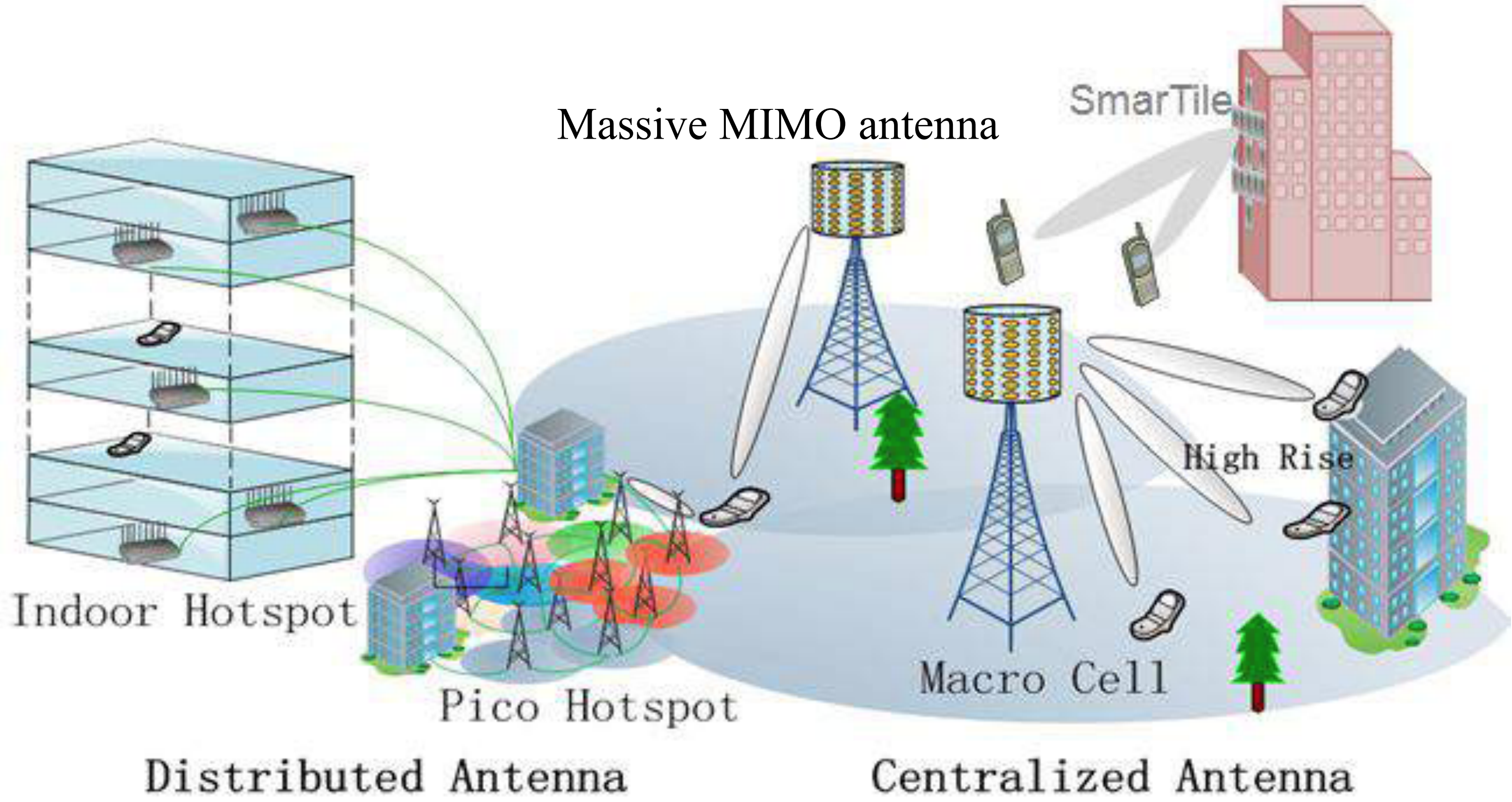
- Joint TDD-FDD operation
- Dynamic TDD
- Single channel full duplexing

New and flexible spectrum usage

- New large spectrum at mmW frequencies
- Carrier Aggregation of discontinuous bands
- Dual-band split user and control plane
- Joint multi-RATs management
- Cognitive techniques (spectrum sensing)

RBF-OFDM = Resource-Block-Filtered OFDM: signal divided into resource blocks that are individually filtered.
FBMC = Filter Bank Multi-Carrier: FIR filtering of OFDM sub-channels

Massive MIMO [M-MIMO] Scenarios



- M-MIMO cell sites can aim narrow beams at specific clients to improve throughput and reliability.
- Base stations with ~ 128 antennas and as many as practical in the phone.
- M-MIMO can also help with security for the Internet of Things [IoT].

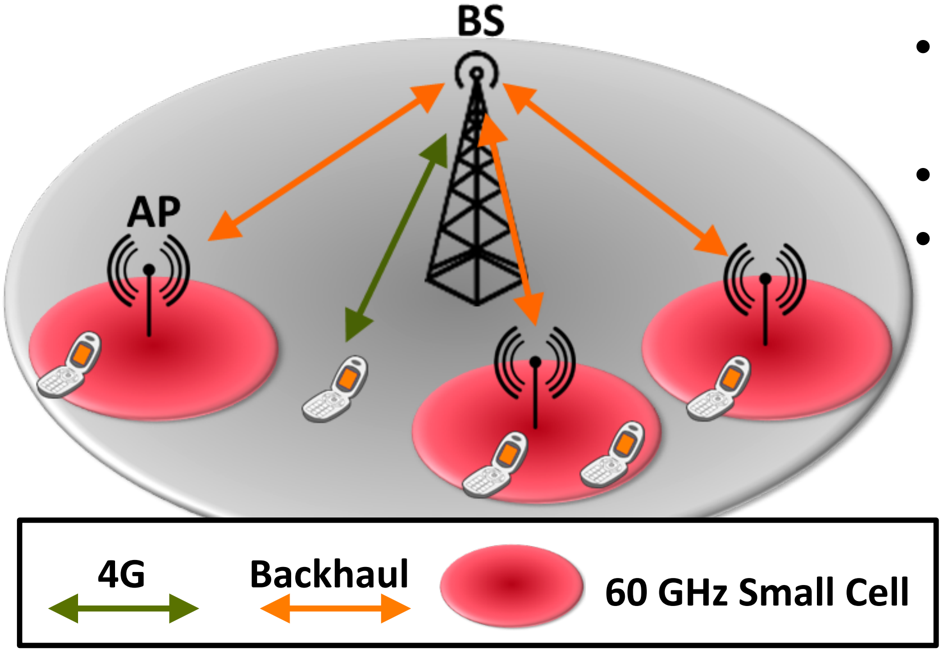
mmW HetNets

Heterogeneous Networks: small cells within macro cells

- Improve user data rate near the access point
- Offload data from the macro cell to the small cell
- Reduce transmit power (terminal and BS)
- Flexible deployment in dense areas

Millimeter-wave small cells

- Supports wireless backhaul and 5G access
- 100x-1000x growth potential!
- Spectrum resources available worldwide (60 GHz, 71-86 GHz)
- Multi-Gbps data rates
- No interference with macro cell



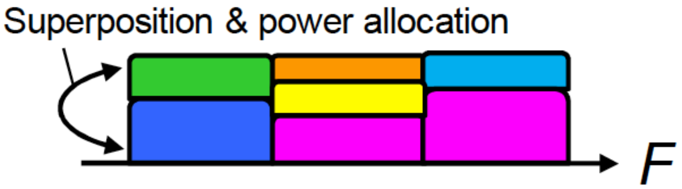
Challenges for mmW Access

- **Radio**: Lower Tx power and Rx sensitivity
- **Antennas**: Directive antennas with beamforming
- **Propagation**: Building penetration, blockage effects, foliage, precipitation

Non-Orthogonal Multiple Access [NOMA]

User multiplexing	Non-orthogonal with SIC (NOMA)
Signal waveform	OFDM (or DFT-s-OFDM)
Link adaptation	AMC + Power allocation

AMC = Adaptive Modulation and Coding
SIC = Successive Interference Cancellation



- 4G orthogonal multiple access: avoids interference and leads to high system capacity.
- For rapid access of small payloads, the procedure to assign orthogonal resources to different users may require extensive signaling and lead to additional latency.
- Research in non-orthogonal multiple access [NOMA], as a complement to orthogonal access, is being considered for 5G.
- Advanced interference cancellation should/must be carried out/implemented on receiver side. Power allocation and multi-user scheduling may be needed at the transmitter side.

WiFi Devices Are Being Developed with mmWave Capabilities

- Qualcomm Atheros packages its AR9642 802.11n transceiver with the **Wilocity 60-GHz chip**, forming a module that covers the three Wi-Fi bands of 2.4, 5, and 60 GHz.
- Millimeter waves [30-300 GHz] permit high data rates that can reach 10 Gbits/s and more.
- A typical half-wave dipole at a cellular frequency like 900 MHz is six inches long, but at 60 GHz one half-wave is only about 2.5 mm in free space and even less when it's made on a dielectric substrate.
- This means the entire structure of a radio including the antenna can be very small. It's easy to make multiple-element phased arrays on a substrate chip that can steer and focus the energy for greater gain, power, and range and compensate for the increased attenuation of mm waves.

