ORTA DOĞU TEKNİK ÜNİVERSİTESİ
MIDDLE EAST TECHNICAL UNIVERSITY

Securing The Internet of Mobile Things in the World of 5G and Beyond

PELIN ANGIN

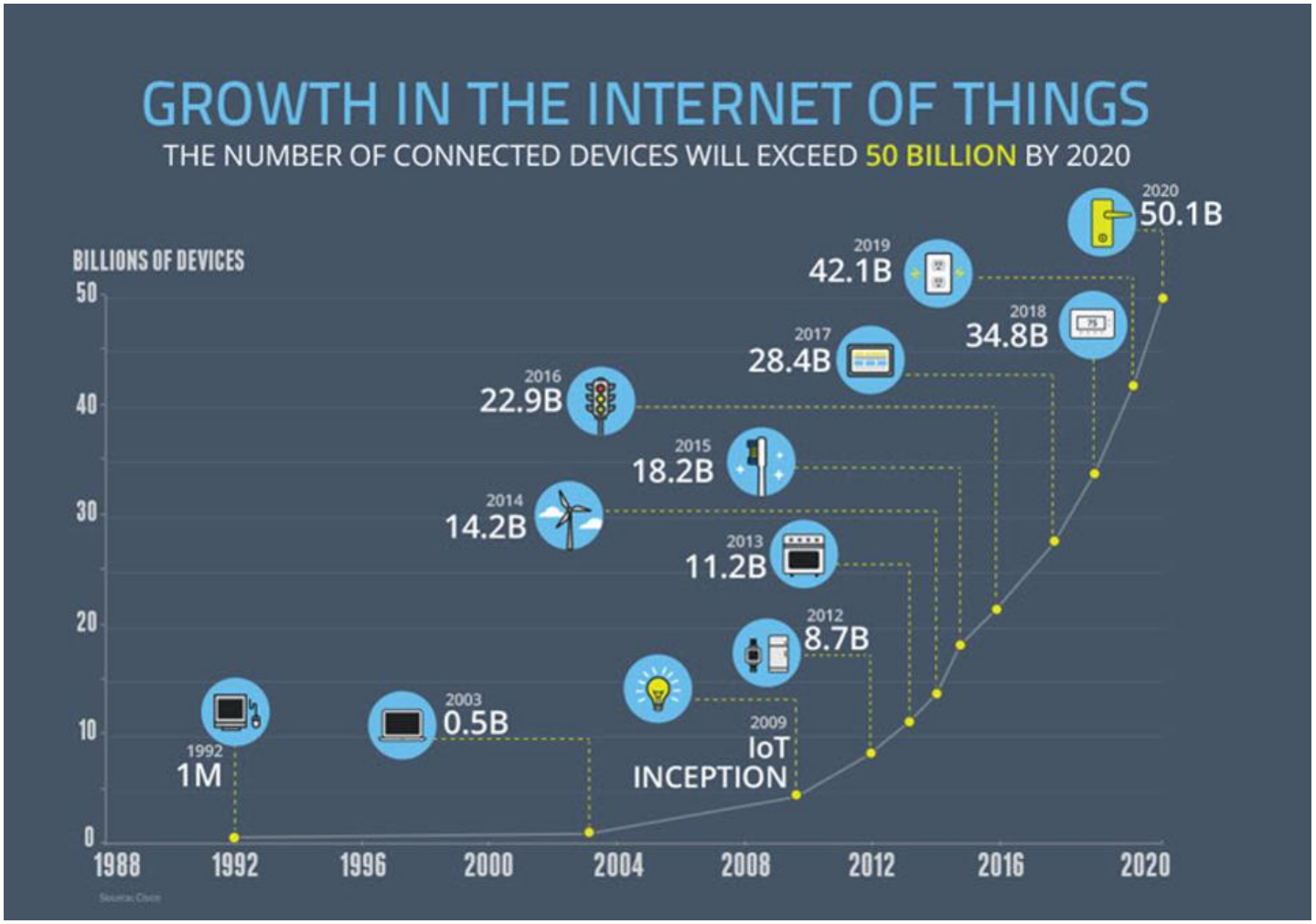
NOVEMBER 23, 2020

METU SYSTEMS SECURITY RESEARCH LABORATORY (S2RL),
METU WIRELESS SYSTEMS, NETWORKS AND CYBERSECURITY LABORATORY (WINS)

