ORDINE DEGLI INGEGNERI DELLA PROVINCIA DI AVELLINO

ORDINE DEGLI INGEGNERI DELLA PROVINCIA DI SALERNO

CORSO PREPARATORIO AGLI ESAMI DI STATO

II sessione 2023

Sistemi di Telecomunicazione di nuova generazione e sicurezza delle comunicazioni

9-13 novembre 2023

ORDINE DEGLI INGEGNERI DELLA PROVINCIA DI SALERNO

Mario Di Mauro, PhD

Gruppo Telecomunicazioni – Università degli Studi di Salerno
Commissione ICT – Ordine degli Ingegneri di Salerno

mario.dimauro@ordingsa.it (PEC)
mdimauro@unisa.it

Mobile Technology Evolution

1G

Analog

Voice only, Limited coverage and mobility. Example: AMPS

2G

Digital

Improved voice, security, coverage. SMS, data. Example GSM, CDMA

3G

Mobile Data

Higher data rates, smartphones, better voice. Example: HSPA / HSPA+

4G

Mobile Broadband

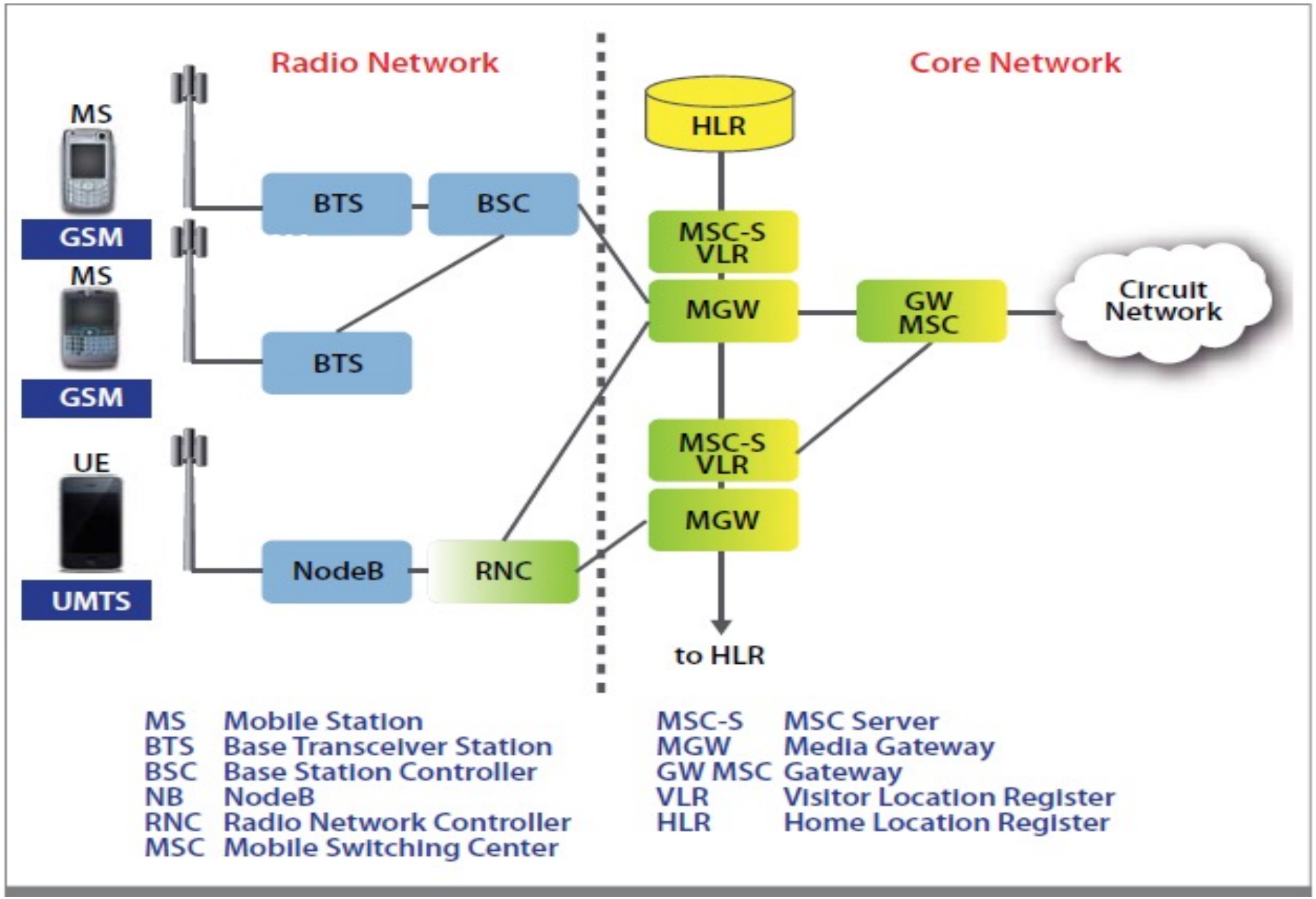
High speed data, better smartphones. Example: LTE / LTE-A