5G Security

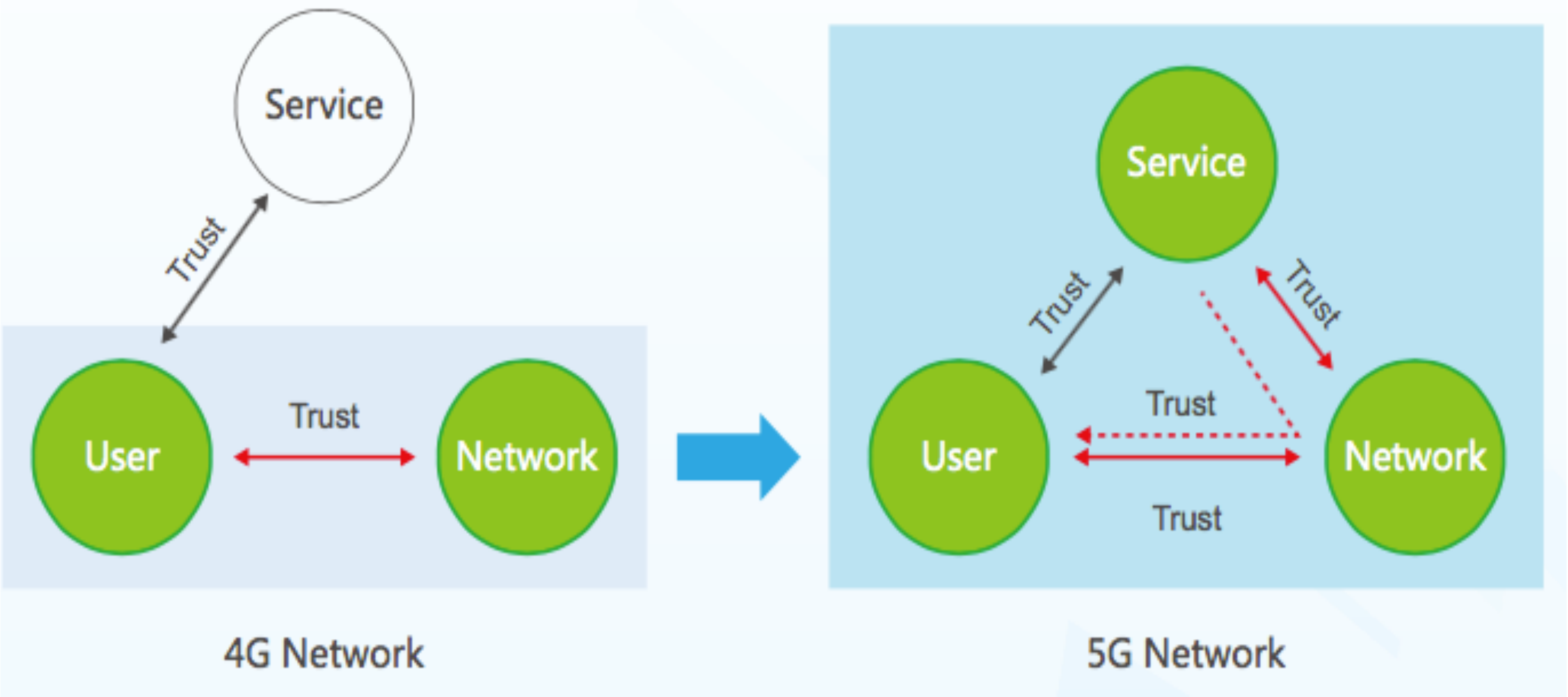
A fundamental capability that networks provide to their customers

CYBER-SECURITY

- 5G will support a wide range of data that needs to be protected against unauthorized access, use, disruption, modification, inspection, etc.
- 5G should provide options beyond node-to-node and end-to-end security available in today's mobile systems, in order to protect users' data against a cyber-security attack.
- Main features [and research challenges]
  - Subscriber Authentication and Key Distribution --- BIG challenges with IoT
  - User Privacy --- provide security mechanism for protection of a variety of trusted information regarding human and machine users
  - Beyond Hop-by-Hop Security --- bearer-independent (e.g., higher layer) security, and extending to network servers, and to device-to-device communications
  - Radio access
    - Improve system robustness against smart jamming, man-in-the-middle attacks
    - Improve security of 5G small cell nodes, taking into consideration their geographical distribution and their easy accessibility
  - Core network
    - Improve resilience and availability of the network against signaling based threats
    - Specific security design for use cases which require extremely low latency

Security Unique to 5G

- **New Trust Models and Identity Management:** Networks need to cooperate with service providers to establish secure and efficient ways of identity management.

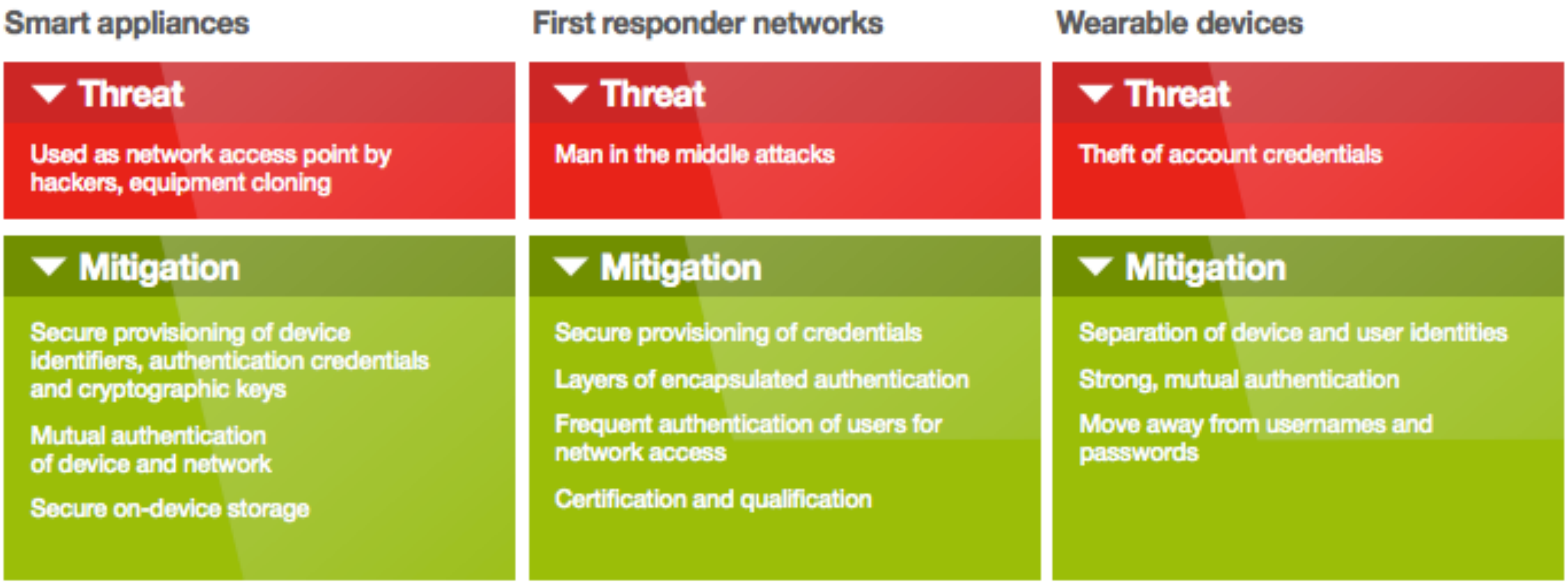


- **Hybrid Authentication:** Authentication by network only, service only, or both.
- **Diverse Identities:** SIM cards in legacy systems, but wide range of 5G nodes (such as wearable devices, smart home appliances) will not have such cards.
- **End-to-end Security and Virtual Network Isolation:** Prevent other applications and other users within the same segment to access user data.

Continued →

Security Unique to 5G --- continued

- **Low Delay Mobility Security:** Applications with delay requirements <1ms and high reliability (e.g., vehicle-to-vehicle applications)
  ➔ Efficient and lightweight solutions are needed
- **User Privacy Protection**: Health data, location, etc.
  - While user data is processed and transferred from different access networks and network functionalities, user’s privacy information should not be compromised

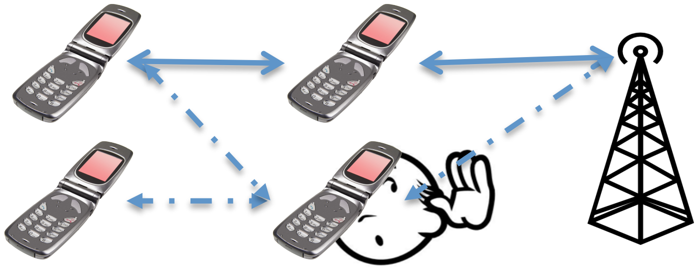


Smart appliances	First responder networks	Wearable devices
▼ Threat	▼ Threat	▼ Threat
Used as network access point by hackers, equipment cloning	Man in the middle attacks	Theft of account credentials
▼ Mitigation	▼ Mitigation	▼ Mitigation
Secure provisioning of device identifiers, authentication credentials and cryptographic keys Mutual authentication of device and network Secure on-device storage	Secure provisioning of credentials Layers of encapsulated authentication Frequent authentication of users for network access Certification and qualification	Separation of device and user identities Strong, mutual authentication Move away from usernames and passwords

Figure from http://simalliance.org/wp-content/uploads/2016/02/SIMalliance_5GWhitepaper_FINAL.pdf

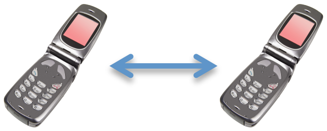
Physical Layer Security

Advantages over Classic Cryptography



- PHY layer security does not depend on adversary's computational complexity
- Cryptographic key distribution and management is challenging in the dynamic and heterogeneous nature of 5G
  - PHY-layer security can enable direct secure data communication and/or can facilitate the distribution of cryptographic keys in 5G network

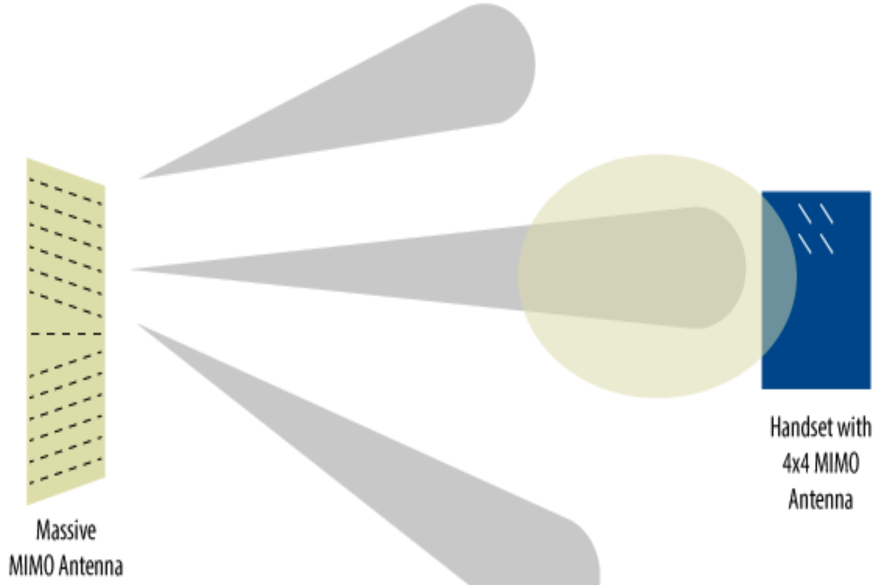
Device-to-Device (D2D) Communications



- Open Research Problems and Challenges Ahead:
  - **Confidentiality**: How to protect data confidentiality between cooperating D2D users against data leakage? Trusted list of devices?
  - **Data Exchange:** How to establish secure data exchange strategies against unintended devices and malicious devices/APs/base stations
  - **D2D Relaying:** Optimal selection of relays and protection methodology against untrusted relays
  - **Secrecy in multi-hop networks**
  - **Spectrum sensing data falsification (Byzantine Attacks)**: Attacker(s) modify or influence the spectrum sensing capabilities independently or collaboratively