IoT: Now Everywhere

Source: https://www.jigsawacademy.com/iot/

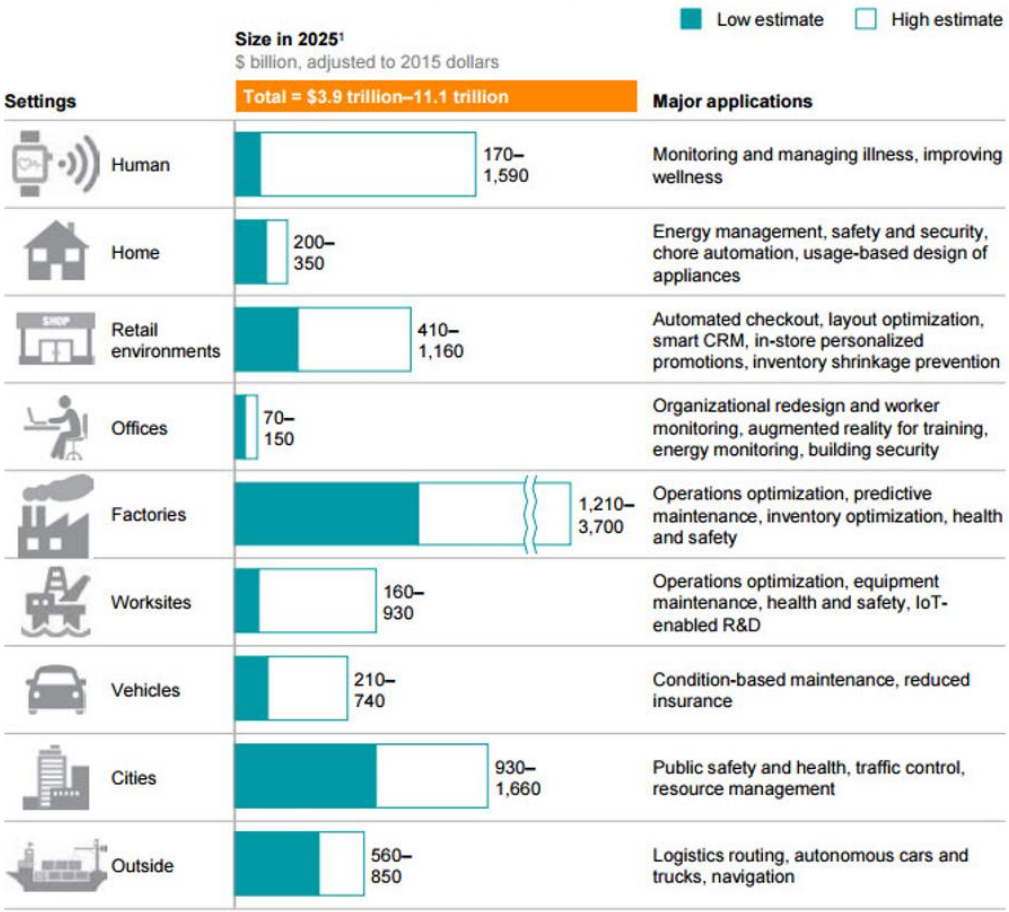
And Growing Very Fast…



Source:
https://www.forbes.com/sites/louiscolumbus/2015/12/27/roundup-of-internet-of-things-forecasts-and-market-estimates-2015/2/#2b677f9f5fa7

With Very High Economic Impacts

Potential economic impact of IoT in 2025, including consumer surplus, is $3.9 trillion to $11.1 trillion



1 Includes sized applications only.
NOTE: Numbers may not sum due to rounding.

SOURCE: McKinsey Global Institute analysis

IoMT

Source: https://www.jigsawacademy.com/iot/

How Secure is IoT?

1

2

3

4

1. https://ahmedbanafa.blogspot.com.tr/2016/10/a-wake-up-call-for-iot.html
2. https://thehacktoday.com/hackers-can-easily-hijack-popular-baby-monitors-to-watch-your-kids
3. https://thehackernews.com/2015/02/smart-tv-spying.html
4. https://www.thedailybeast.com/the-terrifying-us-israeli-computer-worm-that-could-cause-world-war-iii

How Secure is IoMT?

https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

And AI on Top of All…

Offensive AI: a paradigm shift in cyberattacks

1. Impersonation of trusted users
2. Blending into the background
3. Faster attacks with more effective consequences

https://www.weforum.org/agenda/2019/06/ai-is-powering-a-new-generation-of-cyberattack-its-also-our-best-defence/

IoT Security Problems

- Confidentiality
- Device authentication
- Enlarged attack surface
- Data integrity
- Distributed denial of service (DDoS)
- Repudiation
- Device capacity constraints

Security Not The Only Problem for IoMT

- Low latency
- Ultra-reliable communications
- High bandwidth
- Low energy

What Does 5G Promise?

