Security in SDN/NFV and 5G Networks – Opportunities and Challenges

Ashutosh Dutta, Ph.D.
Senior Scientist, Johns Hopkins University Applied Physics Lab (JHU/APL), USA
Co-Chair, IEEE Future Network Initiative
IEEE Communications Society Industry Outreach
IEEE Communications Society Distinguished Lecturer
Email: ashutosh.dutta@ieee.org; Ashutosh.Dutta@jhuapl.edu

05/06/2019

Talk Outline

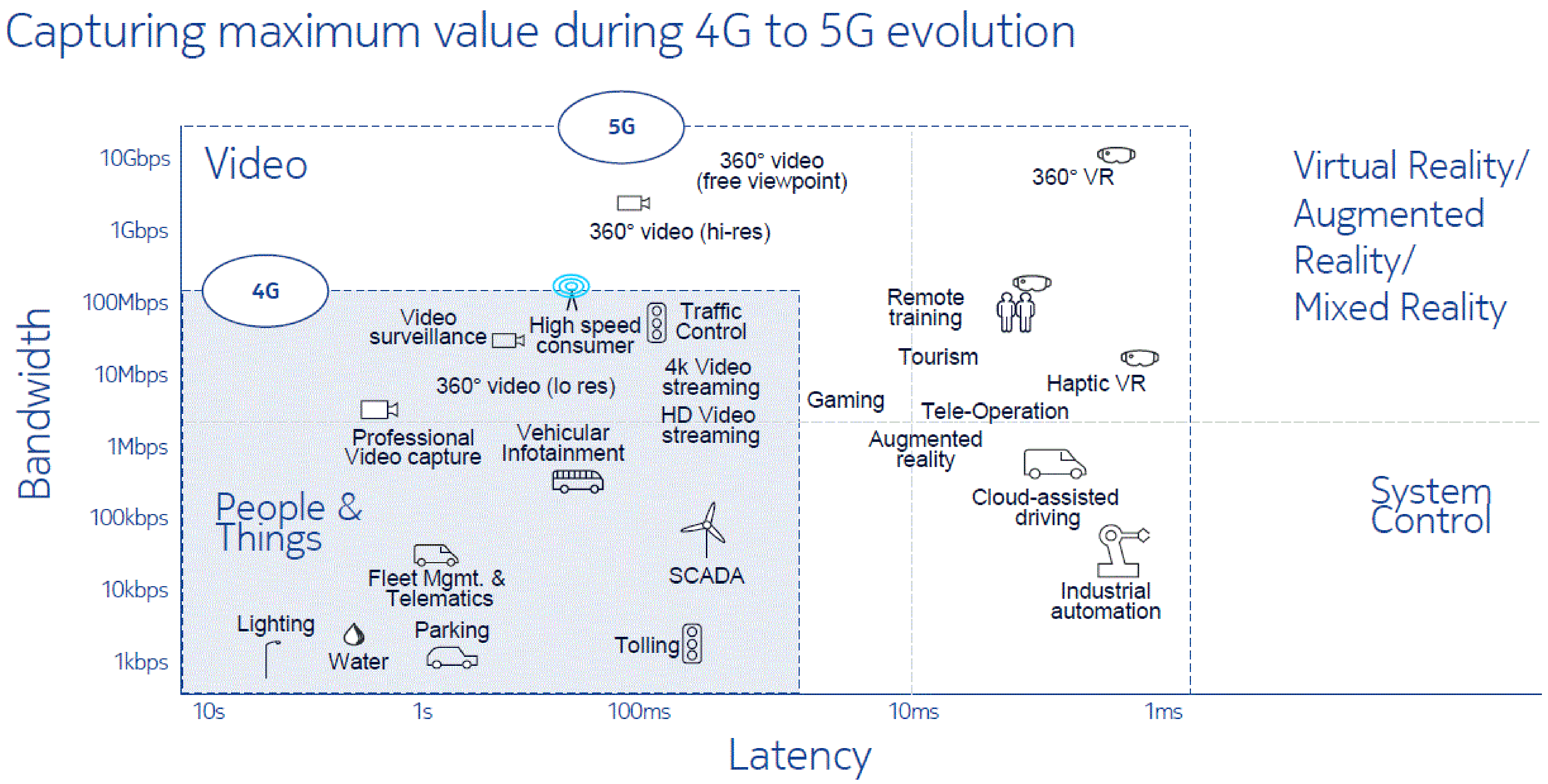
- Drivers for SDN/NFV and 5G Networks
- Cellular Technology Evolution
- Key 5G Characteristics
- Threat Taxonomy
- Opportunities and Challenges in Security Virtualization and 5G
- Security Use Cases
- Industry Standards Activities and Testbed
- Summary