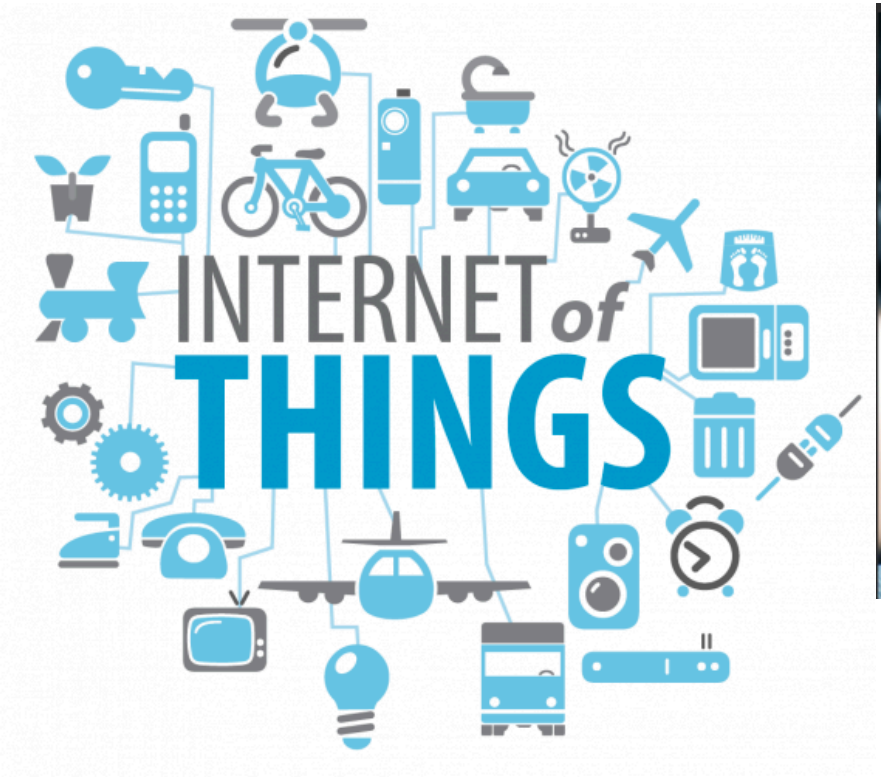
Physical Layer Security using Massive MIMO/Beamforming

- **Unique Advantages**:
  - **Low transmit power:** Decreases eavesdroppers ability to capture signal
  - **Channel State Unknown:** Eavesdropper does not know the CSI to BS
  - **More Degrees of Freedom for Artificial Noise Injection** at a BS due to larger number of antennas
  - **More directivity at mmWave frequencies**



- **Open Research Problems and Challenges Ahead**
  - **Channel matrix is large:** High computational complexity. Low-complexity methods are required
  - **Antennas correlation:** The limits on how antenna correlation affects the secrecy performance of massive MIMO are currently unknown

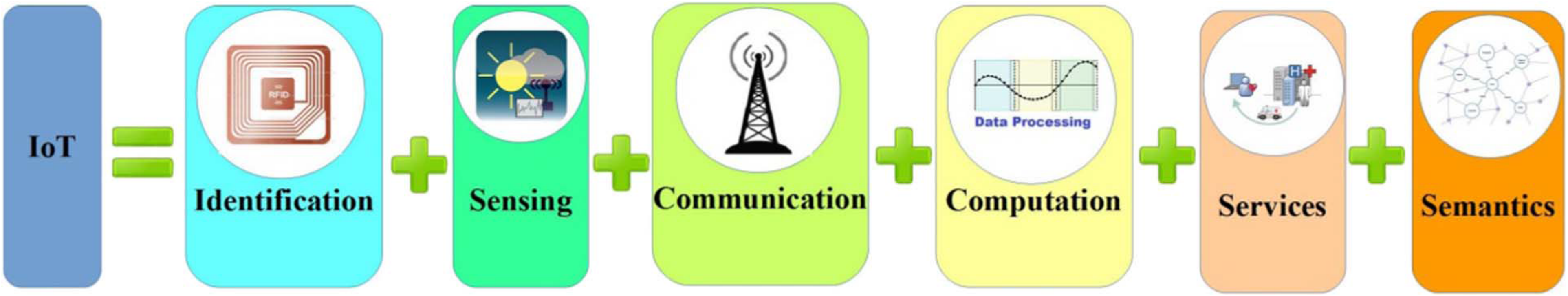
The Internet of Things May Spur the 4th Industrial Revolution



By 2020, it is expected that 250M cars will be connected to the Internet

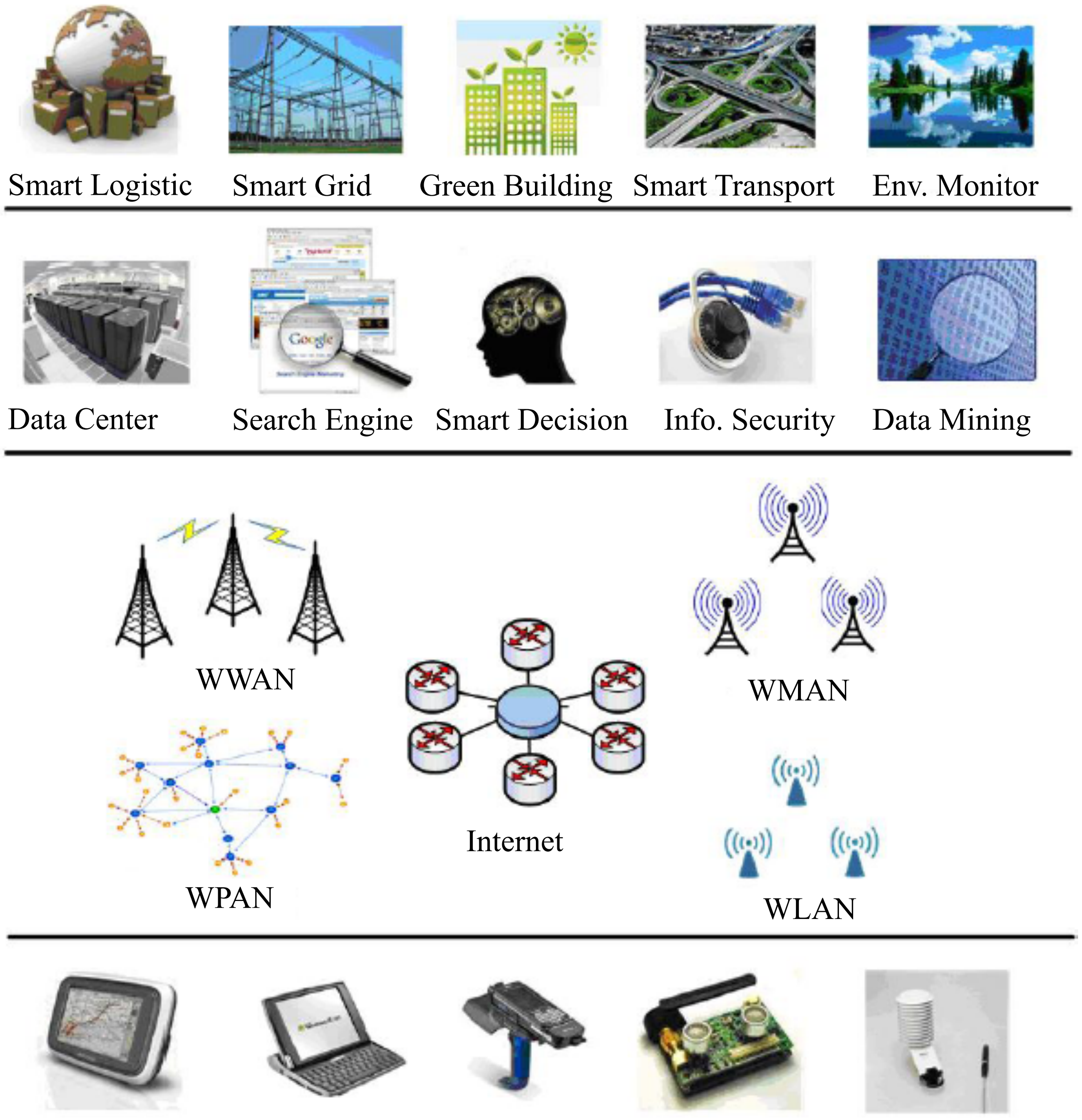
- In 2015, 4.9B connected “Things” were predicted to be in use.
- Google's Nest thermostats and net-connected smoke detectors are already making homes smarter.
- In 2020, 50B connected “Things” are expected to be in use.
- The IoT is expected to be the next revolution in the mobile ecosystem and expected to be a key driver for further wireless/cellular growth.

Internet of Things (IoT)



- The **Internet of Things** is the ecosystem of physical objects, devices, vehicles, buildings and all kinds of other objects that embed electronics, software, sensors and network connectivity.
- Three components: Information Technology [IT], Operational Technology [OT] and Smart Objects.
- These objects collect and exchange vast quantities of information, generating a wealth of actionable insights made available through big data and analytics.
- IoT security threats are substantial: [source: Fierce Wireless February 24, 2016]
  - AT&T has seen an ~ 500 percent increase in vulnerability scans of IoT devices in the last two years.
  - One common cyber attack involves reverse engineering firmware, such as that in home security cameras so the attacker can get access to the cameras' IP address from a file-sharing website and can take over the cameras' streaming video links giving them access to the camera's video feed.