5G Use Cases & Requirements

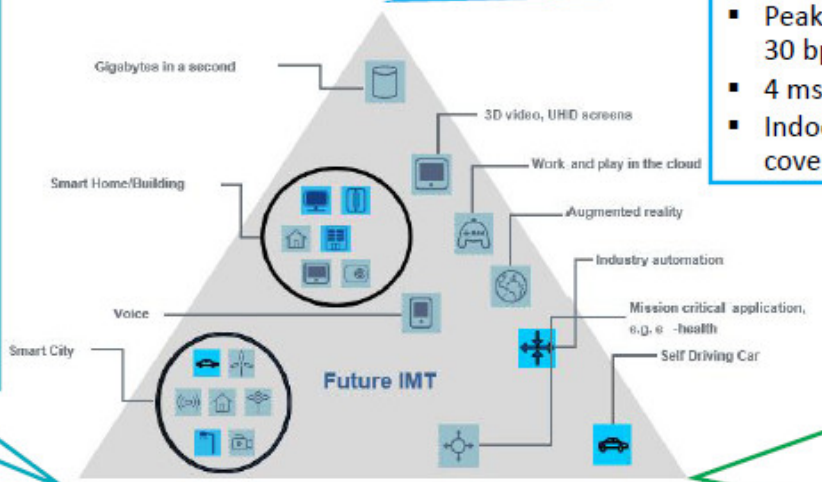
Key challenge for 5G design: support for different services having diverging requirements

Massive Machine Type Communications (mMTC)

- Low data rates (1 to 100 kbps)
- High device density (up to 1,000,000 /km^2)
- Latency: Seconds to hours
- Low power: Up to 15 years battery life

Enhanced Mobile Broadband (eMBB)

- Peak data rates: 20 Gbps (DL) and 10 Gbps (UL)
- Peak spectral efficiency: 30 bps/Hz (DL) and 15 bps/Hz (UL)
- 4 ms user plane latency
- Indoor/hotspot and enhanced wide-area coverage



Source: ITU-R SG5 WP-5D

Ultra-Reliable and Low Latency Communications (URLLC)

- Low to medium data rates (50 kbps to 10 Mbps)
- 0.5 ms user plane latency
- 99.999% reliability and availability within 1 ms
- High mobility

3

© 2019 InterDigital, Inc. All Rights Reserved

INTERDIGITAL.