5G

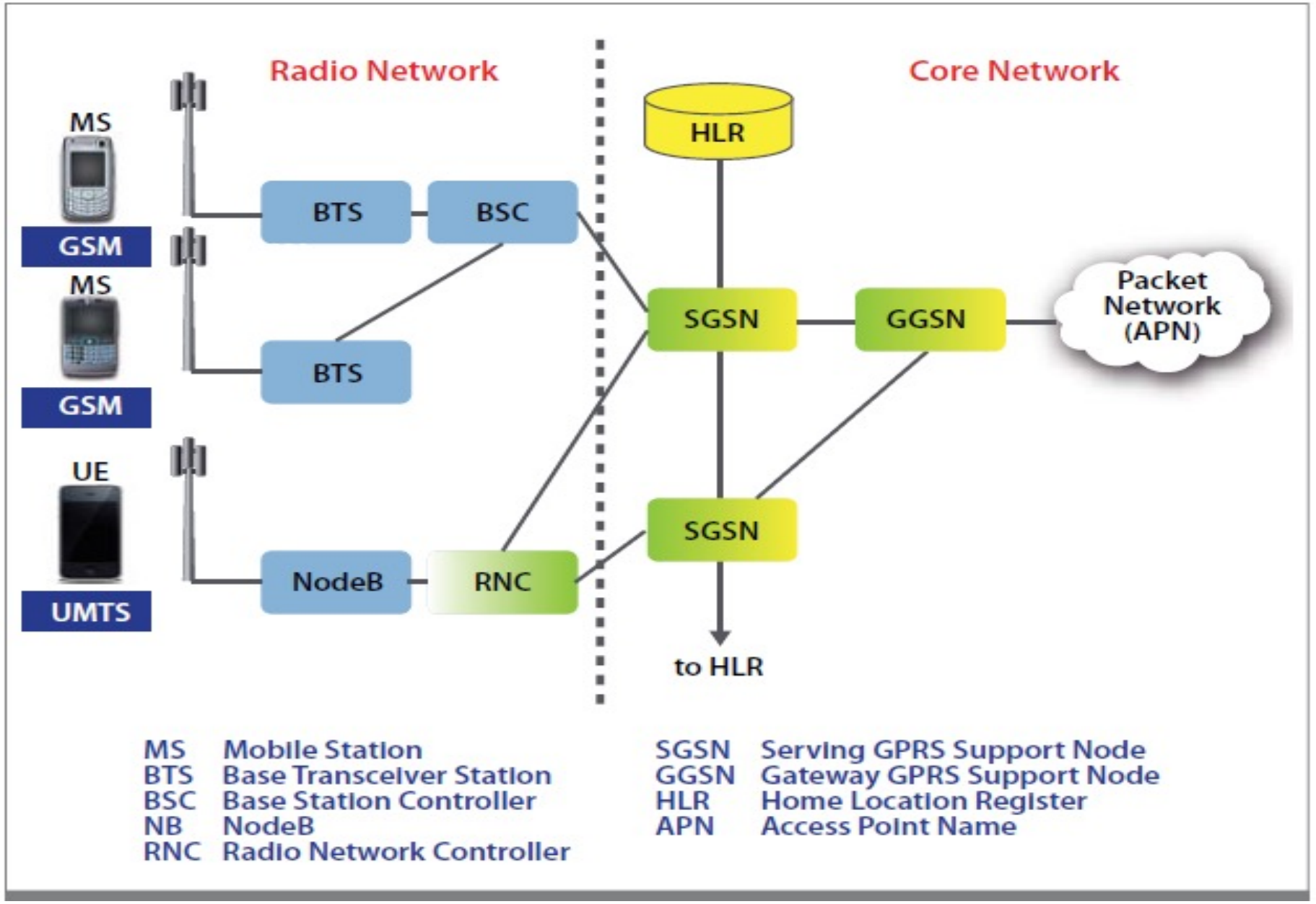
eMBB, mMTC, URLLC

Even higher speeds, ultra-reliable, low latency, high connection density

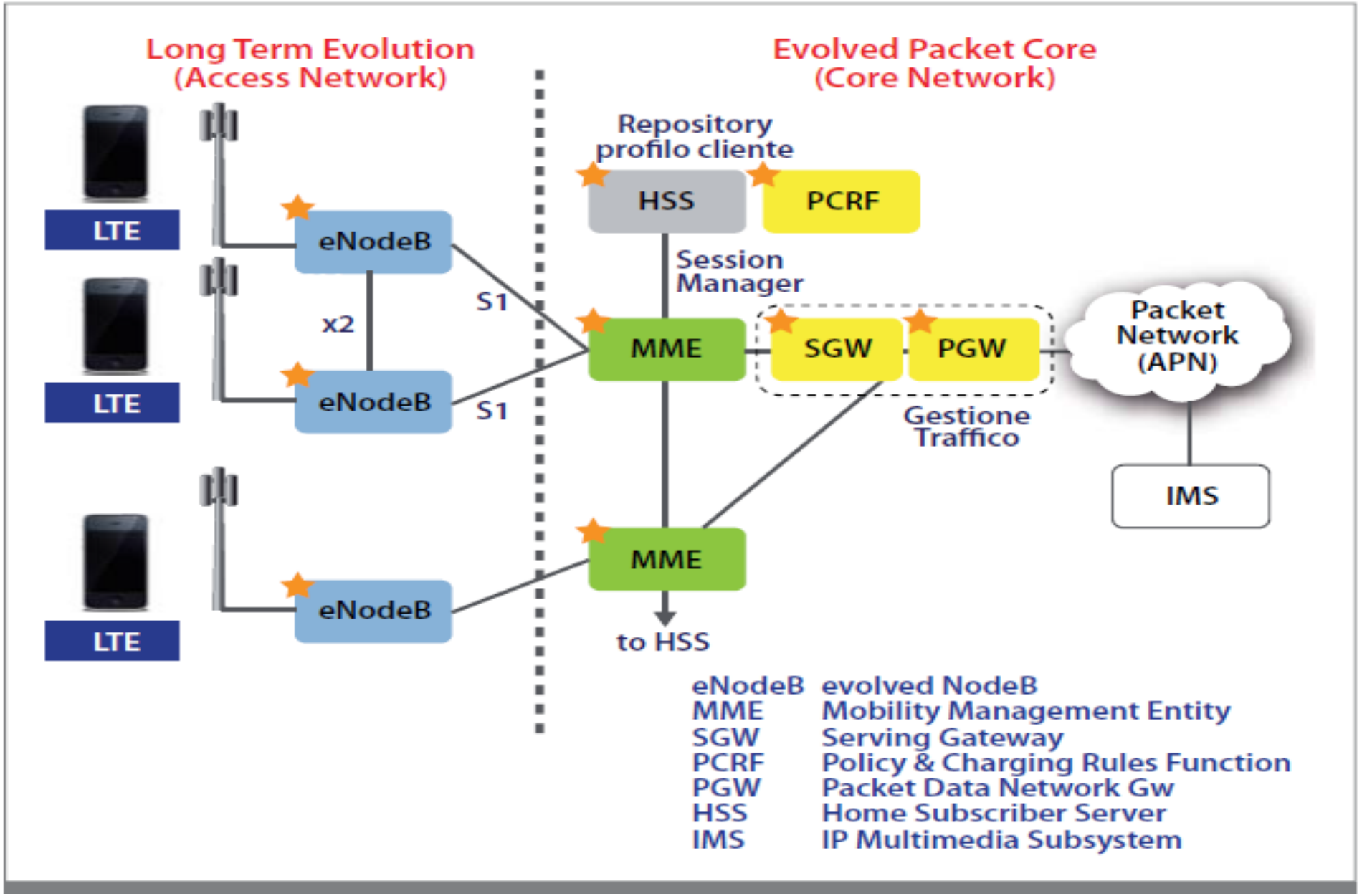
1980 1990 2000 2010 2020



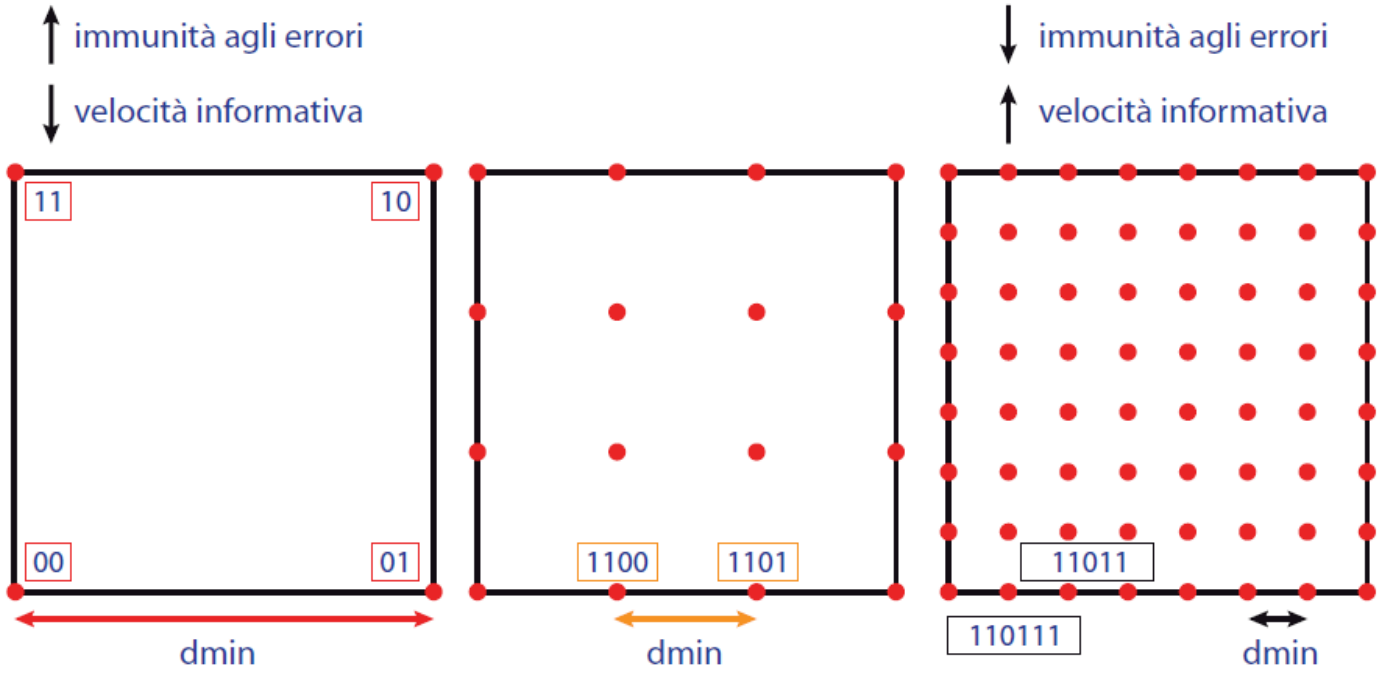
2G / 3G Cellular Architecture



GPRS (2.5G) Cellular Architecture

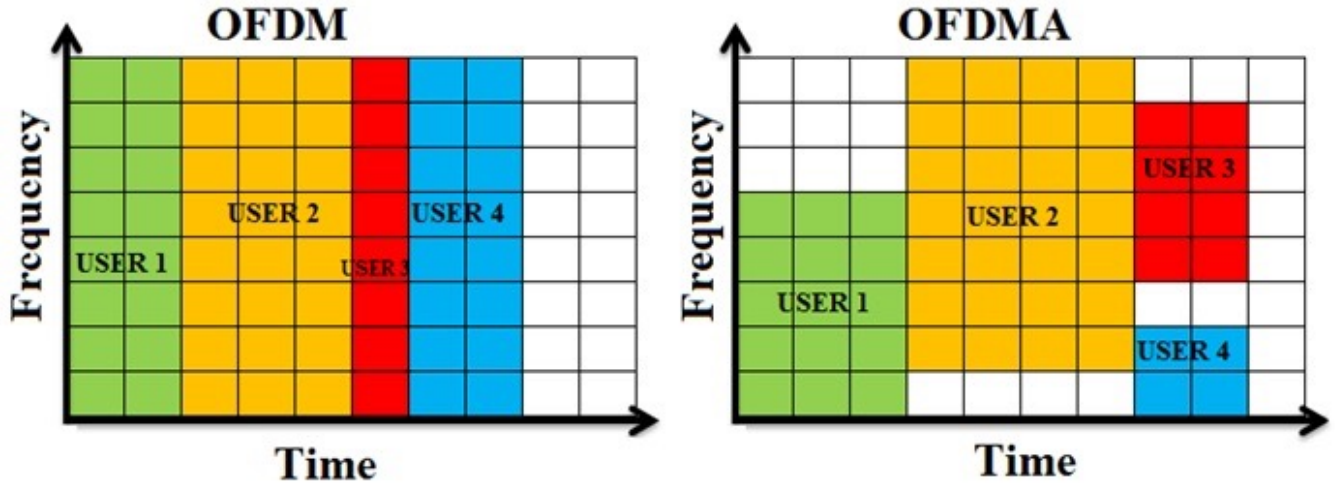


LTE Cellular Architecture



Signal Constellations in LTE (Adaptive)

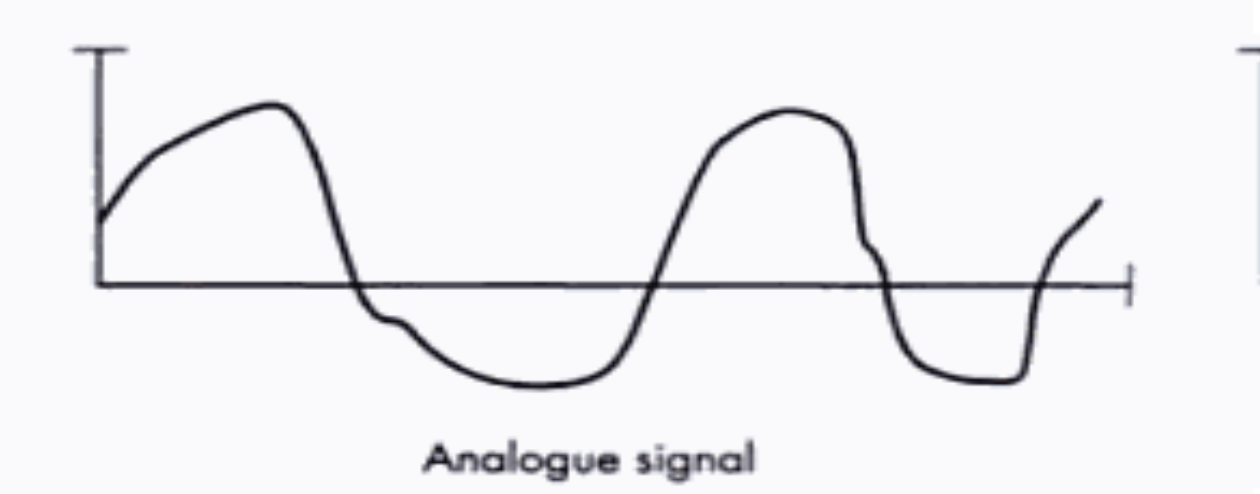
OFDMA Scheme In LTE

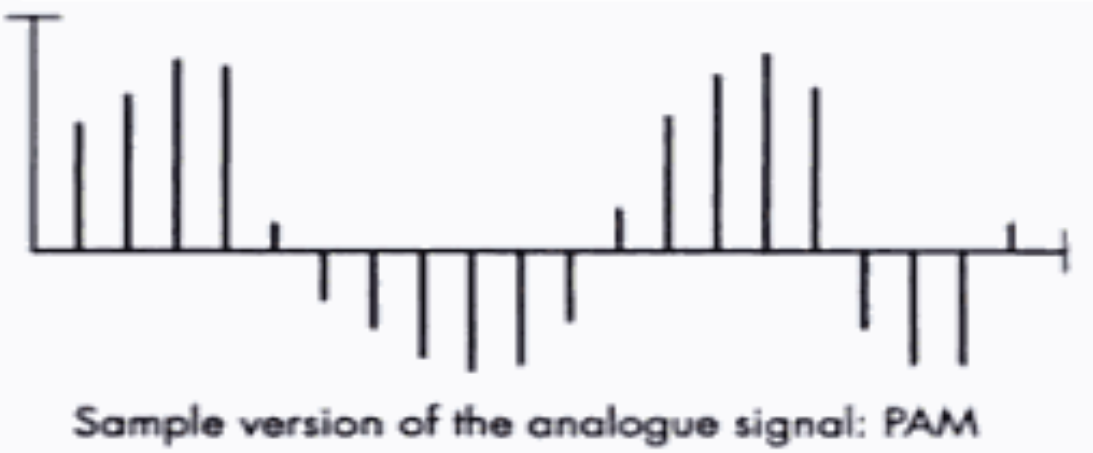


Voice Digitization (3G and beyond)