4 Layer Model for IoT



Integrated Application

Smart Logistic Smart Grid Green Building Smart Transport Env. Monitor

Information Processing

Data Center Search Engine Smart Decision Info. Security Data Mining

Networking (of devices with limited complexity and power)

WWAN Internet WMAN WPAN WLAN

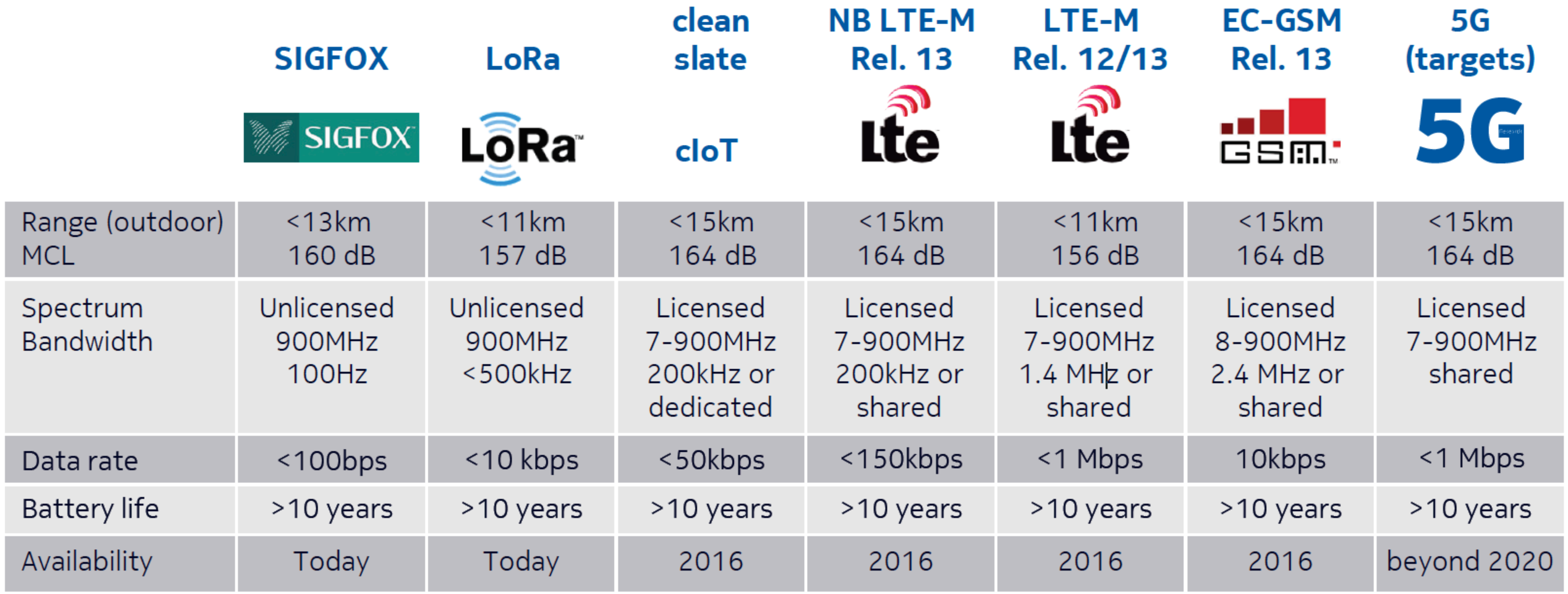
Sensing and Identification

GPS Smart Device RFID Sensor Sensor

IoT networking requires highly scalable capacity and optimal handling of the differing service needs by **network slices and novel protocols)** (bandwidth, asymmetry, latency, priority) for a broad range of IoT apps.

Internet of Things Wireless Alternatives

Plus Bluetooth, Zigbee, …

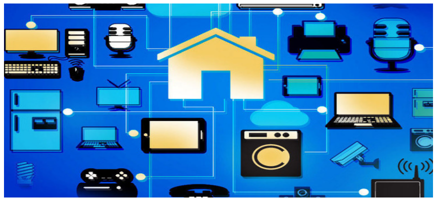


	SIGFOX	LoRa	clean slate cIoT	NB LTE-M Rel. 13	LTE-M Rel. 12/13	EC-GSM Rel. 13	5G (targets)
Range (outdoor) MCL	<13km 160 dB	<11km 157 dB	<15km 164 dB	<15km 164 dB	<11km 156 dB	<15km 164 dB	<15km 164 dB
Spectrum Bandwidth	Unlicensed 900MHz 100Hz	Unlicensed 900MHz <500kHz	Licensed 7-900MHz 200kHz or dedicated	Licensed 7-900MHz 200kHz or shared	Licensed 7-900MHz 1.4 MHz or shared	Licensed 8-900MHz 2.4 MHz or shared	Licensed 7-900MHz shared
Data rate	<100bps	<10 kbps	<50kbps	<150kbps	<1 Mbps	10kbps	<1 Mbps
Battery life	>10 years	>10 years	>10 years	>10 years	>10 years	>10 years	>10 years
Availability	Today	Today	2016	2016	2016	2016	beyond 2020

Source: nokia_lte-m_-_optimizing_lte_for_the_internet_of_things_white_paper.pdf

- More on the way …
- **MulteFire™** – LTE-based technology for small cells, based on 3GPP Releases 13/14 operating solely in unlicensed spectrum for enhanced performance in local area network deployments [Ericsson, Nokia and Qualcomm, …]
- **802.11ah** under study: Low-power networking with 1km range and modified PHY and MAC layers that support for IoT applications. The PHY layer RF link will use OFDM with either 32 or 64 tones, and is essentially a sub-GHZ variation of the IEEE 802.11ac PHY

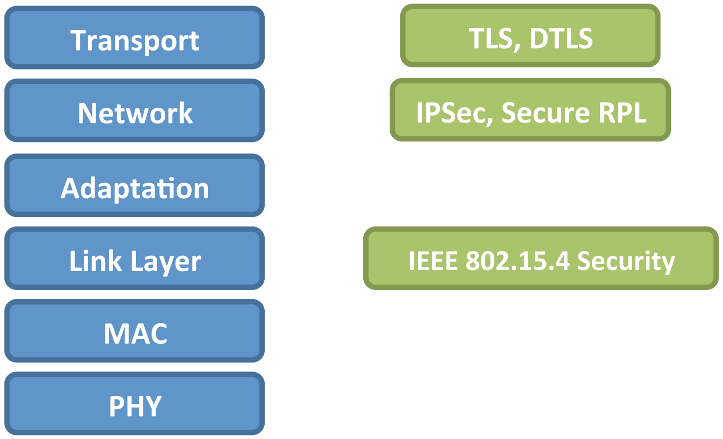
IoT Security --- Principles



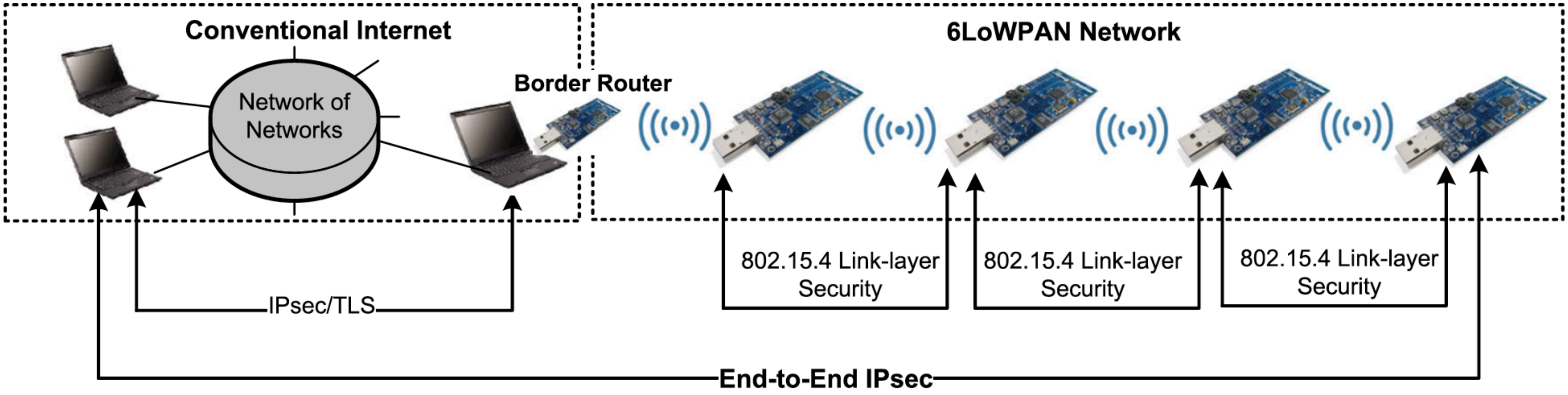
- **End-to-end security mechanisms:** Mobile apps and connected devices must be authenticated separately. The identity of the connected device is best maintained in HW.
- **End-to-end data encryption:** The challenge is making all the authentication and key management happen without user configuration, so the data encrypts automatically.
- **Access and authorization control:** This means giving different user types different levels of data access (e.g., letting utility link to your thermostat on peak power days).
- **Activity auditing:** IoT device manufacturers and service providers need to keep log records so that any breaches can be traced back to the source.
- **Hardened cloud infrastructure:** Hosting data in the cloud can be far more secure than keeping it at home or in a company-run datacenter. ISO 27001 is a security certification standard that specifies security management best practices and comprehensive security controls for datacenters and other environments.
- **Equal protection across multiple protocols:** Devices will communicate over WiFi, cellular, ZigBee, Bluetooth, and other wireless (and wired) protocols. Security has to be equally strong across all of them, regardless of whether the mobile app is talking to a connected device over the Internet or locally (e.g. at home, on the same WiFi network as the connected device).
- **Remote updating:** Devices able to have firmware remotely updated in a secure manner since the security landscape is undergoing continual change.

Security for the IP-Connected IoT

- Conventional internet security protocols are unsuitable for <u>resource-constrained IoT devices</u>
- Need for new protocols at all layers and mechanisms to secure data stored on the devices.
  - IEEE 802.15.4 security protocol provides security over a single hop at the link layer with a <u>shared key</u>.
  - IPSec and secure RPL (Routing Protocol for Low Power and Lossy Networks) at the network layer and Layer Security (TLS) and Datagram TLS (DTLS) secure communications over TCP and UDP respectively
  - Key Distribution is a challenge in IoT.