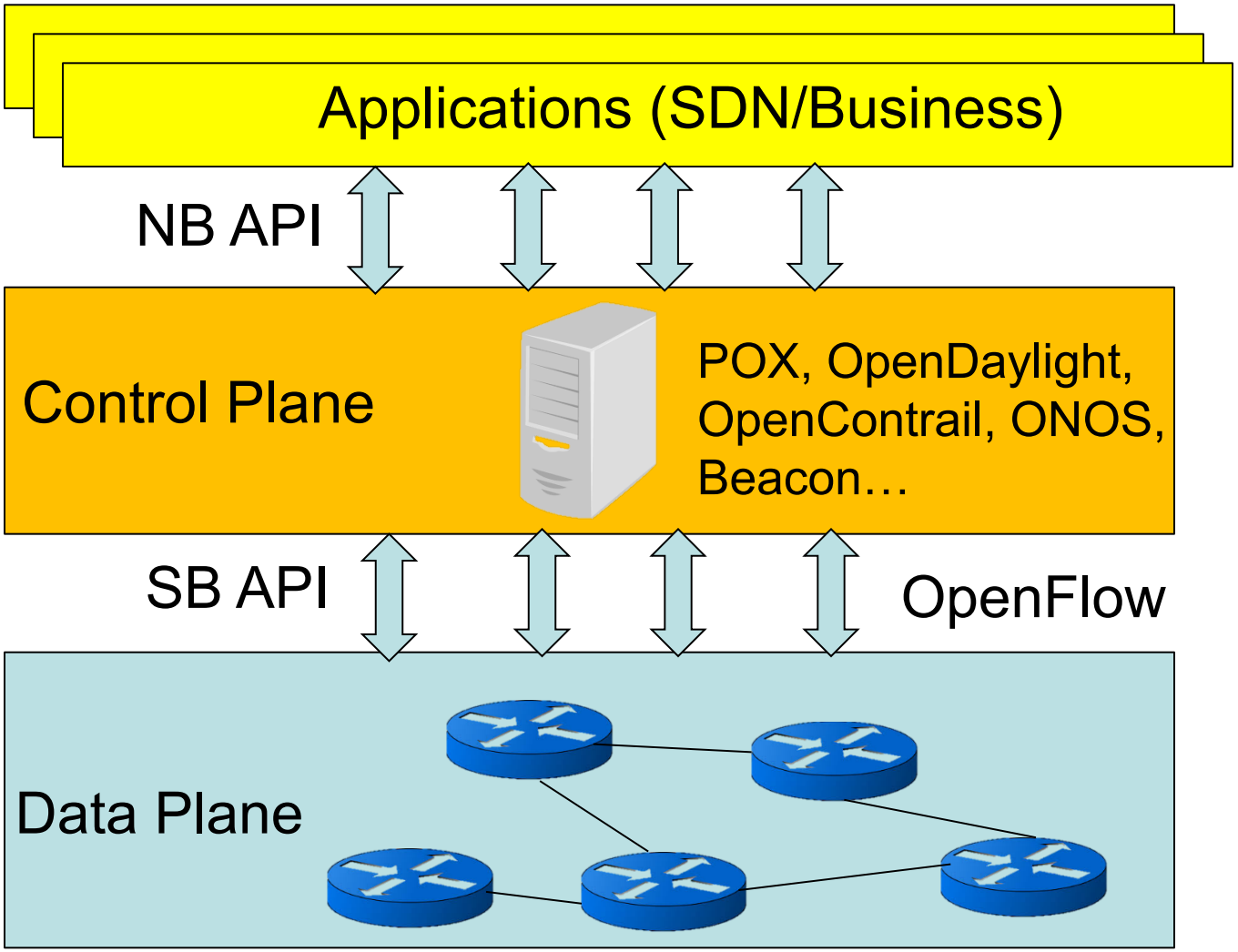
http://telecoms.com/495842/5g-reaches-an-anticlimax-at-mwc-2019/

Two Key Enablers

Software Defined Networking

Network Slicing

SDN Architecture



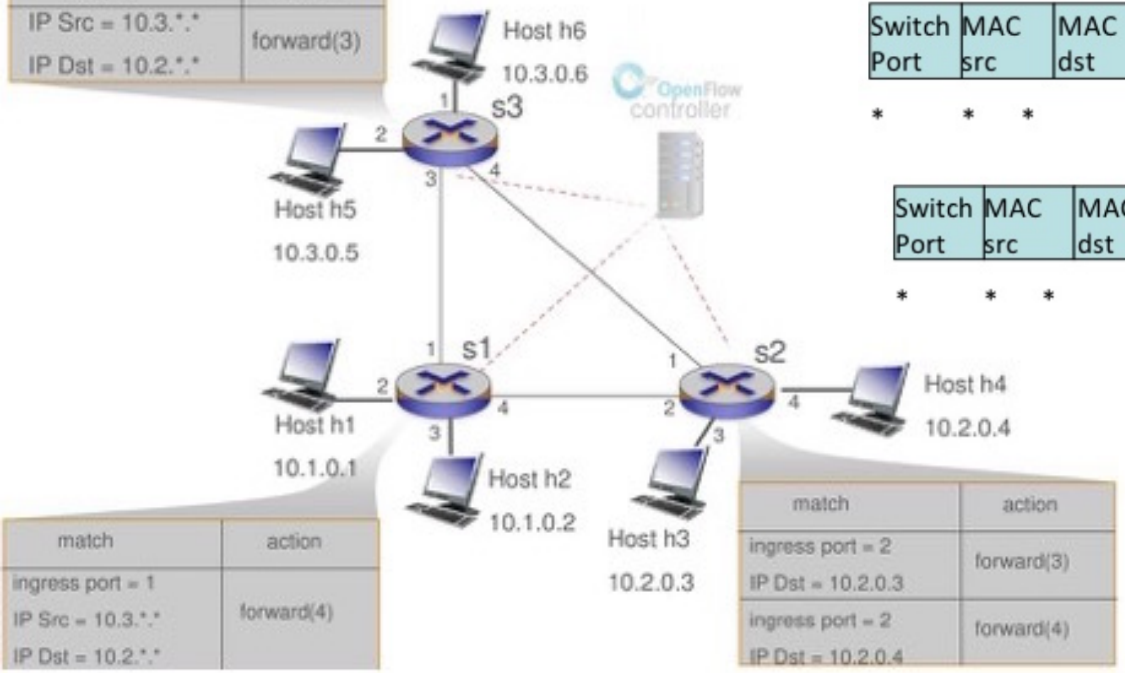
A key enabler for 5G due to the high **flexibility** & **scalability** needs!