Analog to digital conversion

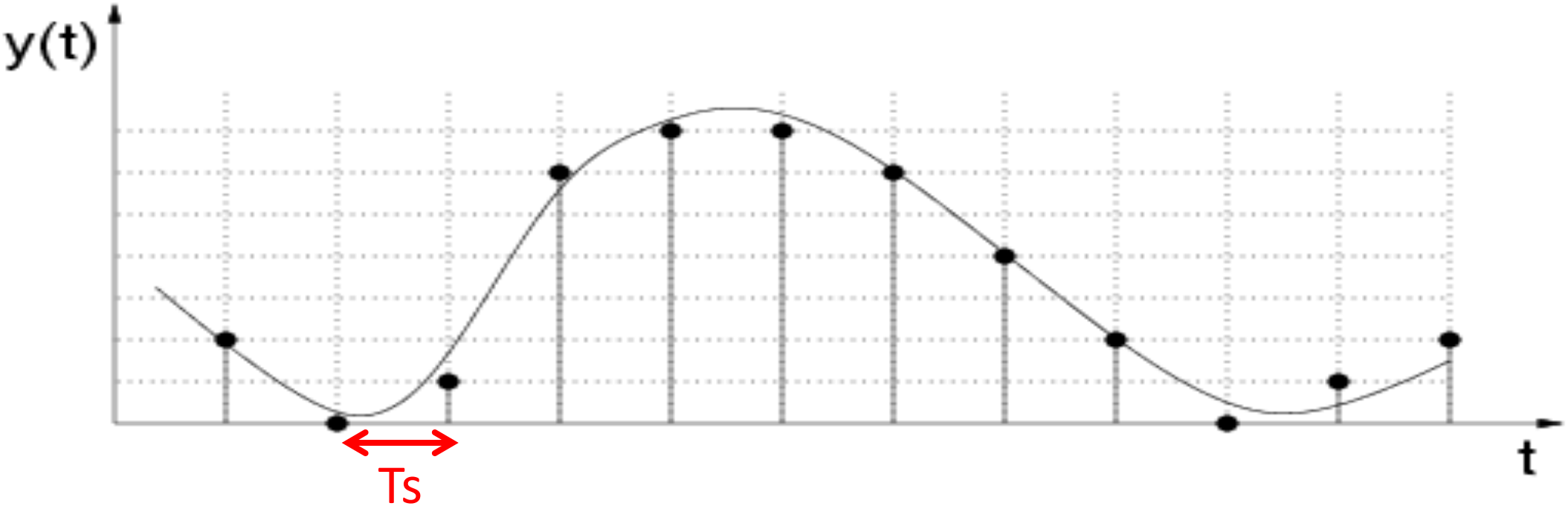
- Sampling Rate
- Number of bits to encode the signal (Quantization)





Example: PCM encoding (G.711)

Ts=125 μsec N=8 bit → N/Ts = 64 kbps



Example: PCM encoding (G.711)

Ts=125 μsec N=8 bit → N/Ts = 64 kbps

Fs = 8KHz

According to Shannon-Nyquist Theorem:

$Fs \geq 2B$

$B_{\text{Human Voice}} \approx (300\ \text{Hz} - 4\text{KHz})$

QoS (Quality of Service)

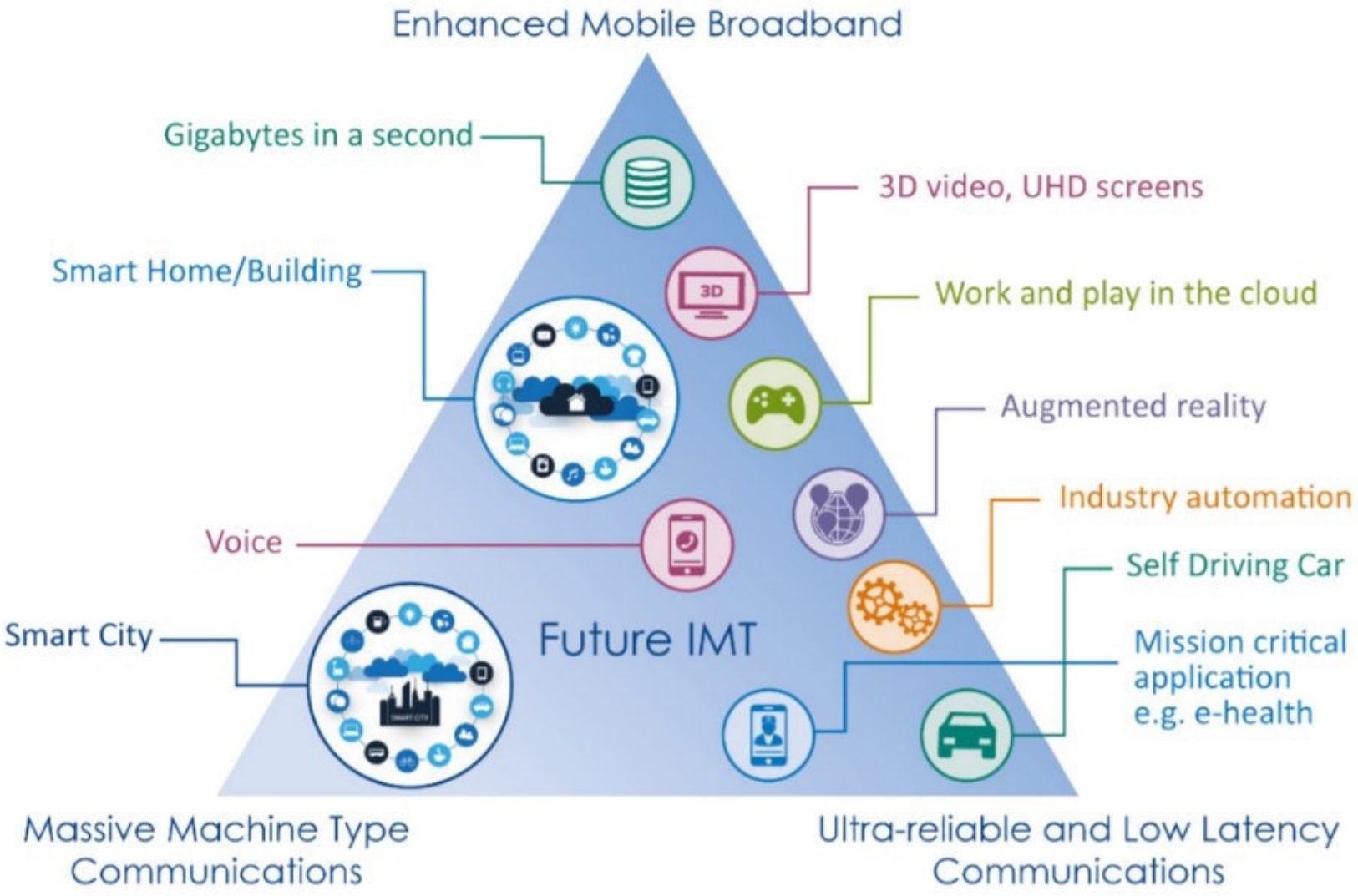
QoS is a major issue in VOIP implementations. The issue is how to guarantee that packet traffic for a voice or other media connection will not be delayed or dropped due interference from other lower priority traffic.

Parameters to consider:

- **Latency**: Delay for packet delivery
- **Jitter**: Variations in delay of packet delivery
- **Packet loss**: Too much traffic in the network causes the network to drop packets
- **Burstiness of Loss and Jitter**: Loss and Discards (due to jitter) tend to occur in bursts

IMT-2020 (5G)

5G usage scenarios



5G KeyPoints[1]

Extreme densification: more small-sized cells (pico-cells, femto-cells, distributed antennas) improves spectrum re-usage.

Increased Bandwidth: moving toward mmWave spectrum (up to 26 GHz for frequency assignment).

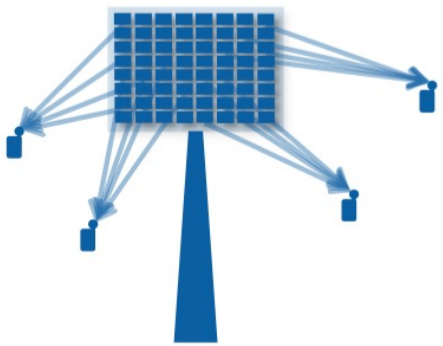
Increased Spectral efficiency: massive MIMO (myriad of tiny antennas on BSs).

[1] Andrews et al. "**What will 5G be?**" *IEEE Journal on Selected Areas in Communications*, vol. 32, n°6, Jun14.

Wireless Lead User Program Research Areas

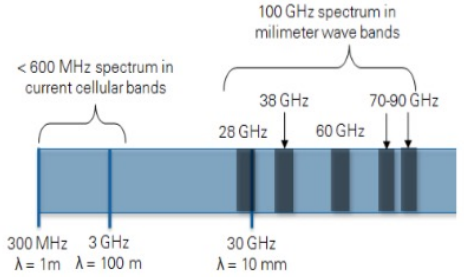
Massive MIMO

Dramatically increased number of antenna elements on base station enabling beamforming.



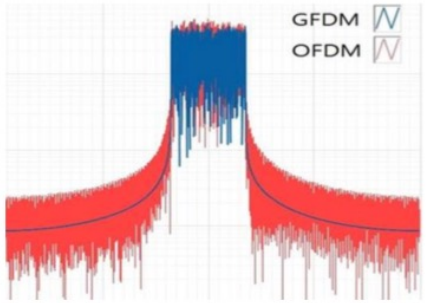
mmWave

Utilize potential of extremely wide bandwidths at frequency ranges once thought impractical for commercial wireless.



Multi Radio Access Technologies (RAT)

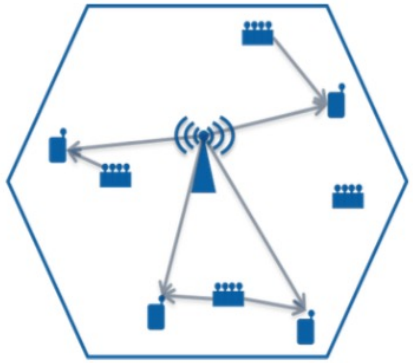
Improve bandwidth utilization through evolving PHY Level and flexible numerology