Transport	TLS, DTLS
Network	IPSec, Secure RPL
Adaptation	
Link Layer	IEEE 802.15.4 Security
MAC	
PHY	



IEEE 802.15.4 = Low Rate Wireless Personal Area Network (LR-WPAN)
6LoWPAN = IPv6 over Low-power Wireless Personal Area Networks

S. Raza *et al.*, "Secure Communications for the Internet of Things – A comparison of link layer security and IPSec for 6LoWPAN," *Security and Communication Networks*, vol. 7, no. 12, pp. 2654 – 2668, Dec. 2014.

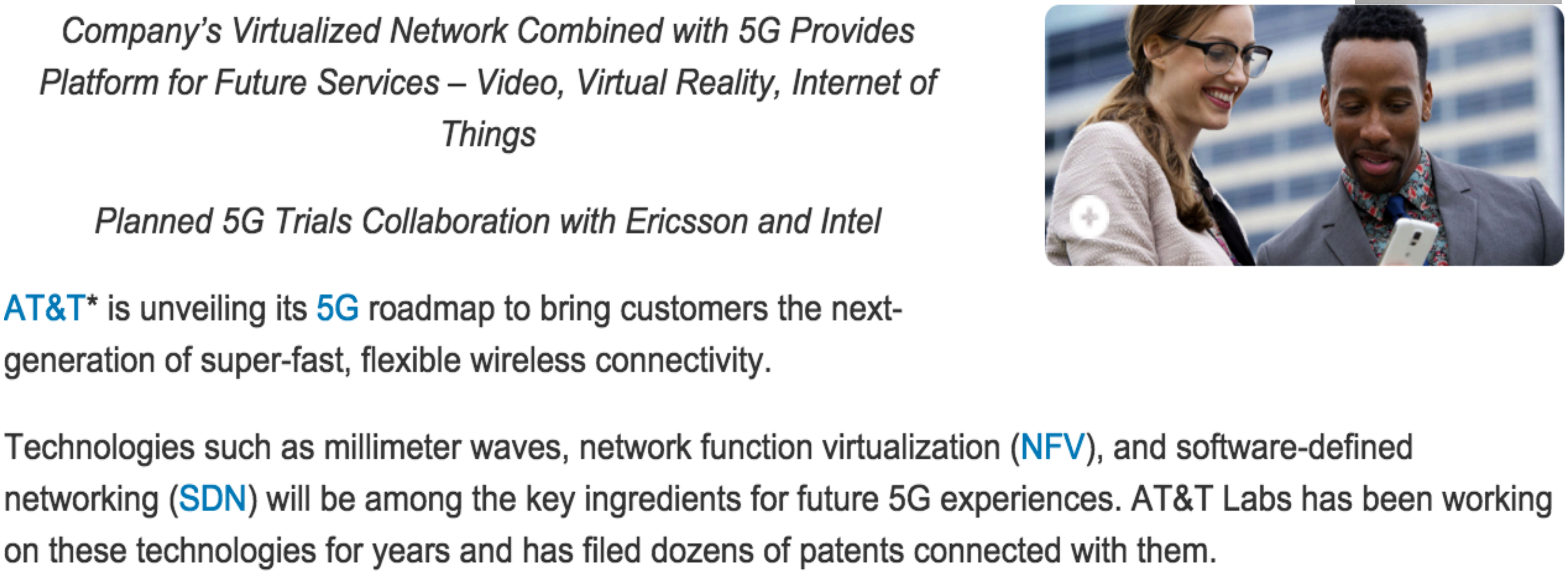
IoT for NYC: Smart Grid will Touch 4M Homes

- New York’s Consolidated Edison plans to connect more than 4 million electricity and gas customers to a smart grid deployed by Silver Spring Networks to cut carbon emissions by 80% by 2050
- Silver Spring plans to use the **IEEE 802.15.4g** wireless interoperability standard, called Wi-SUN (SUN = Smart Utility Networks)
- Wi-SUN will offer speeds of up to 2.4 Mbps, and will support dual-band mesh communications on both 900 MHz and 2.4 GHz frequencies

IoT Streetlight/Lamppost

- Smart streetlights are essentially poles packed with LEDs, small cell LTE base stations, an optional control system for the lights and a smart meter to monitor the poles' power use.
- Today's smart pole has two configurations — a high-power pole packs three big Ericsson RU-11 or -12 60W LTE radios, the low-power version crams in six 5-10W radios that cover a narrow range of about 1,000 feet. In the high power version the radios sit in an expanded base of the pole, while the low power version packs the radios with the antennas in a radome near the LED lights.

AT&T Unveils 5G Roadmap with Trials in 2016



Company's Virtualized Network Combined with 5G Provides Platform for Future Services – Video, Virtual Reality, Internet of Things

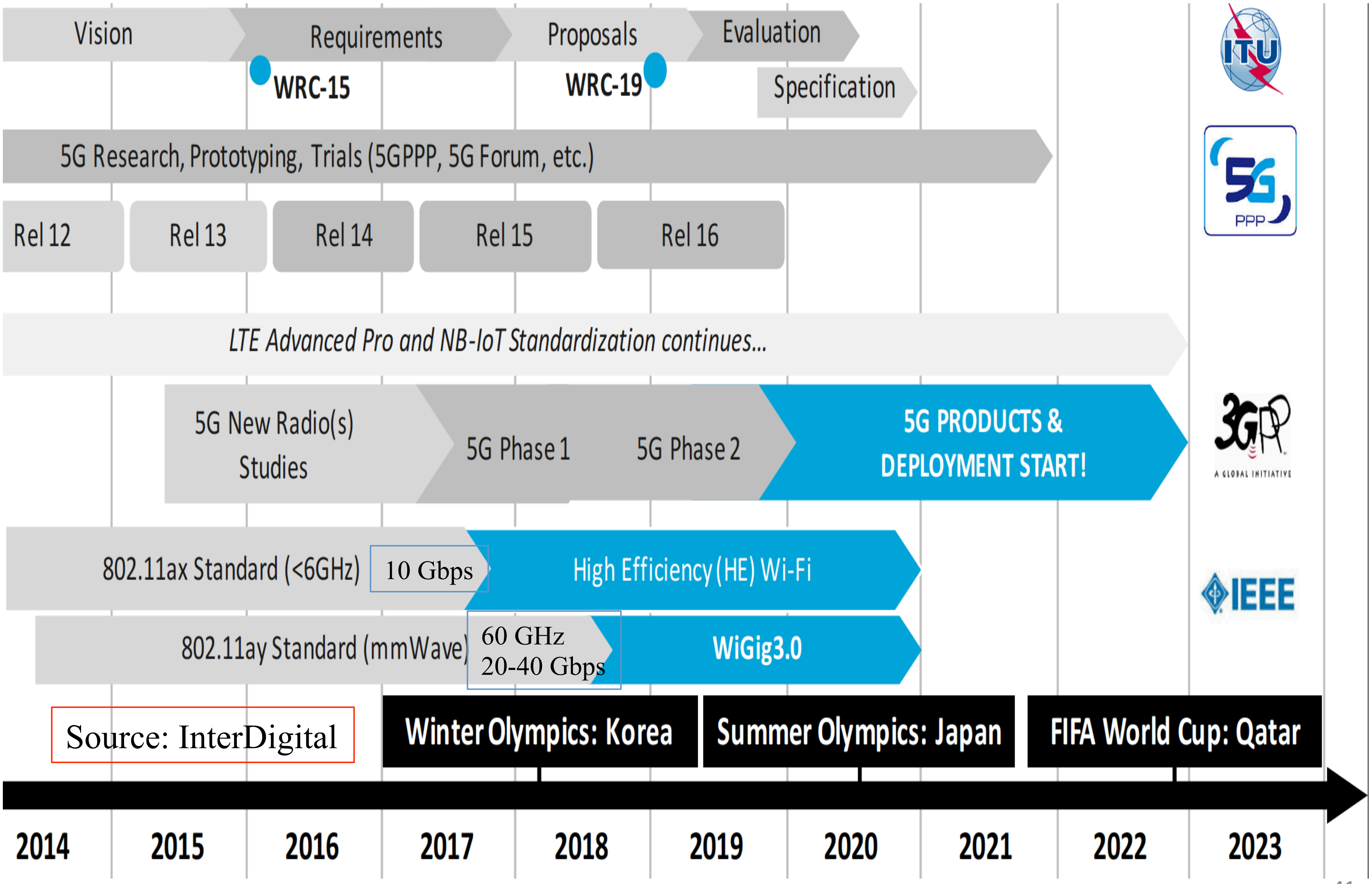
Planned 5G Trials Collaboration with Ericsson and Intel

AT&T* is unveiling its 5G roadmap to bring customers the next-generation of super-fast, flexible wireless connectivity.

Technologies such as millimeter waves, network function virtualization (NFV), and software-defined networking (SDN) will be among the key ingredients for future 5G experiences. AT&T Labs has been working on these technologies for years and has filed dozens of patents connected with them.

- *We expect 5G to deliver speeds 10-100 times faster than today's average 4G LTE connections. Customers will see speeds measured in gigabits per second, not megabits. For reference, at one gigabit per second, you can download a TV show in less than 3 seconds. AT&T February 12, 2016.*
- Don't get too excited yet since:
  - No agreement yet on 5G standards. Carriers are currently using their own ideas of the best technology for high-speed data services, with a 3GPP target of 2018-2020.
  - AT&T hopes to use the high-speed wireless service to offer broadband to homes in remote areas, and that it can do this even before mobile data standards are finalized.

5G Roadmap



Vision

Requirements

Proposals

Evaluation

WRC-15

WRC-19

Specification

5G Research, Prototyping, Trials (5GPPP, 5G Forum, etc.)

Rel 12

Rel 13

Rel 14

Rel 15

Rel 16

LTE Advanced Pro and NB-IoT Standardization continues...

5G New Radio(s) Studies

5G Phase 1

5G Phase 2

5G PRODUCTS & DEPLOYMENT START!