OpenFlow

Header Fields	Counters	Actions

Ing Port	Eth Src	Eth Dst	Eth Type	VLAN ID	VLAN Prio	IP Src	IP Dst	IP Proto	IP ToS	Port Src	Port Dst

match	action
IP Src = 10.3.*.* IP Dst = 10.2.*.*	forward(3)



match	action
ingress port = 1 IP Src = 10.3.*.* IP Dst = 10.2.*.*	forward(4)

match	action
ingress port = 2 IP Dst = 10.2.0.3	forward(3)
ingress port = 2 IP Dst = 10.2.0.4	forward(4)

Switch Port	MAC src	MAC dst	Eth type	VLAN ID	IP Src	IP Dst	IP Prot	TCP sport	TCP dport	Action
*	*	*	*	*	*	5.6.7.8	*	*	*	port6

Switch Port	MAC src	MAC dst	Eth type	VLAN ID	IP Src	IP Dst	IP Prot	TCP sport	TCP dport	Action
*	*	*	*	*	*	*	*	*	22	drop

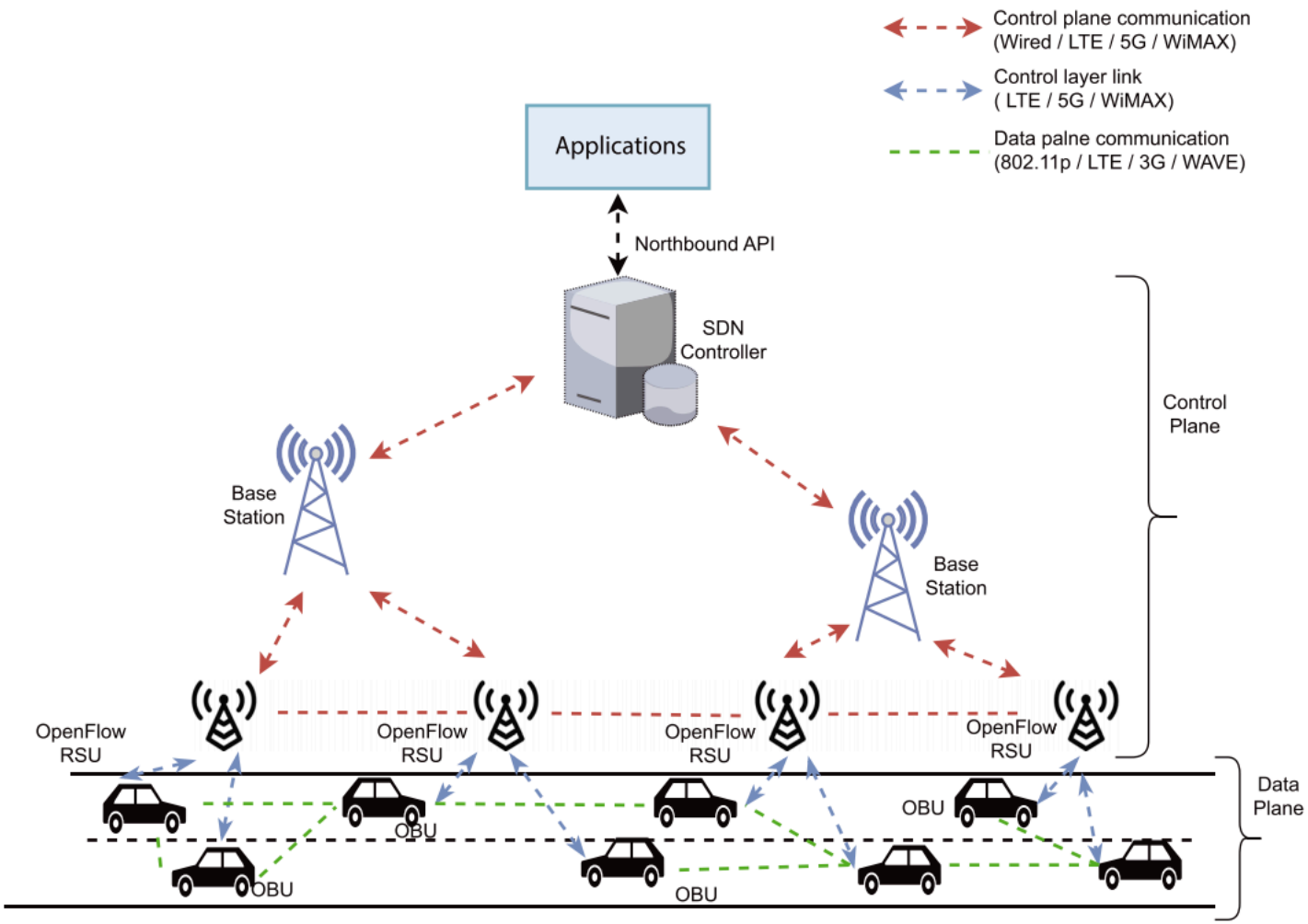
* Figures from “Computer Networking: A Top Down Approach” by Kurose and Ross