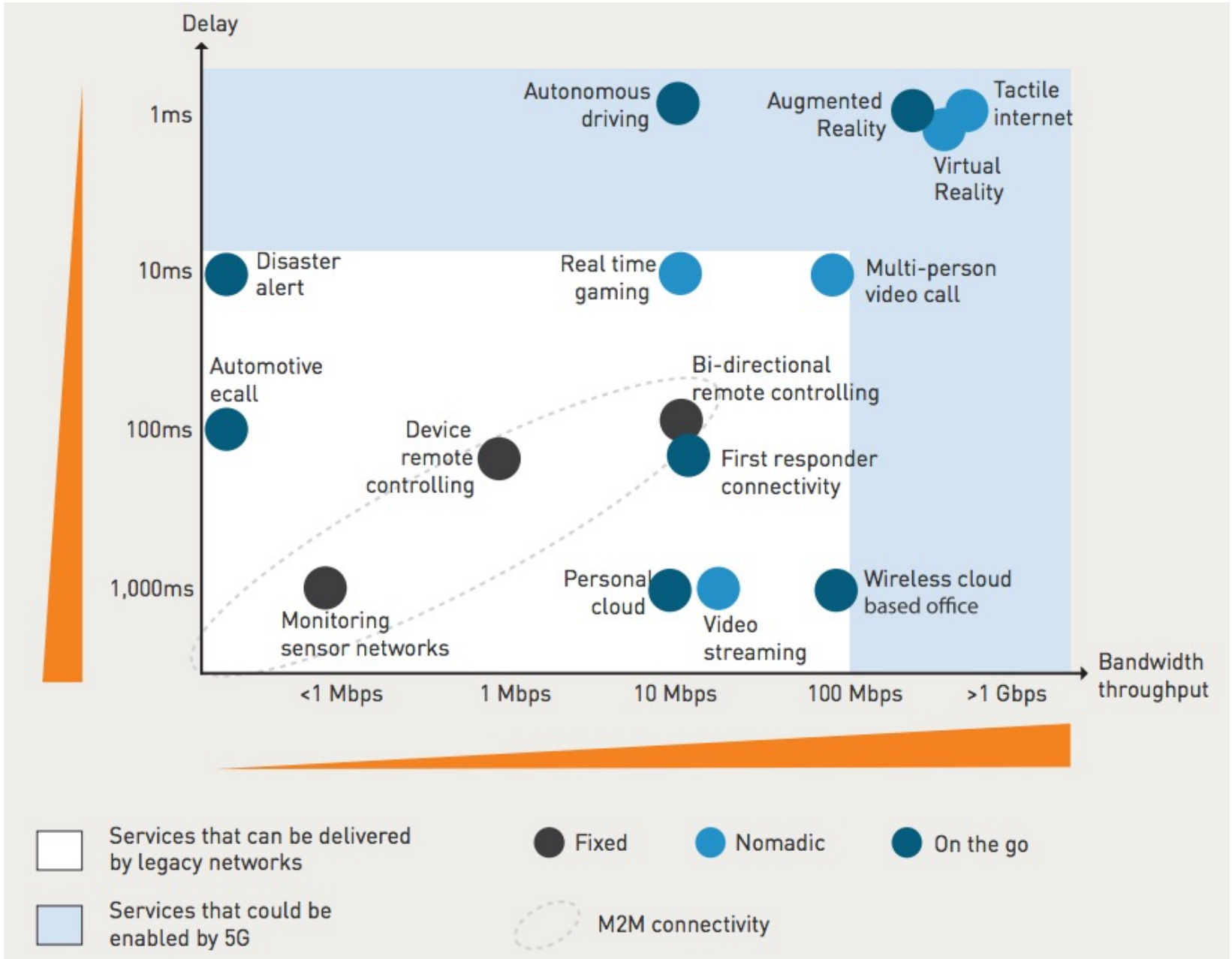


Wireless Networks

Consistent connectivity meeting the 1000x traffic demand for 5G

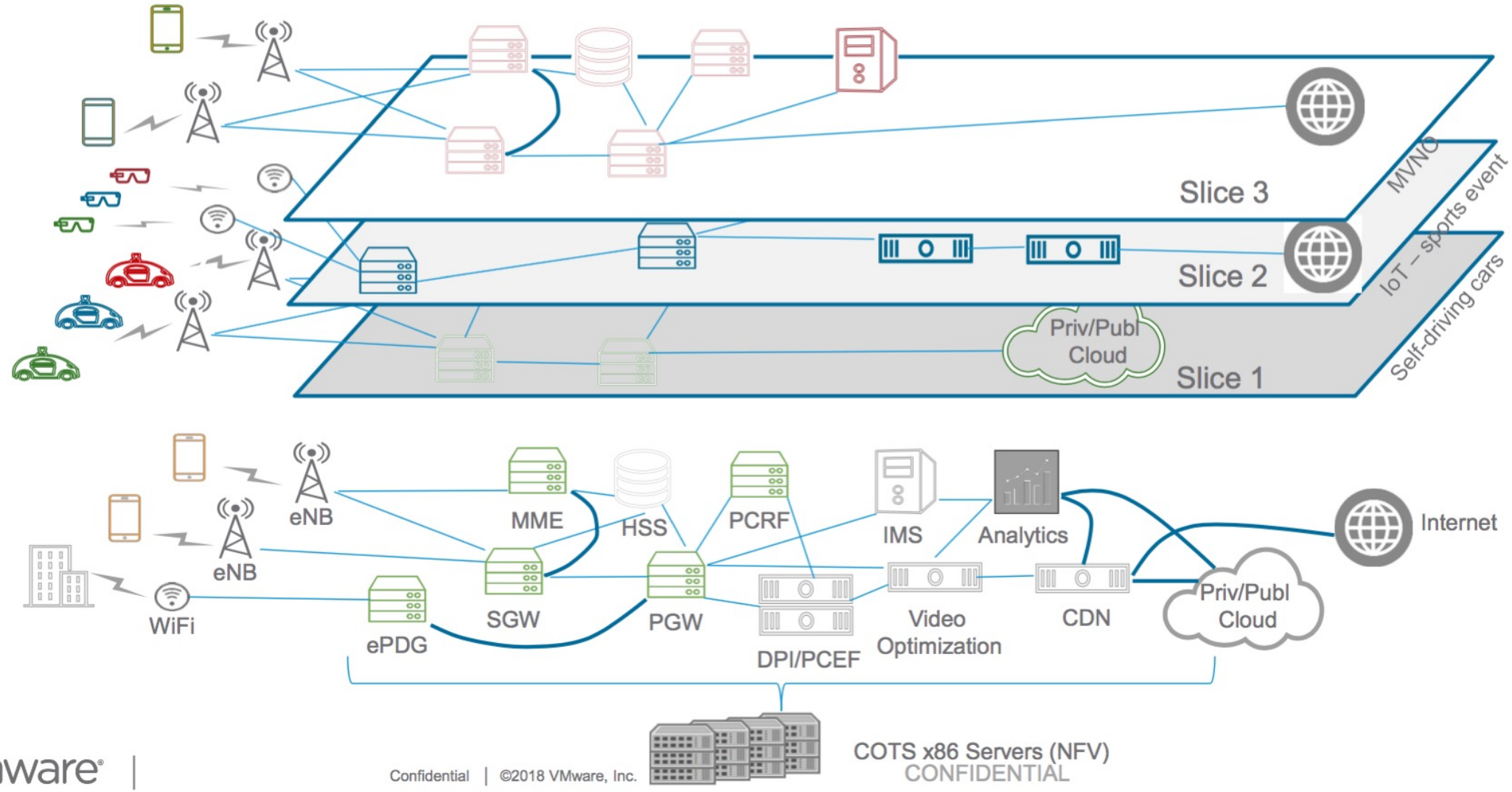
- Densification
- NFV
- SDN
- CRAN





Generation	Max speed	Aver. speed
2G	0.3 Mbps	0.1 Mbps
3G	7.2 Mbps	1.5 Mbps
3G+ (HSPA)	42 Mbps	5 Mbps
4G (LTE)	150 Mbps	10 Mbps
4G+ (LTE-A)	300 Mbps - 1 Gpbs	15 Mbps - 50 Mpbs
5G	1-10 Gbps	> 50 Mbps