802.11ax Standard (<6GHz)

10 Gbps

High Efficiency (HE) Wi-Fi

802.11ay Standard (mmWave)

60 GHz
20-40 Gbps

WiGig3.0

Winter Olympics: Korea

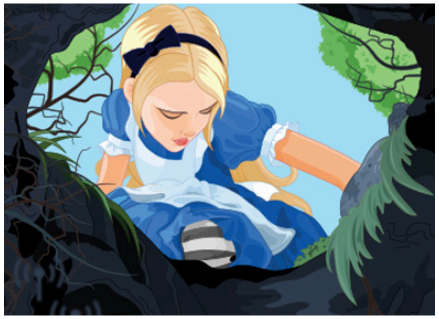
Summer Olympics: Japan

FIFA World Cup: Qatar

2014 2015 2016 2017 2018 2019 2020 2021 2022 2023

Source: InterDigital

The Skeptics View of 5G

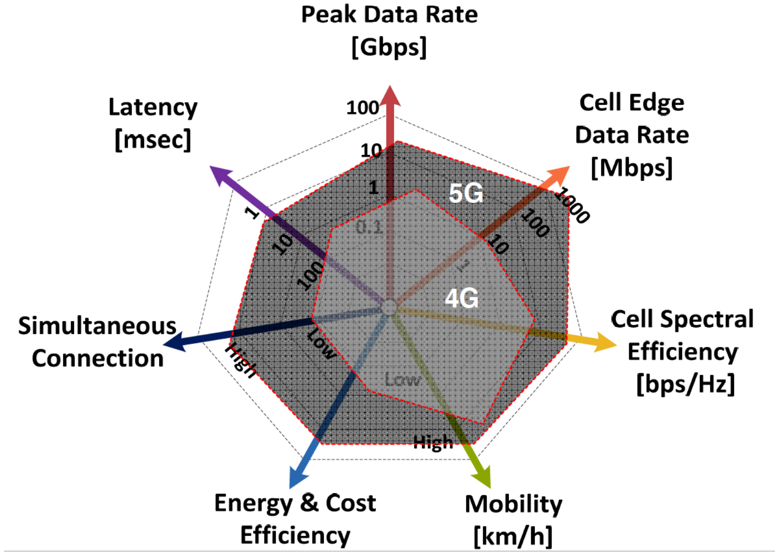


“Only when you know how to see through the illusions should you dare to travel through the rabbit hole....” *Alice in Wonderland*, Lewis Carroll, 1865

- Like *Alice in Wonderland*, the mobile world may be turned topsy-turvy with an accelerated push to 5G. There is a good deal of skepticism about 5G: **premature**, **market doubts**, **technology driven**, **non standardized**,…. We’ve all heard these before, but the skeptics say:
  - The lessons on 3G, 3.5G (HSPA), 4G were never (painfully) learned: that the ideal approach for operators and vendors is to leave time to “harvest” profits from investments.
  - The astonishing leap of faith is that by providing gigabit wireless speed at low latency, one will enable “new business models,” for now largely unimagined.
  - The purported “business cases” for 5G includes the “Ghost of 2G Past,” in the form of telematics, rebranded M2M, and now rebranded once more as “IoT”.
  - The notion that we need vast infrastructure upgrades to send tiny amounts of data with lower latency smells of desperation. And, all the low-latency video-related services – which again can be made more than workable with a combination of cellular plus WiFi.
  - Meanwhile, just to muddy the waters and prevent any smooth sailing towards the mythical 5G world, we have a slew of new variants: LTE-A, LTE-U, low-energy LTE, …
- And finally from an AT&T executive
  - “We as an industry have been really good at overpromising and under delivering when it comes to new technology.”
  - “Let’s make sure that before we start hyping what it’s going to be, that those standards are agreed to.”

Source: http://www.comsoc.org/ctn/5g-down-rabbit-hole

Concluding Remarks
5G + IoT = A New Era of Connectivity



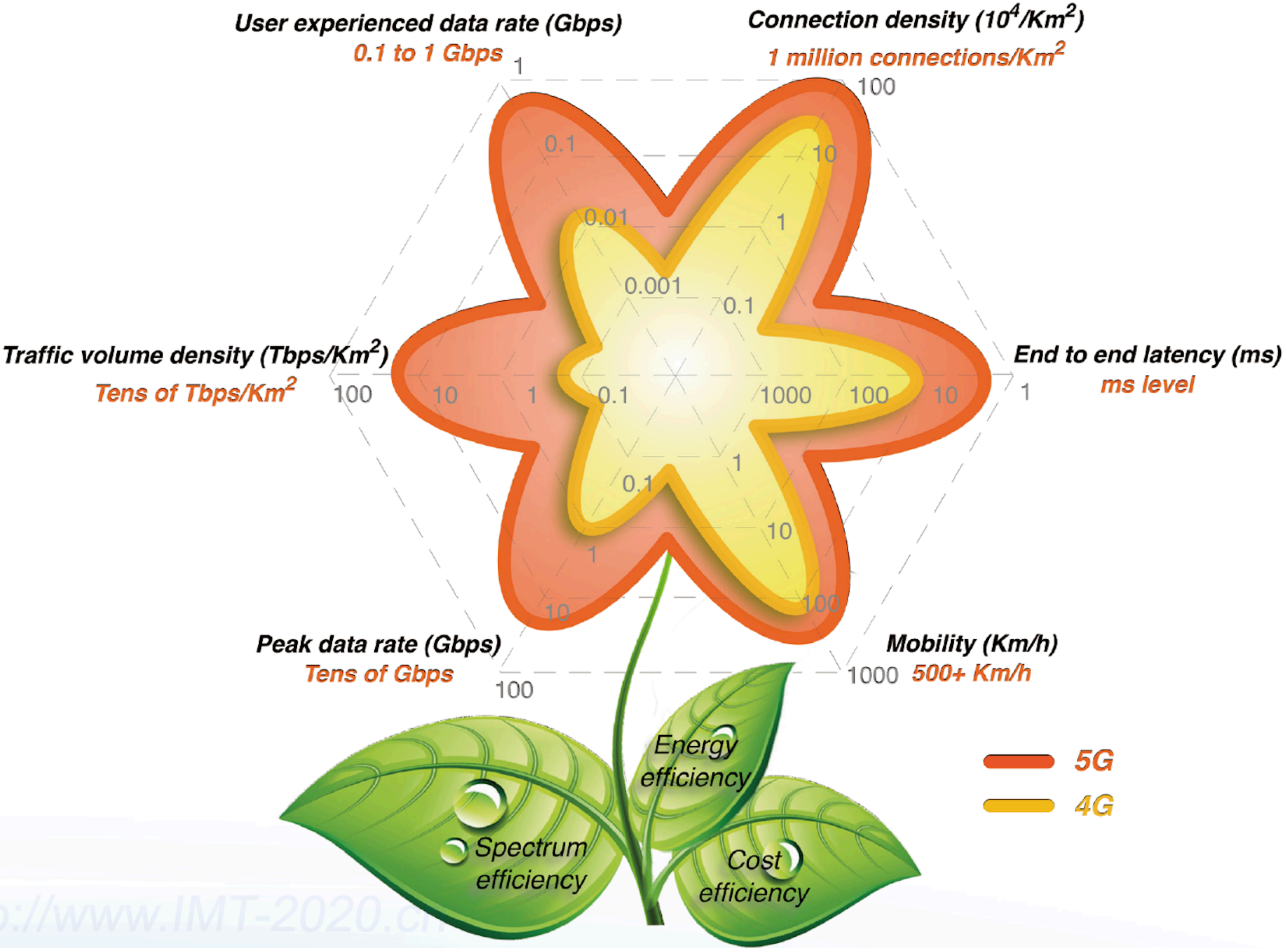
The 5G challenge and path is clear

- To succeed the unified 5G/IoT network must be flexible, exceptionally capable, and economical enough to address the skeptics concerns and successfully navigate all of the expected and unexpected scenarios.
- We are at a point of inflection created by the synergies of 5G gigabit wireless connectivity and the revolutionary Internet of Things --- with connectivity for everyone and everything.
- Together their impact will be transformational and will be central to everything we do, forever alter how people access and use information, and will ultimately create …