SDN: An Enabler for Network Security

- Easier collection of network usage information
  - Support for improved algorithm design for detecting attacks
- Improved policy enforcement
- Improved anomaly detection
- Intelligent response through selective blocking of malicious traffic
- Acting on anomalies by diverting specific flows to special enforcement points/security services

https://www.business.att.com/learn/tech-advice/the-security-benefits-of-software-defined-networking--sdn-.html#

Use Case: SDN-Enabled VANETs



Jitendra Bhatia et al., “Software defined vehicular networks: A comprehensive review,” Int J Commun Syst. 2019.

SDN-Enabled VANETs (SDVN)

- Appropriate Path
  - Detailed routing decisions
  - Avoidance of congestion due to shortest path node use
- Channel/Frequency
  - Availability of multiple wireless interfaces, cognitive radios…
  - Adaptive radio frequency selection
  - Conserving channel for emergency services
- Transmission Power
  - Selection of proper energy level of wireless interfaces and transmission range through controller's feedback based on collection of neighbor information from vehicles

Jitendra Bhatia et al., "Software defined vehicular networks: A comprehensive review," Int J Commun Syst. 2019.

SDVN – Specific Use Cases

- Smart Parking
- Smart Grid for Electric Vehicles
- Platooning
- Emergency response
- …

Maio et al., “Enabling SDN in VANETs: What is the Impact on Security?” Sensors, 2016.

How Does SDVN Provide Security?

- **Smart Parking:**
  - Sensors (Zigbee, LoRa, Wi-Fi…) vulnerable to wide range of attacks
  - Jamming to prevent reception of sensor data at WSN gateway, hence RSU --> RSUs gather detailed info about channel quality, build list of bad channels
  - Eavesdropping on vehicle beacons --> decoupling ID from vehicle using pseudonym system switching IDs by RSUC

Maio et al., “Enabling SDN in VANETs: What is the Impact on Security?” Sensors, 2016.

How Does SDVN Provide Security?

- **Smart Grid for Electric Vehicles:**
  - Malware in infrastructure
  - Electrical power level not tolerated by internal charging component of OBU, shortened battery life, battery explosion…
  - Detect, isolate and mitigate attacks as soon as they appear
  - SDN can detect fixed Electrical Vehicle Supply Equipment behaving suspiciously and isolate from network

Maio et al., "Enabling SDN in VANETs: What is the Impact on Security?" Sensors, 2016.

How Does SDVN Provide Security?

- **Platooning:**
  - Replay attack for messages by platoon leader

  -> Use globally synchorized time by controller for all vehicles / nonce generated by RSUC
  - Jamming to prevent beacon receipt by platoon leader

  -> Dynamic selection of good channels / channel blacklisting by controller
  - DoS to prevent platoon instructions

  -> Adjusting flow timeouts / SDN controller monitoring all communication, extracting topological and forwarding information to build holistic graph for comparison with incoming traffic