Hierarchical Network Slicing: *Toward Virtual Service Networks*

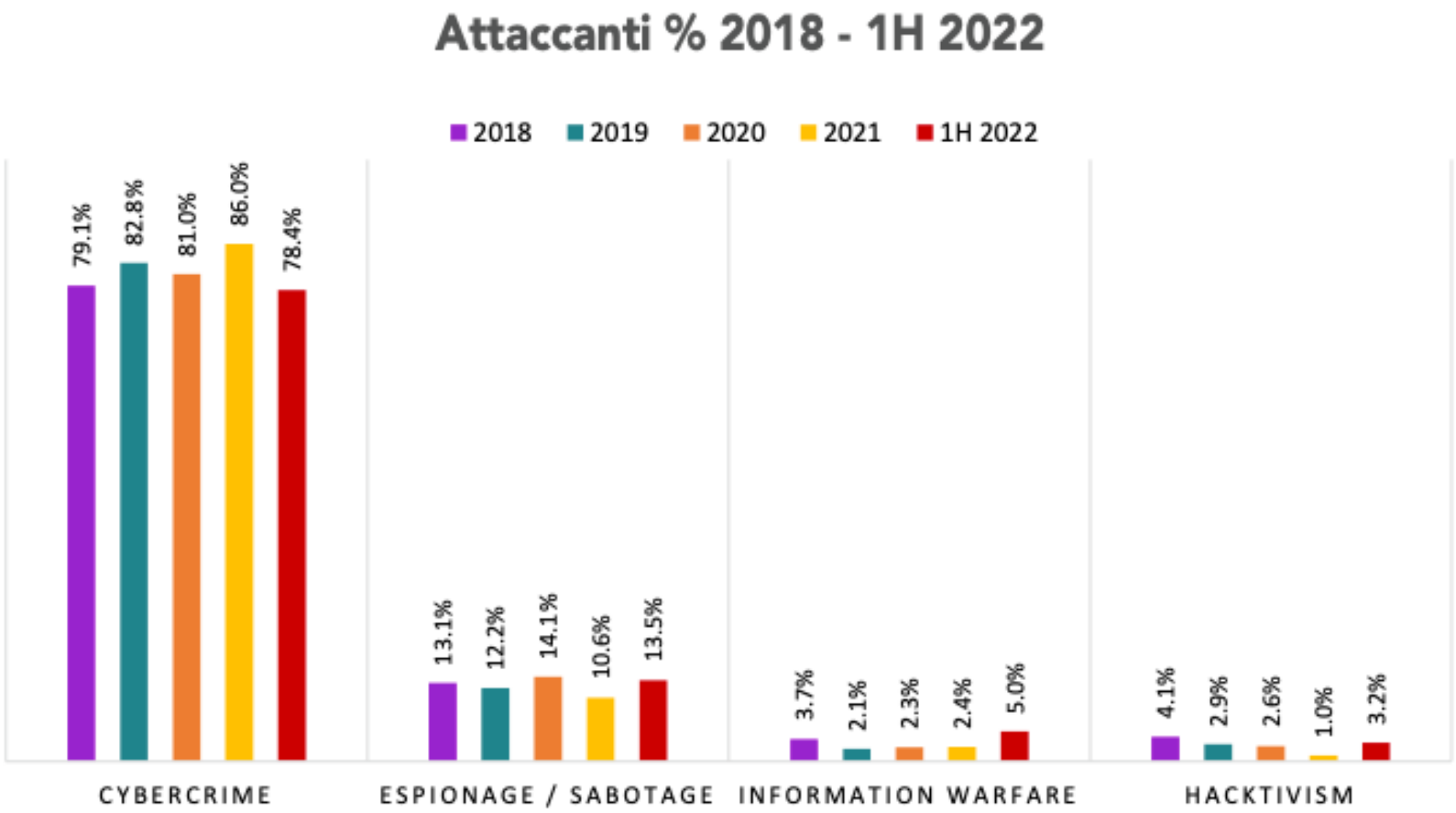


New Trends in Cybersecurity

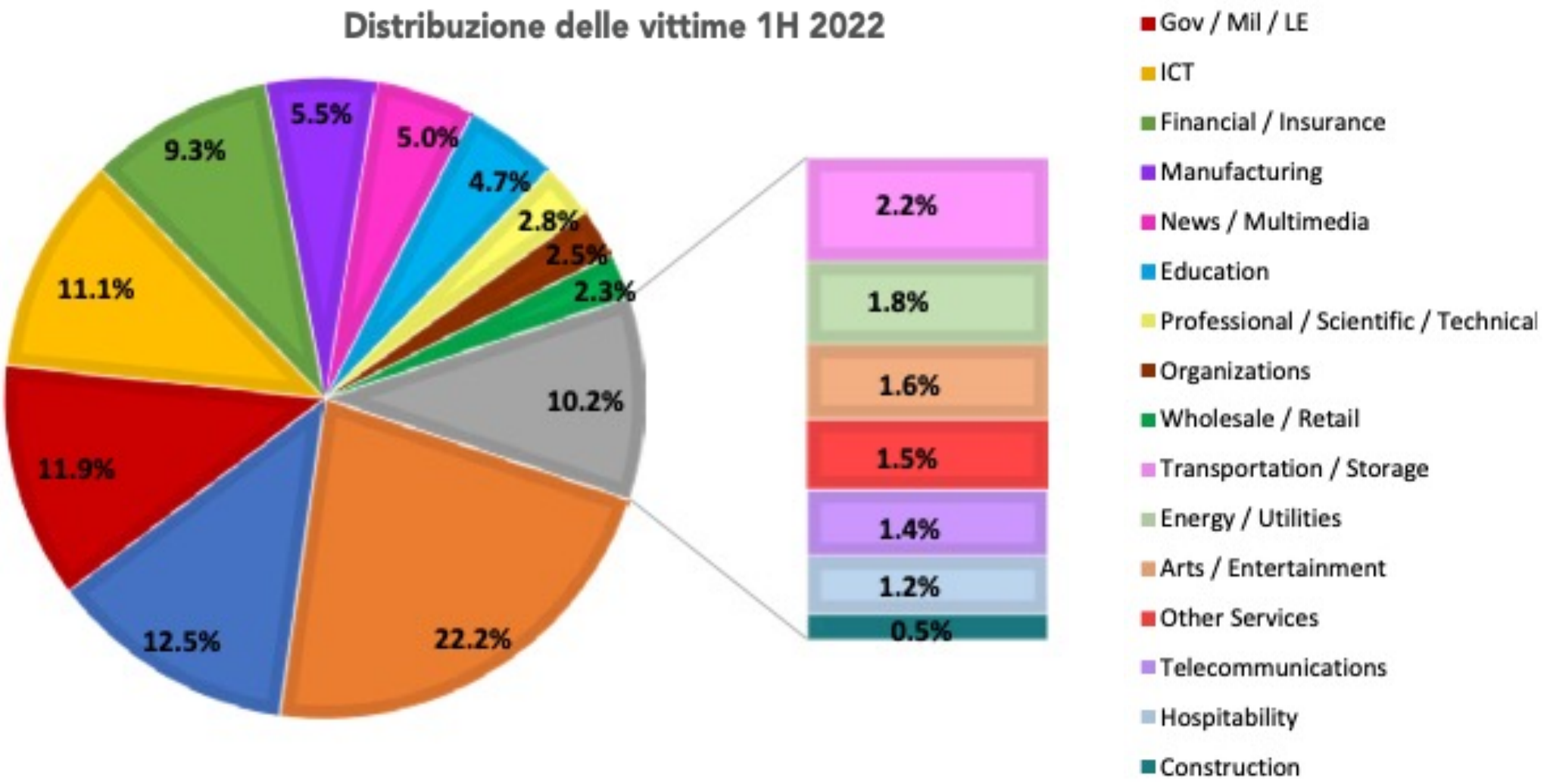
Distribuzione degli attaccanti per tipologia (2018 – 1H 2022)

ATTACCANTI PER TIPOLOGIA	2018	2019	2020	2021	1H 21	1H 22	1H 2021 su 1H 2022	Trend 2022
Cybercrime	1.229	1.381	1.518	1.763	925	894	-3.4%	↗
Espionage-Sabotage	203	203	264	217	95	154	62.1%	↑
Information Warfare	58	35	44	49	26	57	119.2%	↑
Hacktivism	64	48	48	20	7	36	414.3%	↑
Espionage-Sabotage + Inf. Warfare	261	238	308	266	121	211	74,4%	↑
Totale	1.554	1.667	1.874	2.049	1.053	1.141	+8,4%	↗