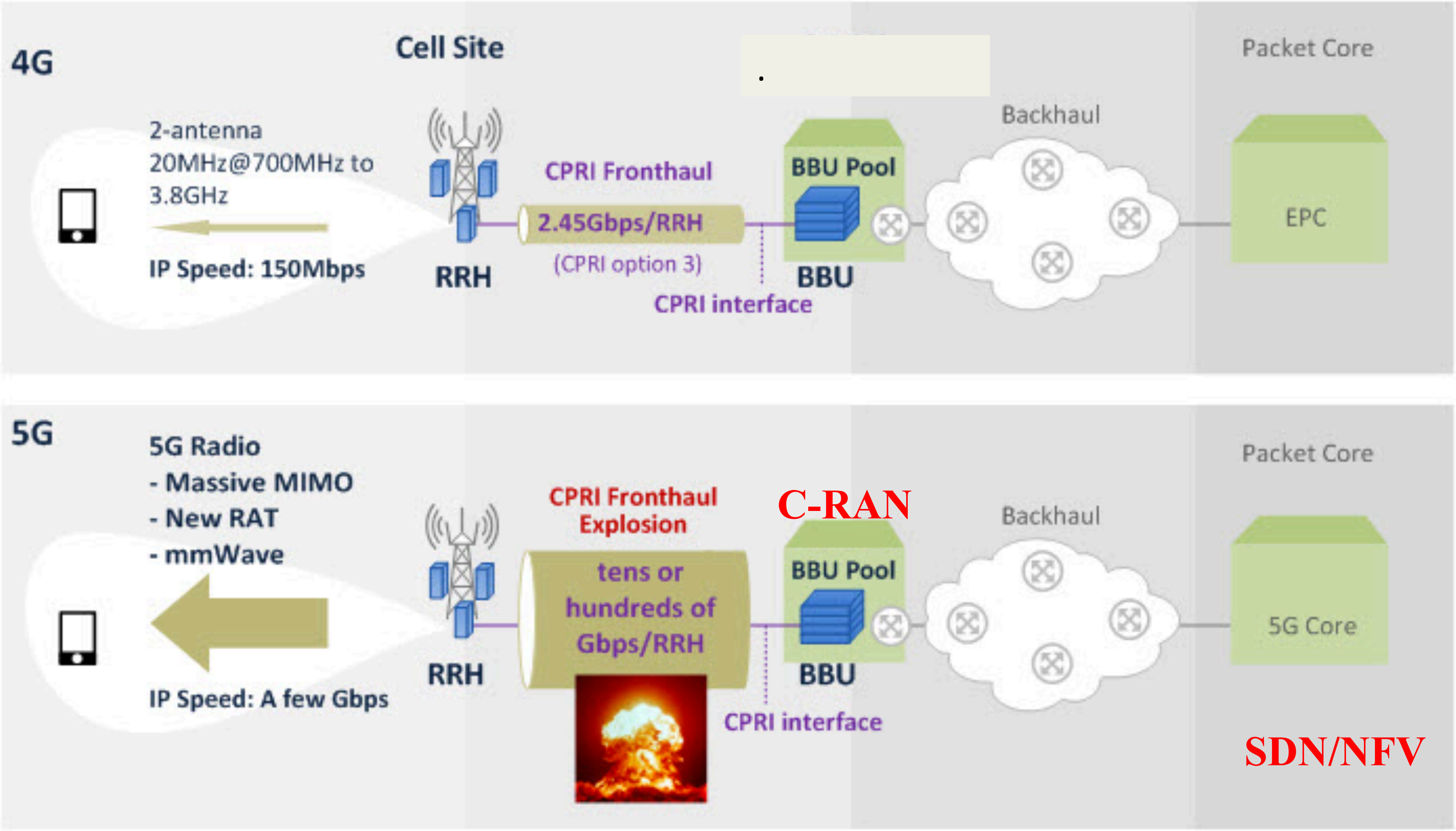
The Internet of Tomorrow

Backup

5G Key Technical Challenges

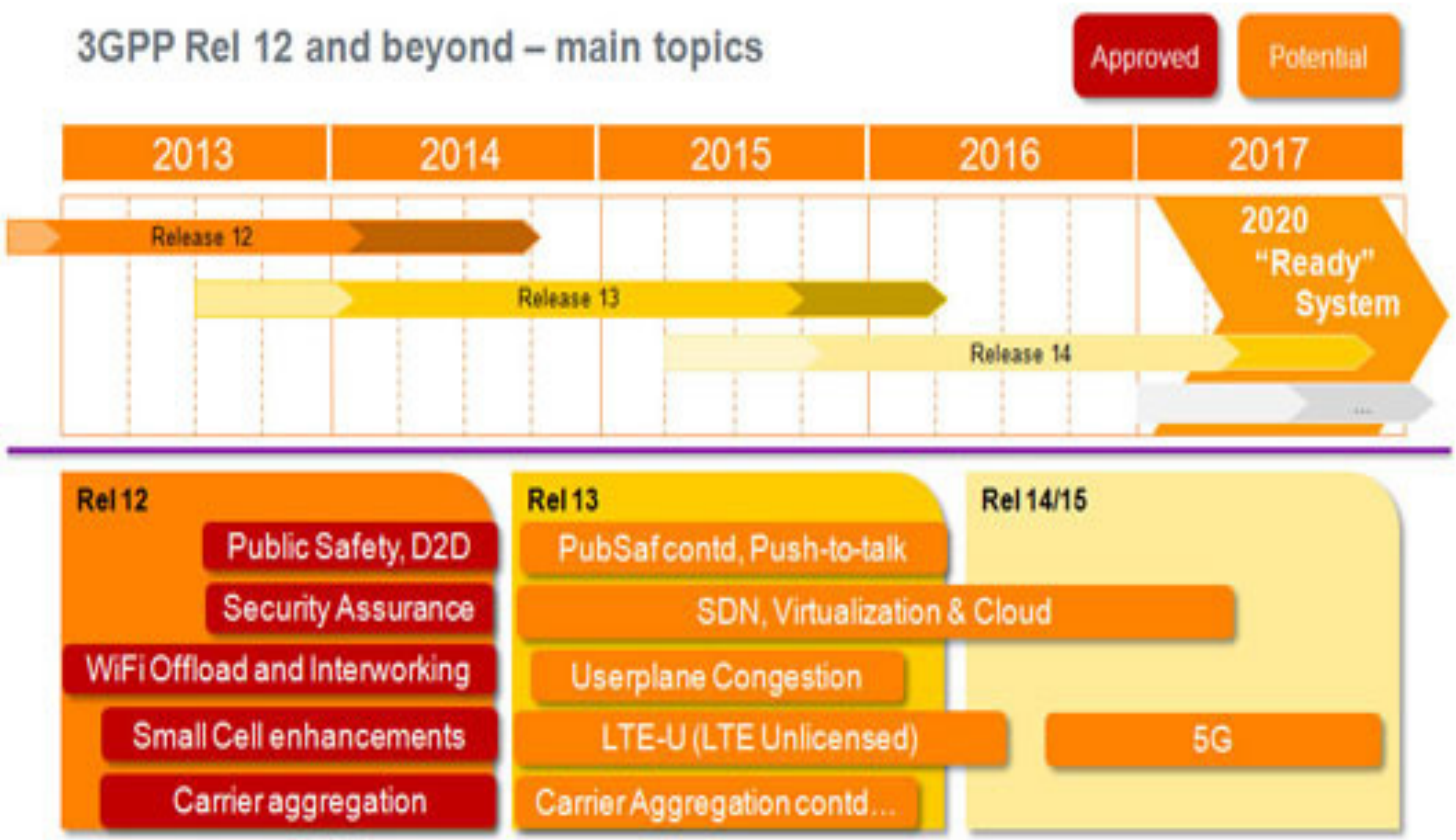


5G Is Revolutionary Compared to 4G



The two big software networking promises of **SDN and NFV** (typically lumped together) are cost savings, and service agility, and the ability to launch and decommission customized services rapidly and efficiently.

3GPP LTE 5G Roadmap



3GPP Rel 12 and beyond – main topics

Approved

Potential

2013

2014

2015

2016

2017

Release 12

Release 13

Release 14

2020
"Ready"
System

...

Rel 12

Public Safety, D2D

Security Assurance

WiFi Offload and Interworking

Small Cell enhancements

Carrier aggregation

Rel 13

PubSaf contd, Push-to-talk

SDN, Virtualization & Cloud

Userplane Congestion

LTE-U (LTE Unlicensed)

Carrier Aggregation contd…

Rel 14/15

5G

5G Data Requirements

	LTE	LTE-A
Peak Data Rate	50 Mbps 150 Mbps	500 Mbps 1 Gbps
Spectral Efficiency	16.32	30
Carrier Bandwidth	Up to 20 MHz	Up to 100 MHz
Latency (RTT)	~10 ms	~5 ms

5G

<1 ms latency (when needed)	10-50 Gbps peak data rates	90% Energy reduction per service
100-500 MHz Carrier Bandwidth	Higher Density: Millions of connections per Km^2	Higher Traffic Volume: 1-10 Tbps per Km^2
Rapid Service Creation (from days to minutes)	Sustainable Total Cost of Owner for all players	User Definable Security & Privacy

5G Emerging Networking Technologies

Software-Defined Networking [SDN]

SDN is an approach to networking in which routing control is decoupled from the physical infrastructure enabling a networking fabric across multi-vendor equipment

Network Function Virtualization [NFV]

NFV moves network services out of dedicated hardware devices into software. Functions that in the past required specialized hardware devices can now be performed on standard servers

SDN/NFV Orchestration

The new network operating system. Supports lifecycle management, global resource management, validation and authorization of new requests, policy management, system analytics, interface management

Fog Computing / Edge Computing

Extends cloud computing and services to the edge of the network and into devices. Similar to cloud, fog provides network, compute, storage (caching) and services to end users. The distinguishing feature of Fog reduces latency and improves QoS resulting in a superior user experience

Contextual Networking [CN]

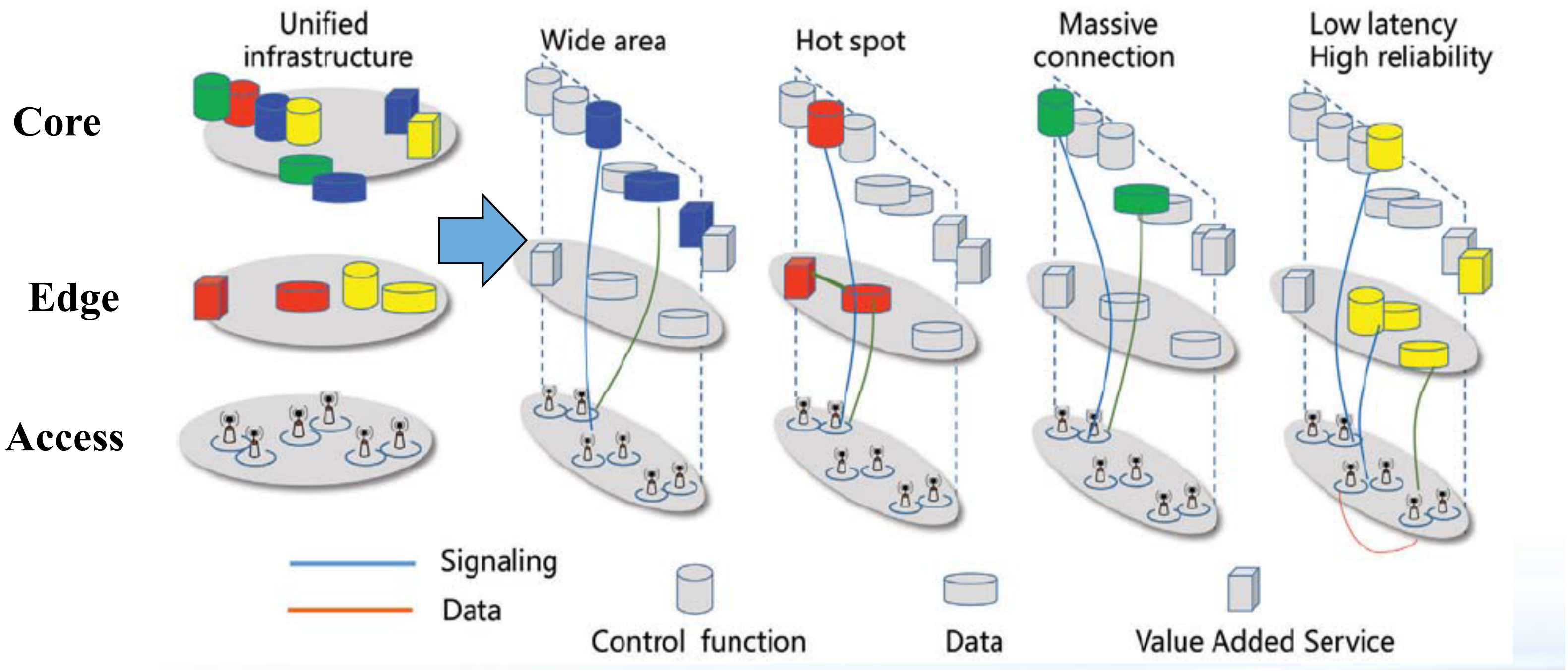
5G may not deliver infinite bandwidth but it may well deliver a reasonable perception thereof. CN includes all categories of analytics (behavioral, predictive, etc.) and cross layer techniques applied to enable the more efficient and “just in time” use network capacity