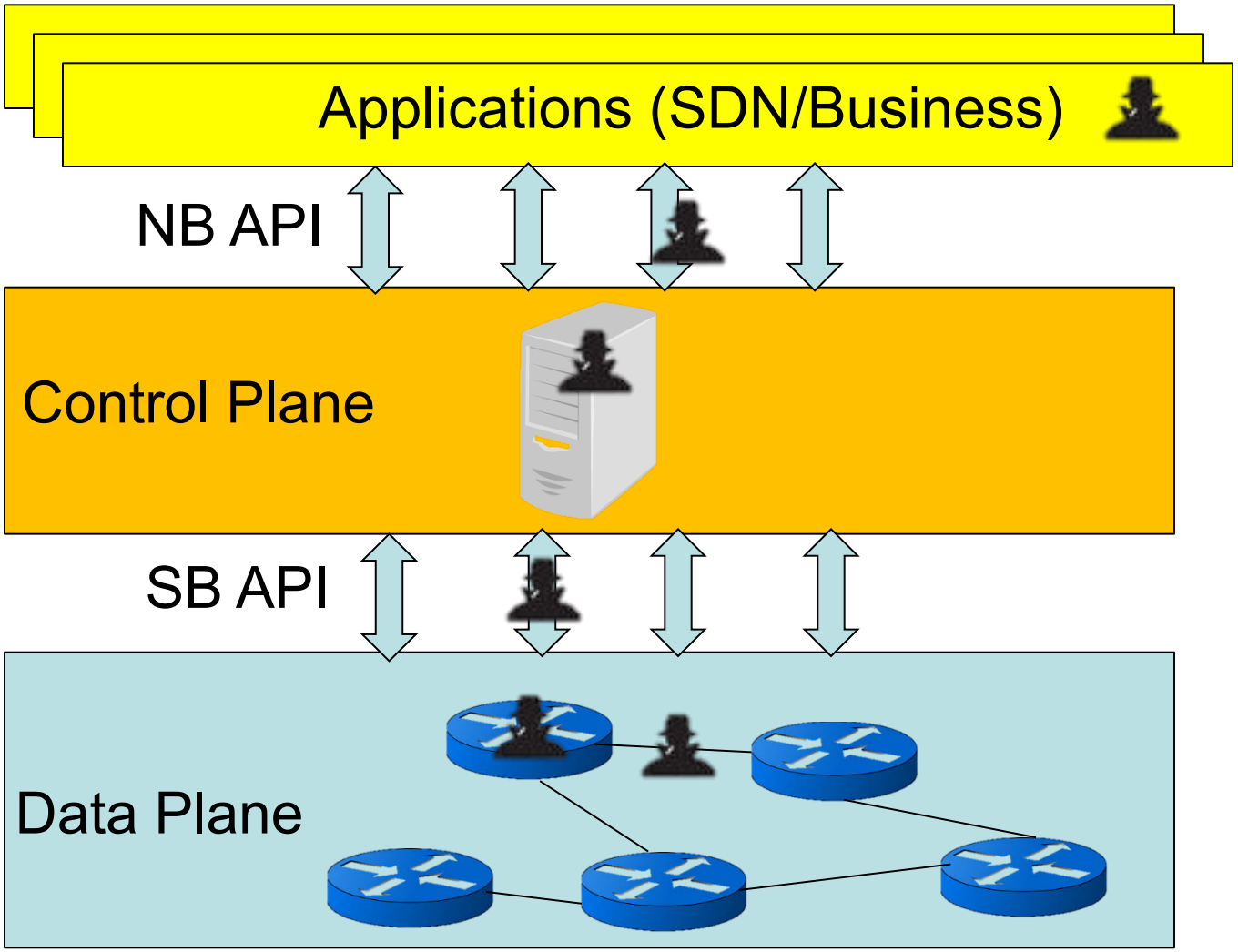
Maio et al., “Enabling SDN in VANETs: What is the Impact on Security?” Sensors, 2016.

SDVN Challenges

- Rapid change management
- Security***
- Latency control
- Scalability
- Network heterogeneity
- Trustworthiness evaluation, misbehavior detection, revocation
- Definition of boundaries for SDN integration

Jitendra Bhatia et al., “Software defined vehicular networks: A comprehensive review,” Int J Commun Syst. 2019.

Attacking SDN



- DoS
- Controller identity spoofing
- Route poisoning
- …

DoS Mitigation Approaches For SDN

- Thresholding techniques → May deny legitimate traffic
- Statistical/entropy-based approaches → May deny legitimate traffic
- Rule (policy)-based approaches → Requires expert analysis, may be slow, hard to implement
- ML approaches → Computing power, dataset issues
- Table entry-based approaches

Programming Protocol-Independent

SDN

Is P4 Programming the Future of SDN?