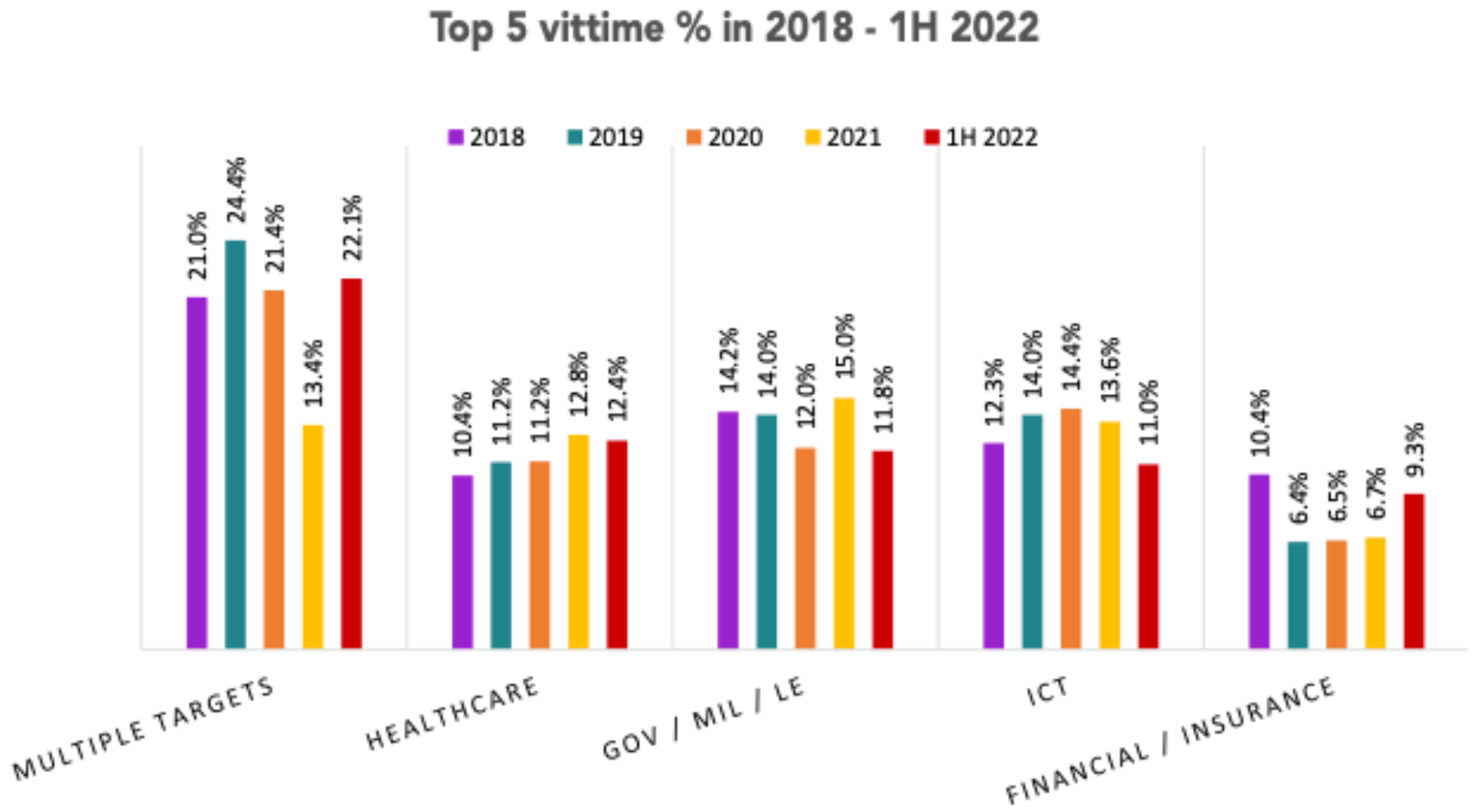
New Trends in Cybersecurity



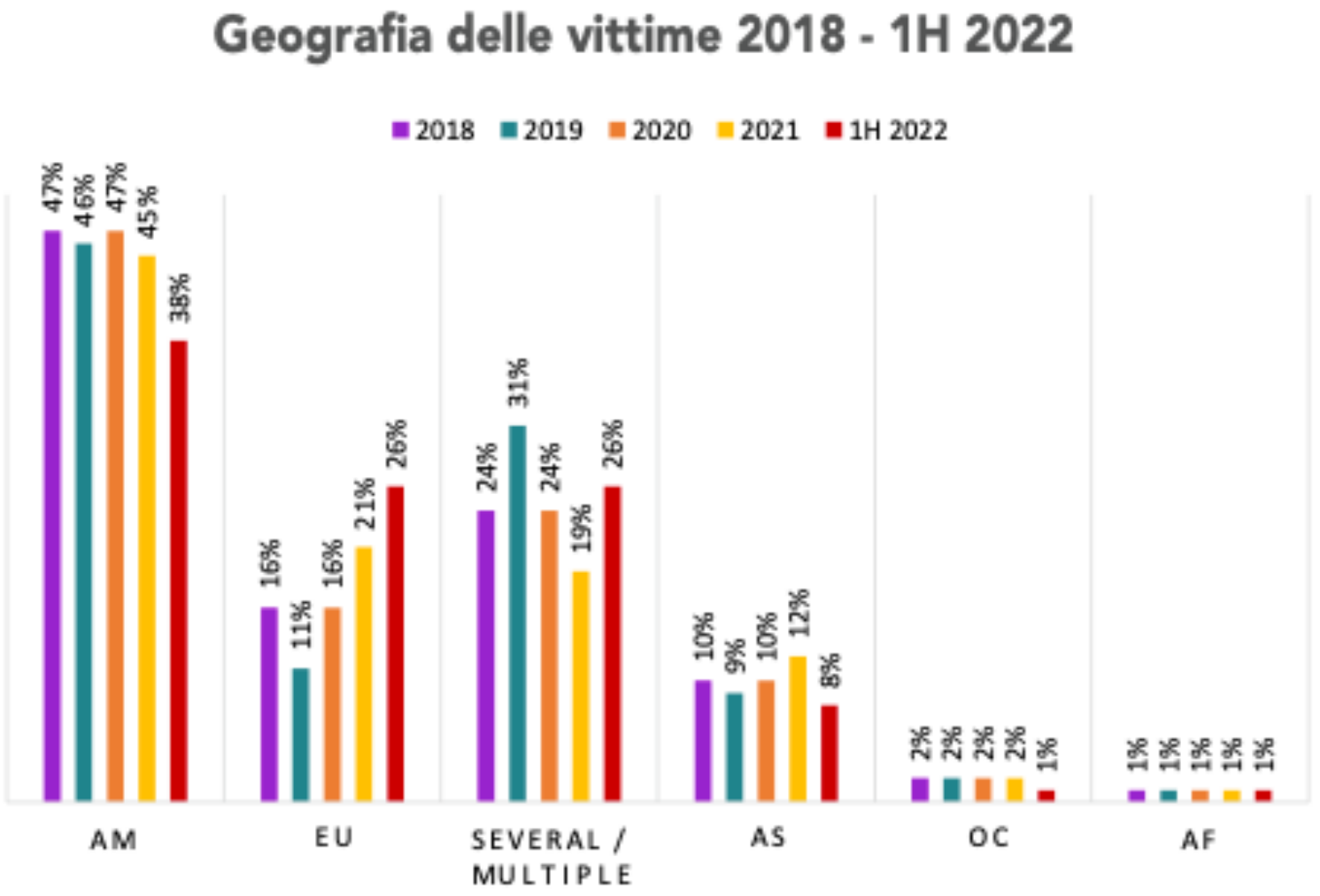
New Trends in Cybersecurity



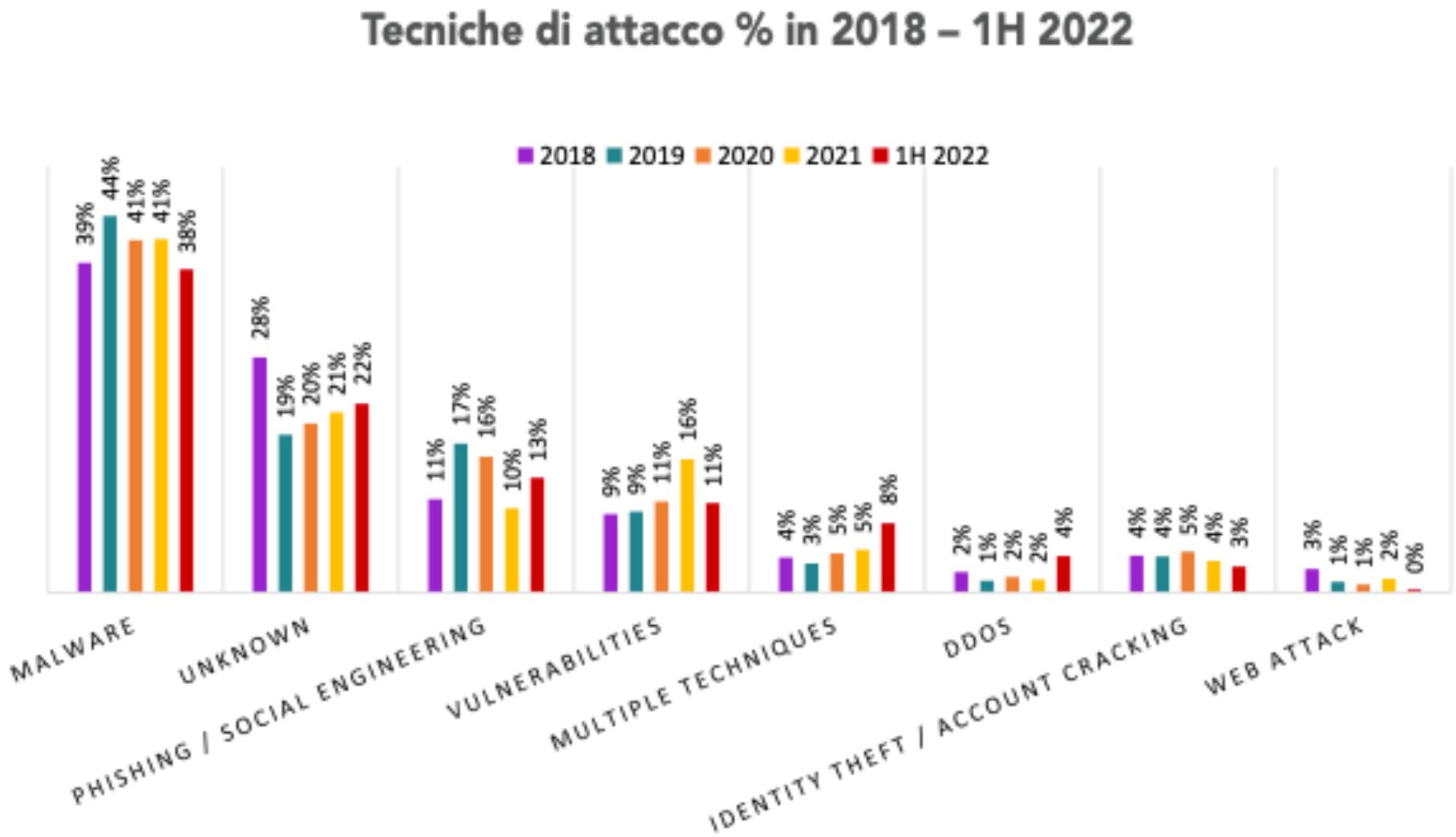
New Trends in Cybersecurity



New Trends in Cybersecurity

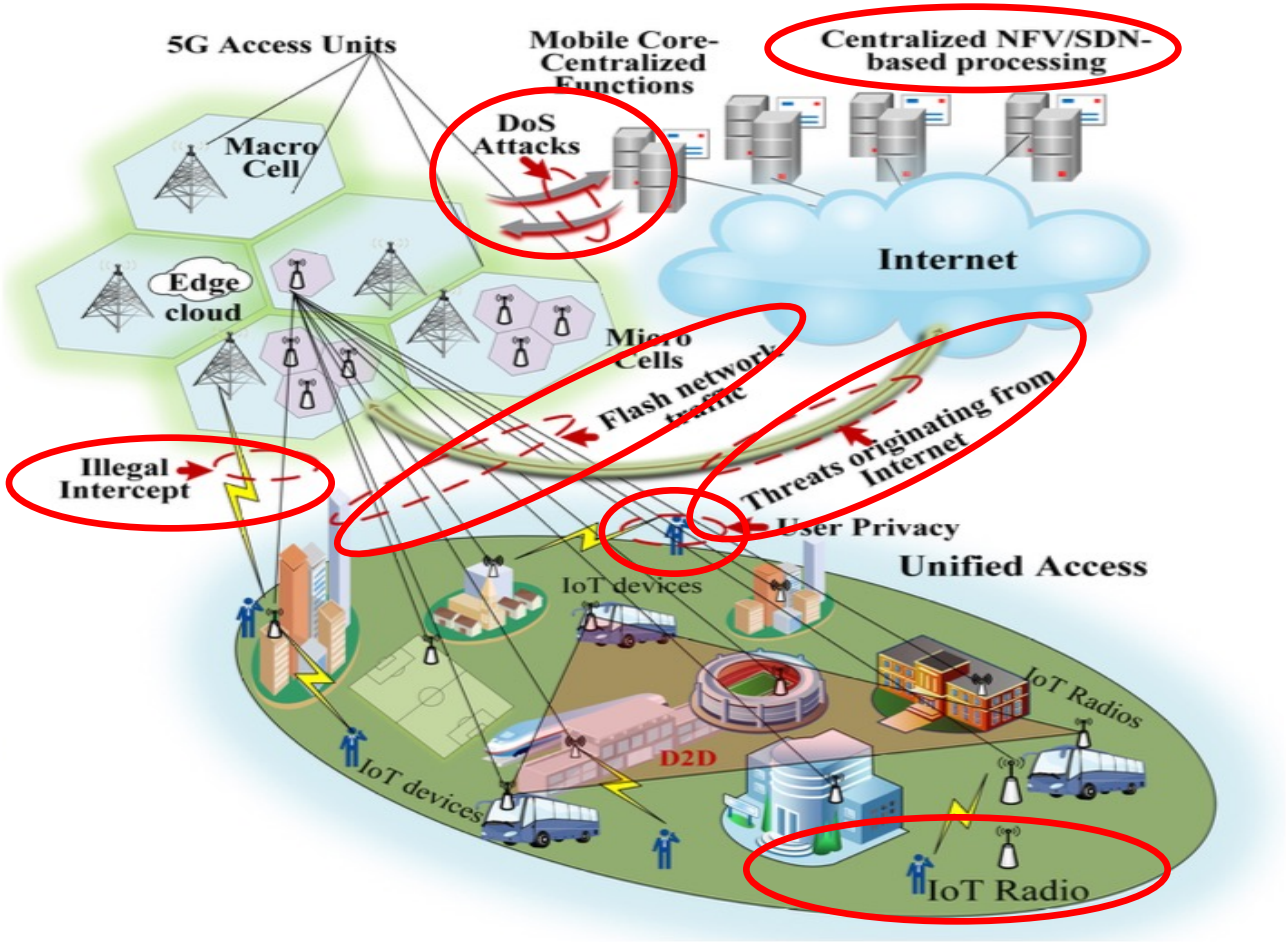


New Trends in Cybersecurity



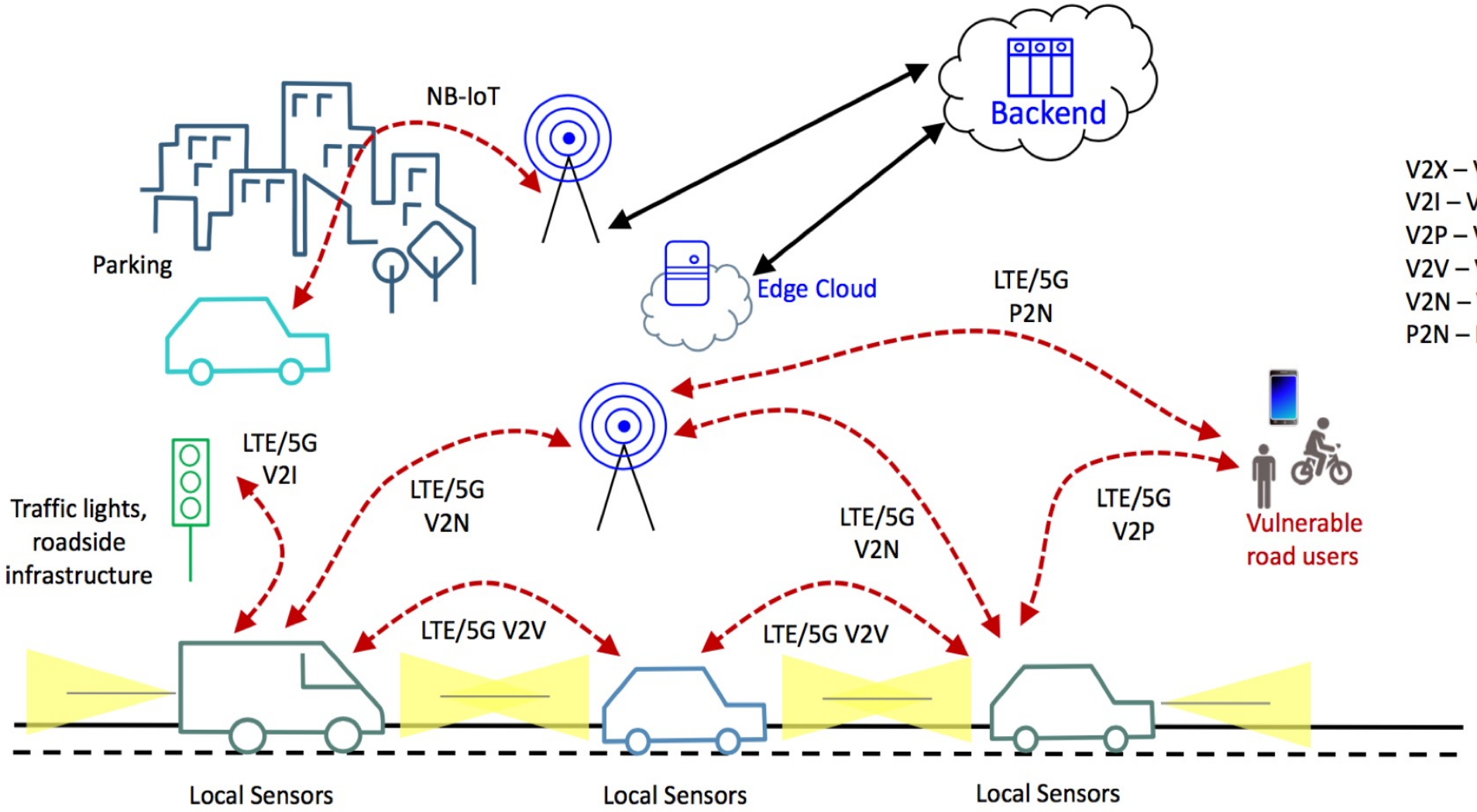
5G & IoT

- **Flash network traffic:** High number of end-user devices and new things (IoT).
- **Security of radio interfaces:** Radio interface encryption keys sent over insecure channels.
- **User plane integrity:** No cryptographic integrity protection for the user data plane.
- **Mandated security in the network:** Service-driven constraints on the security architecture leading to the optional use of security measures.
- **Roaming security:** User-security parameters are not updated with roaming from one operator network to another, leading to security compromises with roaming.
- **Denial of Service (DoS) attacks on the infrastructure:** Visible nature of network control elements, and unencrypted control channels.
- **Signaling storms:** Distributed control systems requiring coordination, e.g. Non-Access Stratum (NAS) layer of Third Generation Partnership Project (3GPP) protocols.
- **DoS attacks on end-user devices:** No security measures for operating systems, applications, and configuration data on user devices.