Information Centric Networking [ICN]

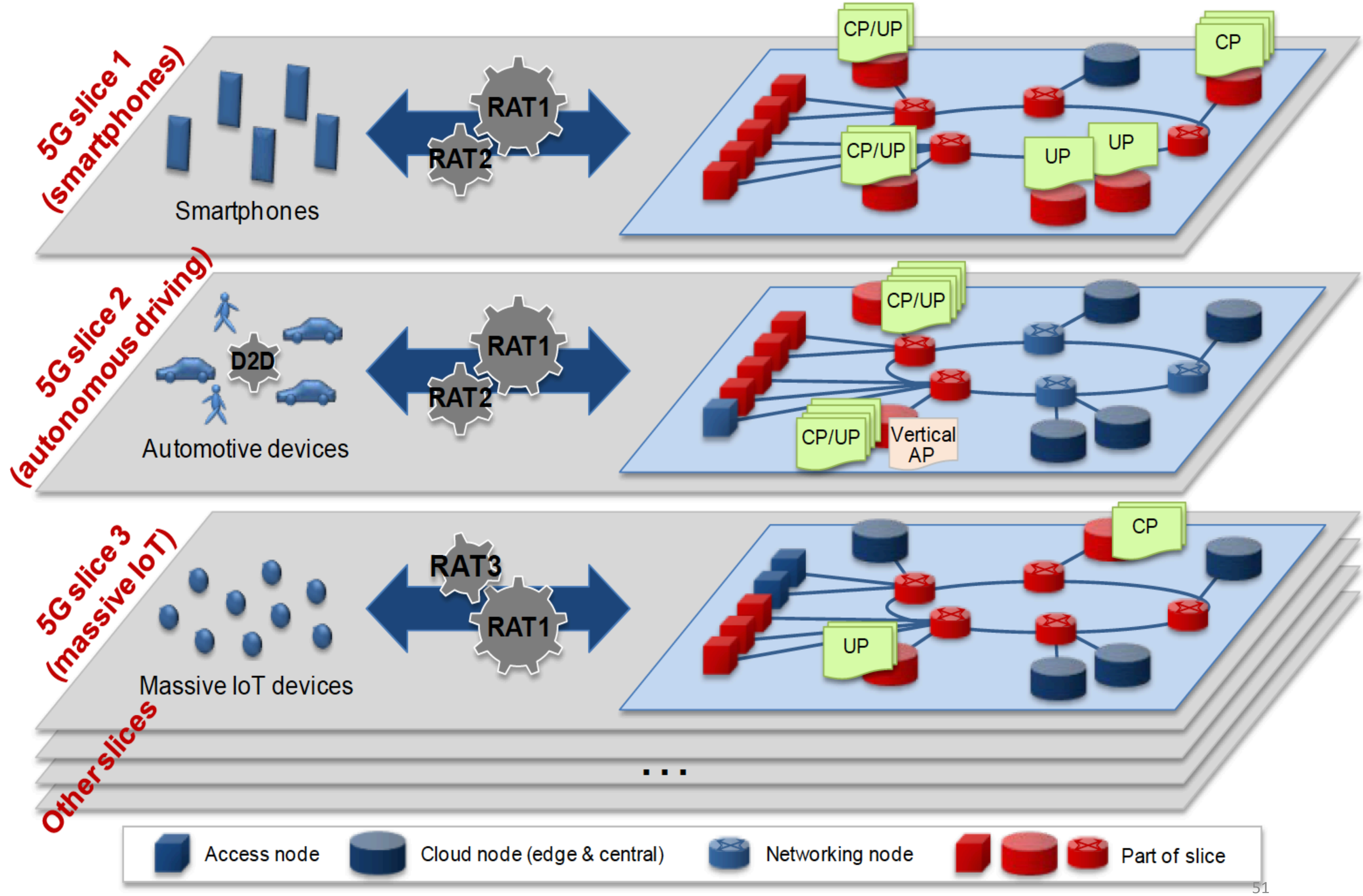
ICN directly routes and delivers content at the packet level of the network, enabling automatic and application-neutral caching in memory wherever it’s located in the network. Improved mobility, security, privacy, resiliency, multicast support, etc.

5G NFV: Network Slicing

- A network slice is an end-to-end logically isolated network including devices, access, transport and core network function to support diverse scenarios on a common infrastructure.
- Enables operators to launch a range of highly differentiated network services, each aimed at a distinct vertical market but relying on the same infrastructure.
- Key issues:
  - Identify and select the slice in device, access and core part
  - Guarantee the end-to-end QoS of a slice
  - Design the slices to different scenarios



NFV: Network Slices Implemented on the Same Infrastructure

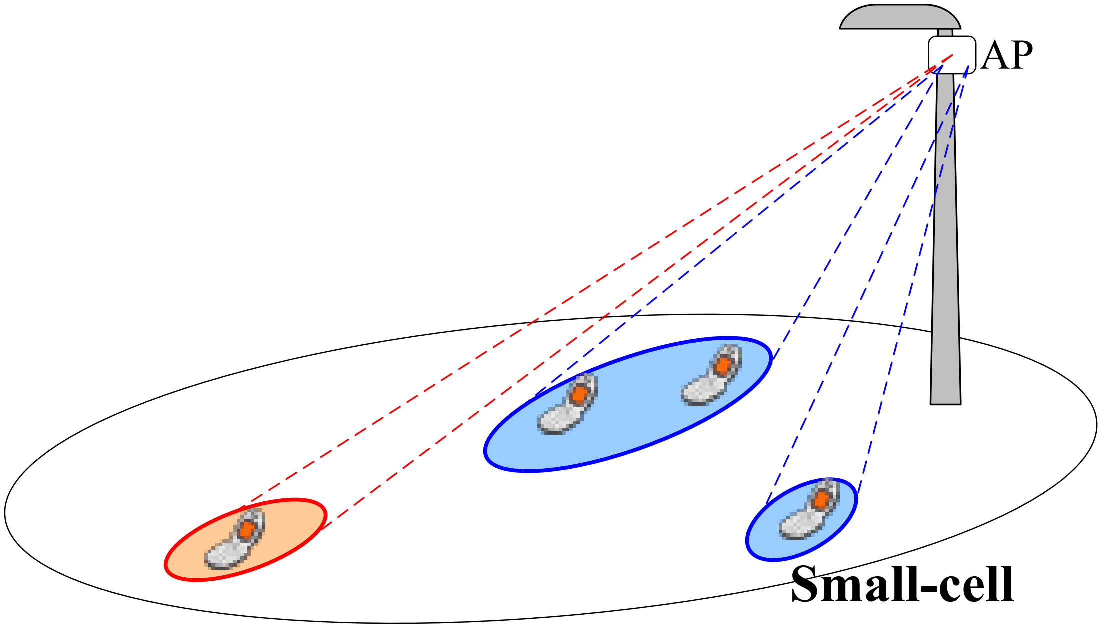


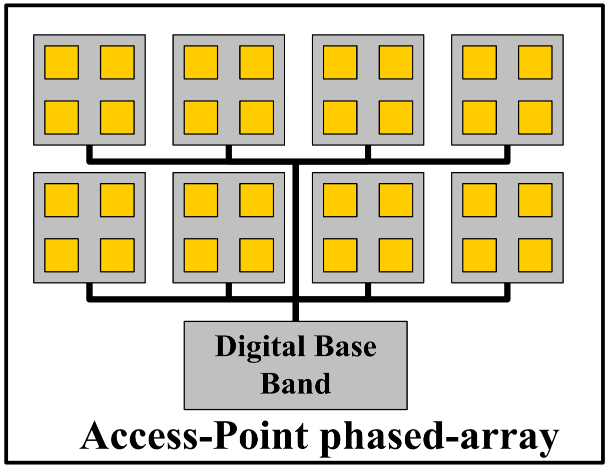
Source: NGMN White Paper

60 GHz Radio for Access Point

Module architecture

- Frequency multiplexing: inter and intra channels
- Spatial multiplexing: simultaneous multiple beams
- Scalability: capacity, range, power consumption, size

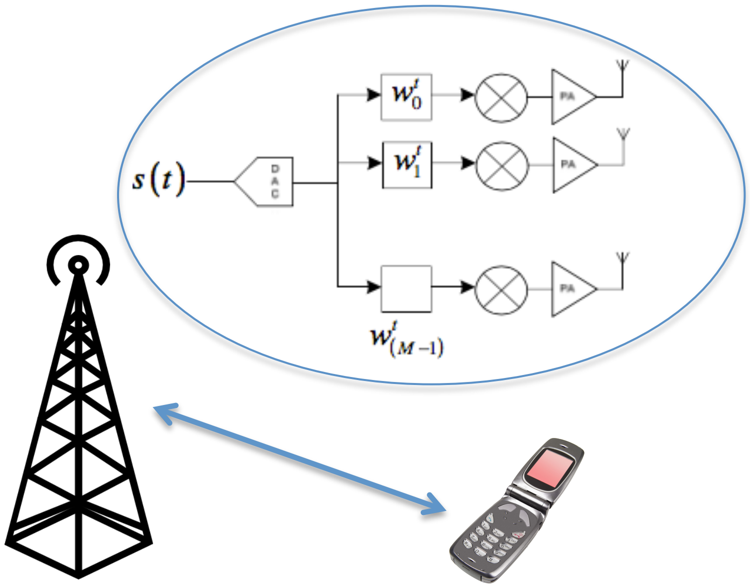




Physical Layer Security with mmWaves

Millimeter Wave Communication

- **Unique Advantages:**
  - **Directional Transmissions:** Enables large overlap of coverage area, no clear cell boundaries
  - **Short range transmissions:** Only geographically neighboring eavesdroppers
  - **More antennas can be utilized**: higher beamforming gain



- **Open Research Problems and Challenges Ahead:**
  - **Secrecy performance using analog (or hybrid) beamforming for millimeter wave**
  - **Power allocation problem for secrecy maximization:** How to optimally allocate transmit power between signal and artificial noise in millimeter wave