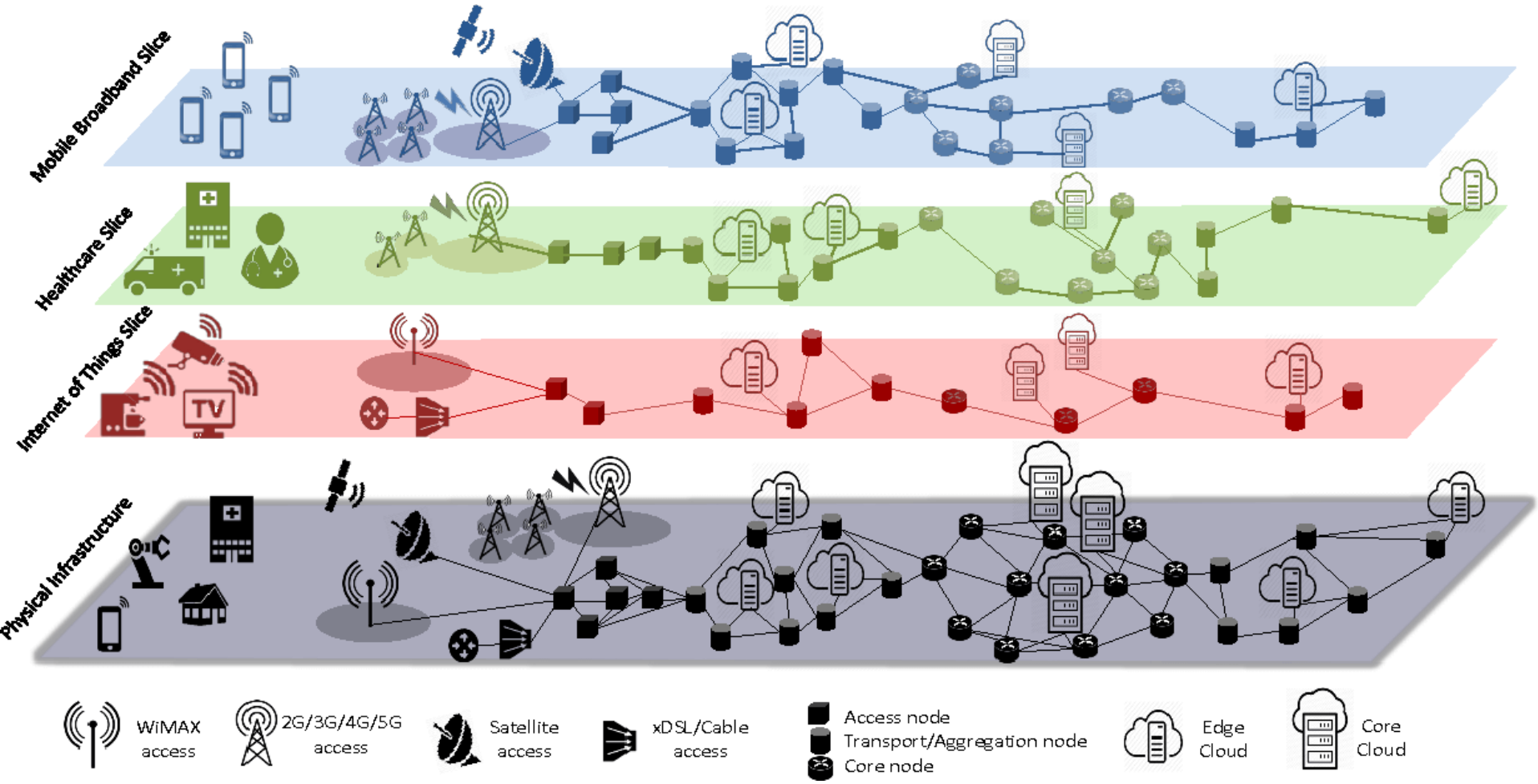
April 27, 2018 | Marian Pritsak

- Do
pa
pro
- Pro
sta
- De
independence of underlying hardware
- A P4 program can work on any switch that can support P4,
reg
- Wo
(pa
rule
out

Can P4 save Software-Defined Networking?

Published by castroflaviojr on October 24, 2017

One Slice For Each…



https://www.onug.net/blog/5g-network-slicing-and-enterprise-networking/

Why Does Slicing Matter For IoT?

- Service quality and reliability guarantees
- **Enhanced security** through traffic isolation
  - Assigning resources that cannot be influenced by services on different slices
  - Like running several different networks on one physical network
- Ease of network management

Slicing Challenges

- Effective and efficient resource allocation
- Dynamic slice creation and management
- **Slice isolation**
- **Virtualization attacks**
- Mobility management
- **E2E security policy enforcement**

THANK YOU ☺

QUESTIONS?