**Source: 5G Security: analysis of Threats and Solutions (Ahmad et al., IEEE CSCN17)*

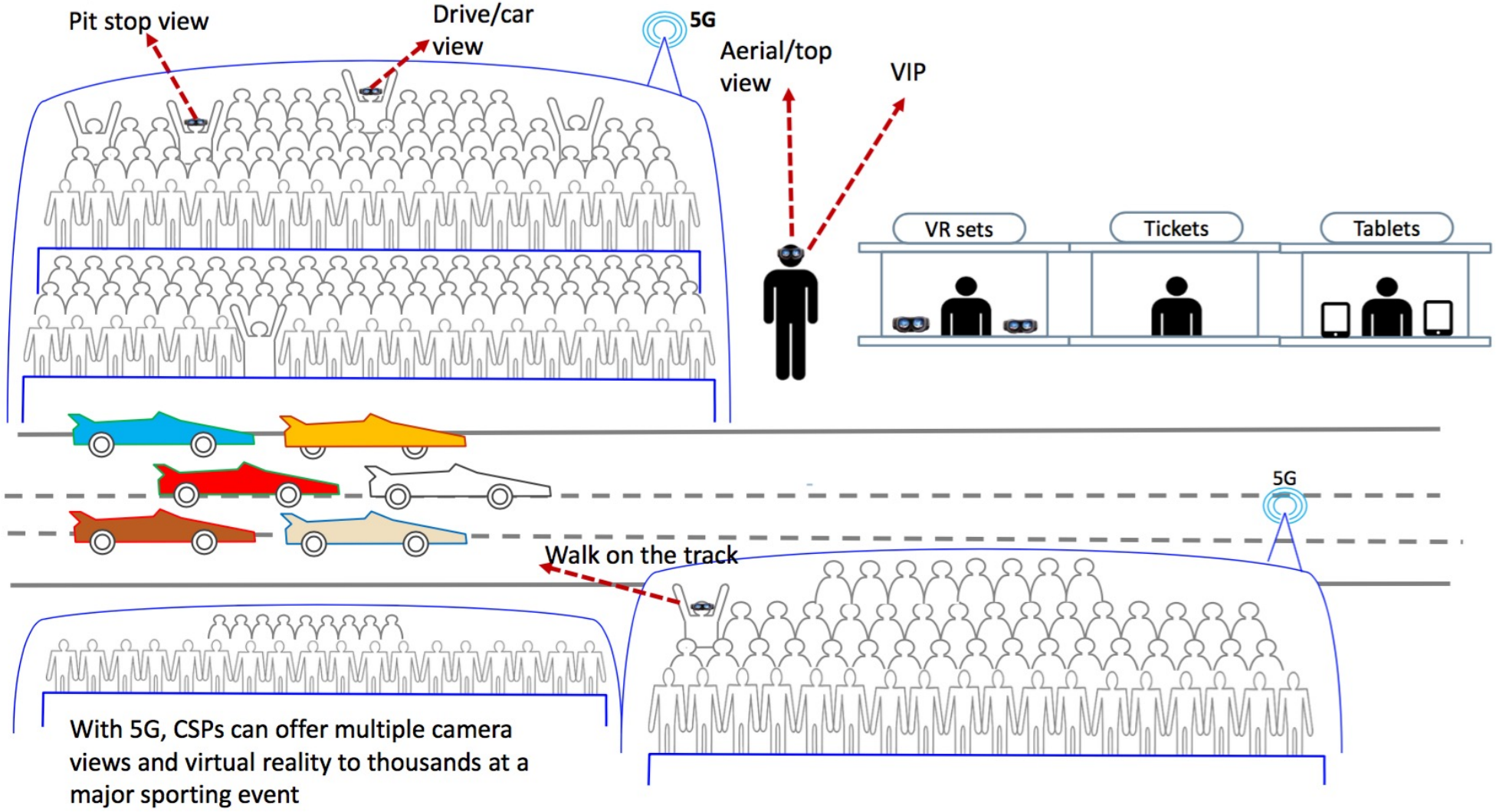
Cellular V2X Concept



V2X – Vehicle to Everything
V2I – Vehicle to Infrastructure
V2P – Vehicle to Pedestrian
V2V – Vehicle to Vehicle
V2N – Vehicle to Network
P2N – Pedestrian to Network

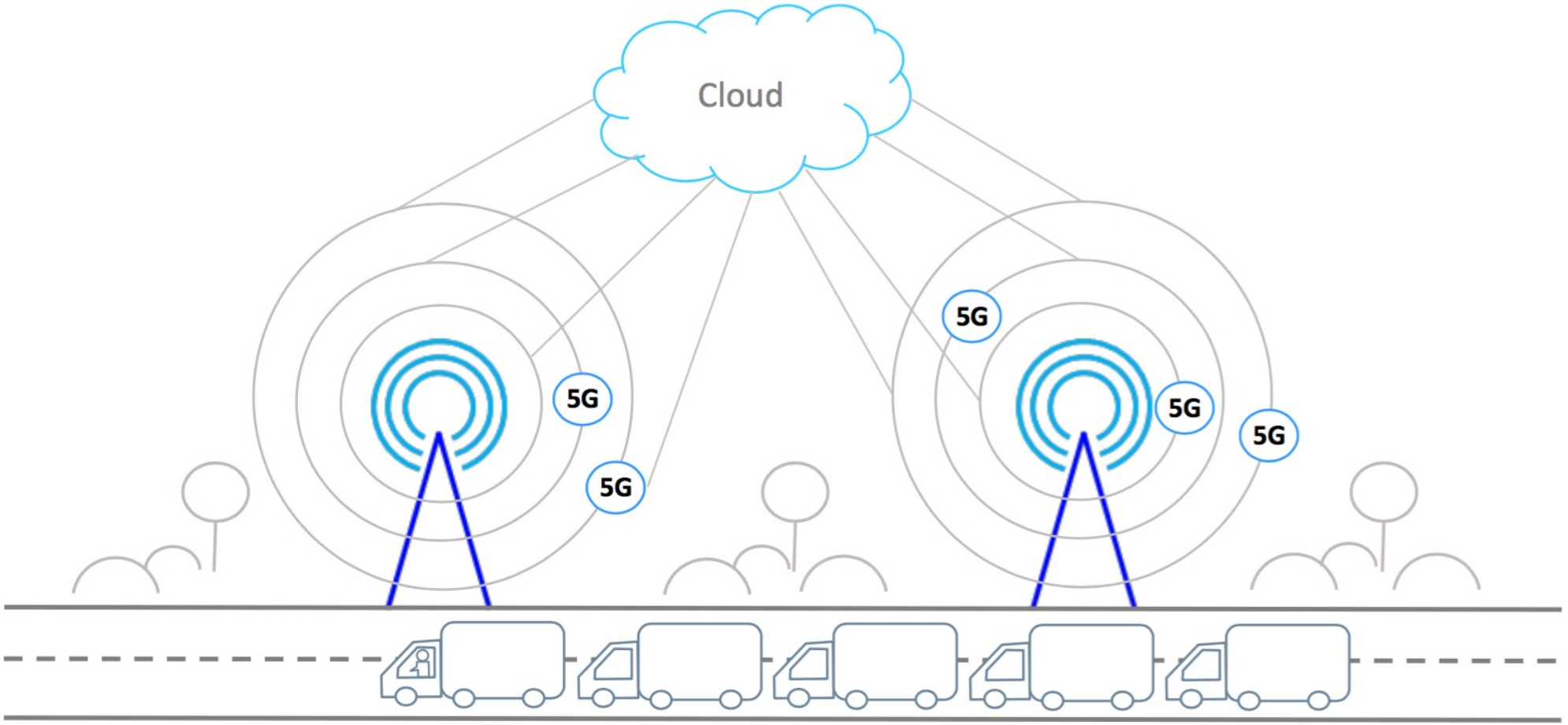
Source: Nokia

5G Connected Stadiums



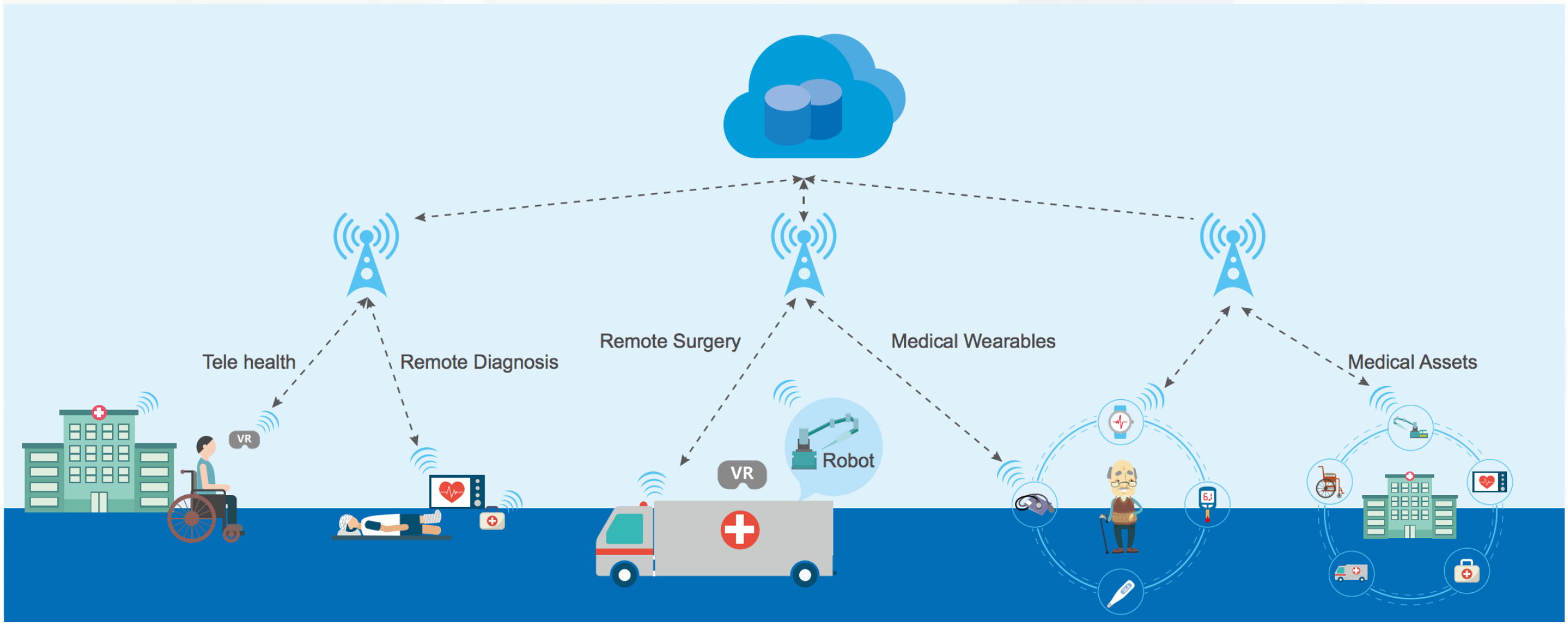
Source: Nokia

5G Autonomous Driving: Platooning

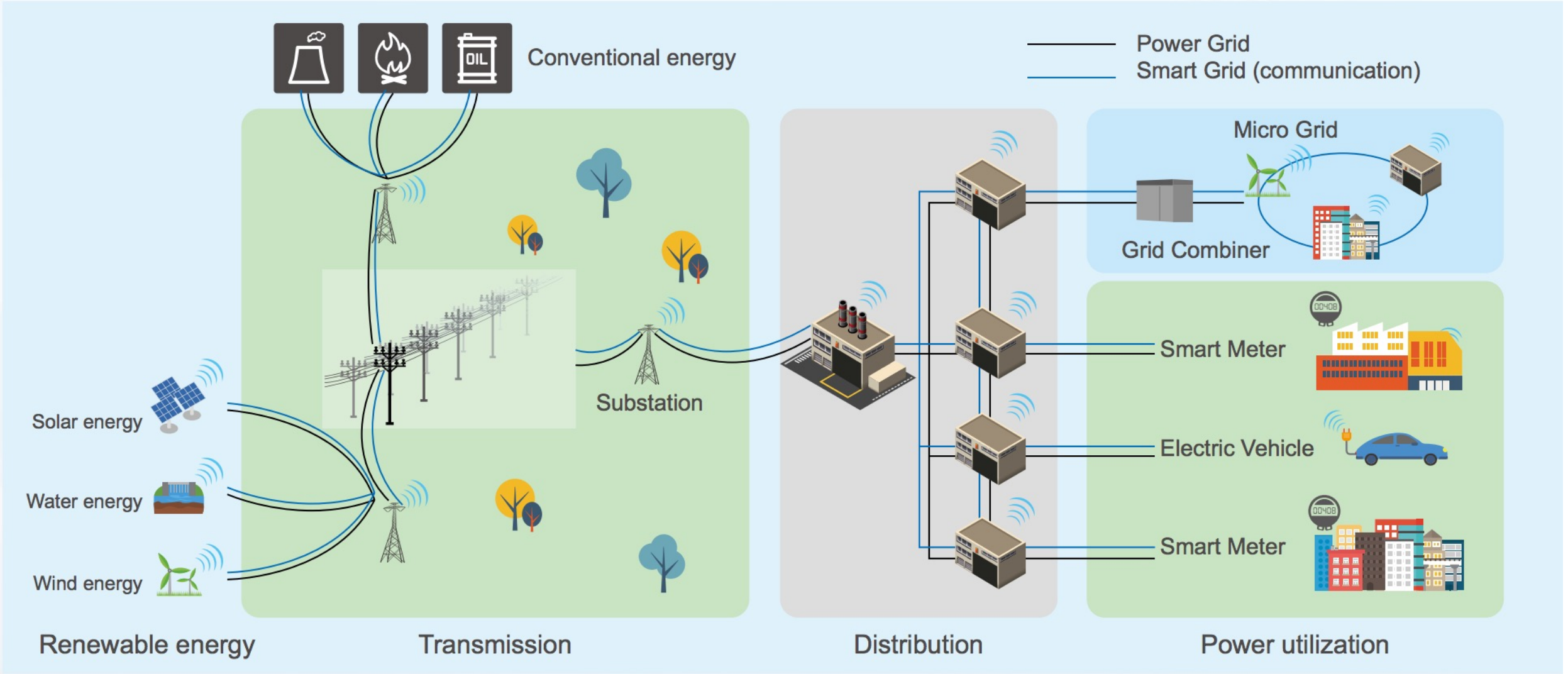


5G is the most promising enabler of truck platooning in which long convoys of trucks are automatically governed and require only a single driver in the lead vehicle

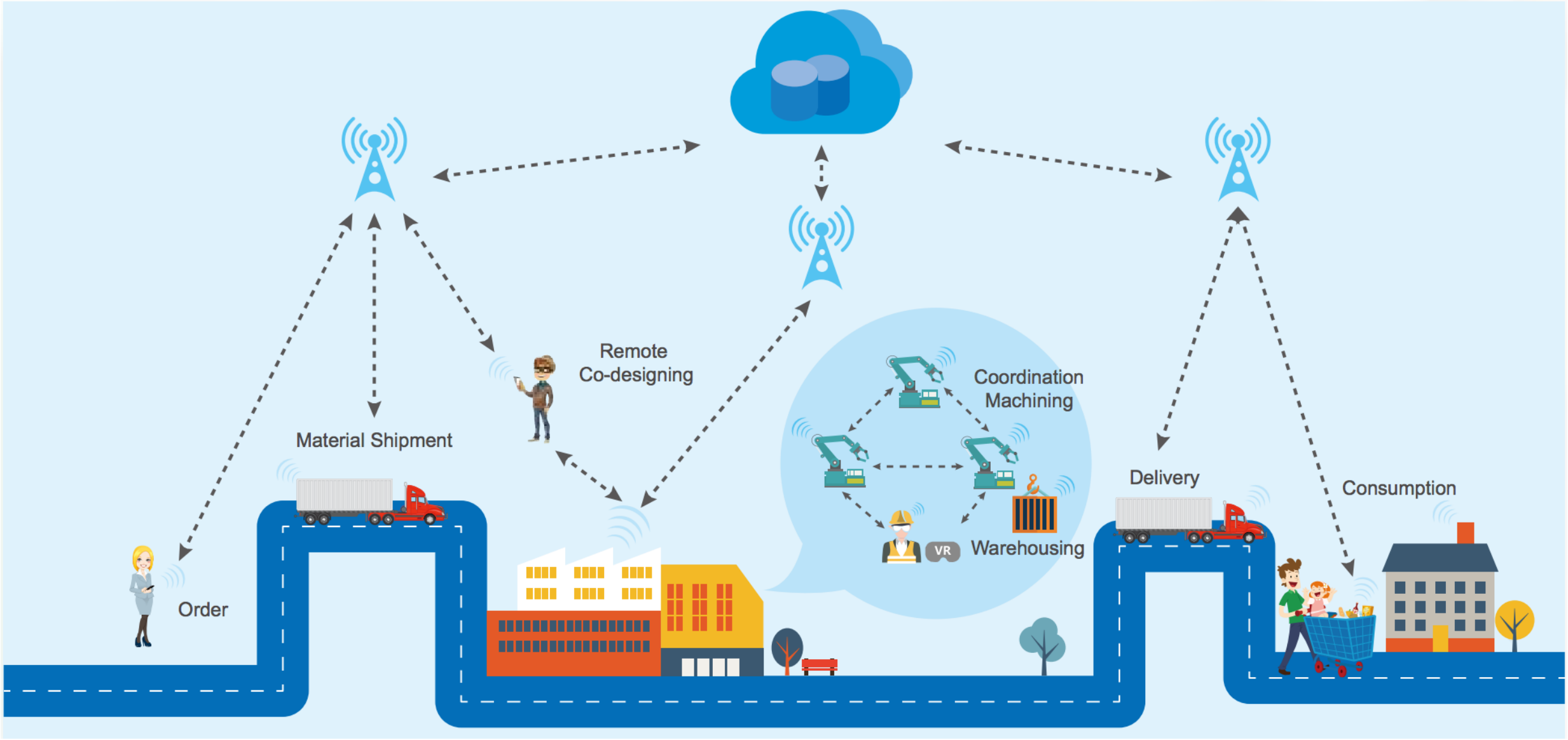
Source: Nokia



Huawei: Remote Health

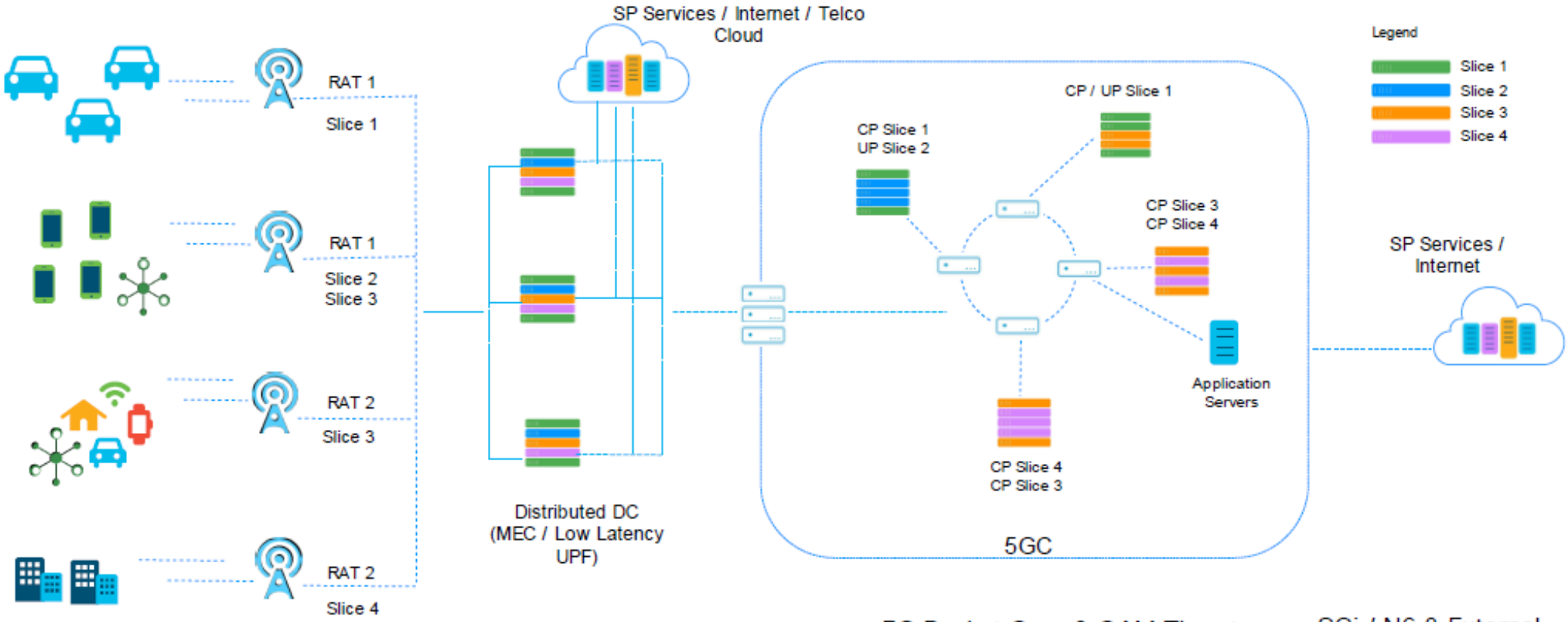


Huawei: Smart Energy



Huawei: Smart Manufacturing

Threats in 5G & Evolving Architectures



Device Threats
- Malware
- Sensor Susceptibility
- TFTP MitM attacks
- Bots DDoS
- Firmware Hacks
- Device Tampering

Air Interface Threats
- MitM attack
- Jamming

RAN Threats
- MEC Server Vulnerability
- Rogue Nodes

Backhaul Threats
- DDoS attacks
- CP / UP Sniffing
- MEC Backhaul sniff
- API vulnerabilities

5G Packet Core & OAM Threats
- Virtualization
- Network Slice security
- API vulnerabilities
- IoT Core integration
- Roaming Partner vulnerabilities
- DDoS & DoS attacks
- Improper Access Control

SGi / N6 & External Roaming Threats
- IoT Core integration
- VAS integration
- App server vulnerabilities
- Application vulnerabilities
- API vulnerabilities

Thanks for your attention!