Emerging Services and Applications

A Driver for Network Evolution

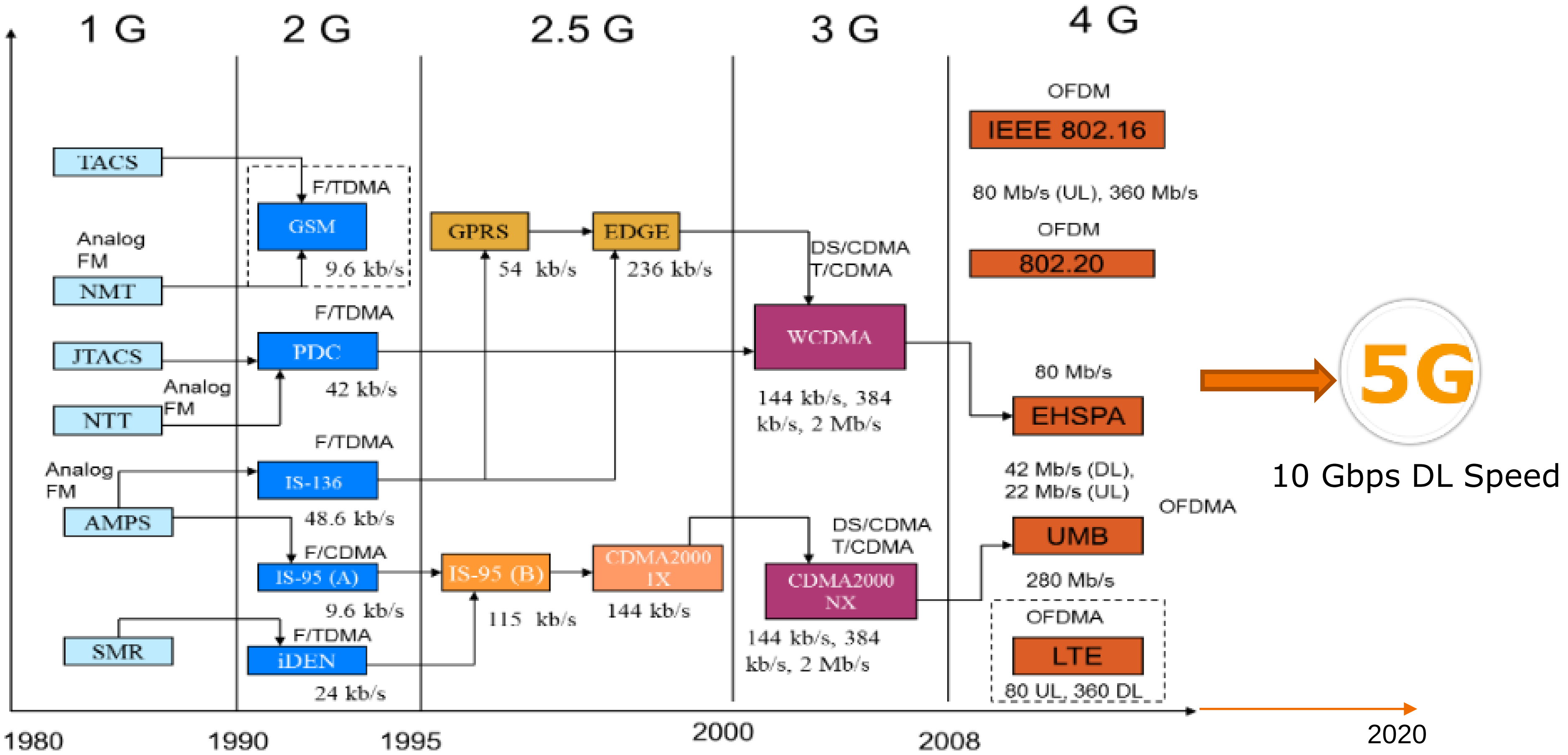
Smart Workplace
Asset Tracking
Internet of Things
Security
WebTV
Video
Smart Meter
Digital Content
Smart City
Robotics
Mobilize Everything
Semantic Web
Big Data
SmartGrid
Augmented Reality
M2M
Digital Learning
Sensor Network
Wearable Computing
BYOD
Voice Recognition
Digital Life
Virtualization
Gesture Computing
Entertainment
Gamification
Gaming
Connected Car
Social Internet
Location Based Services
Mobile Payment
Mobile Advertisement
mHealth
Knowledge Management
Virtual Personal Assistant
User Generate Content
Software Defined Anything

SLAs associated with Types of Applications



Source Nokia

Evolution of wireless access technologies



1 G
2 G
2.5 G
3 G
4 G

TACS
Analog FM
NMT
JTACS
Analog FM
NTT
Analog FM
AMPS
SMR

F/TDMA
GSM
9.6 kb/s
F/TDMA
PDC
42 kb/s
F/TDMA
IS-136
48.6 kb/s
F/CDMA
IS-95 (A)
9.6 kb/s
F/TDMA
iDEN
24 kb/s

GPRS
54 kb/s
EDGE
236 kb/s
IS-95 (B)
115 kb/s
CDMA2000 1X
144 kb/s

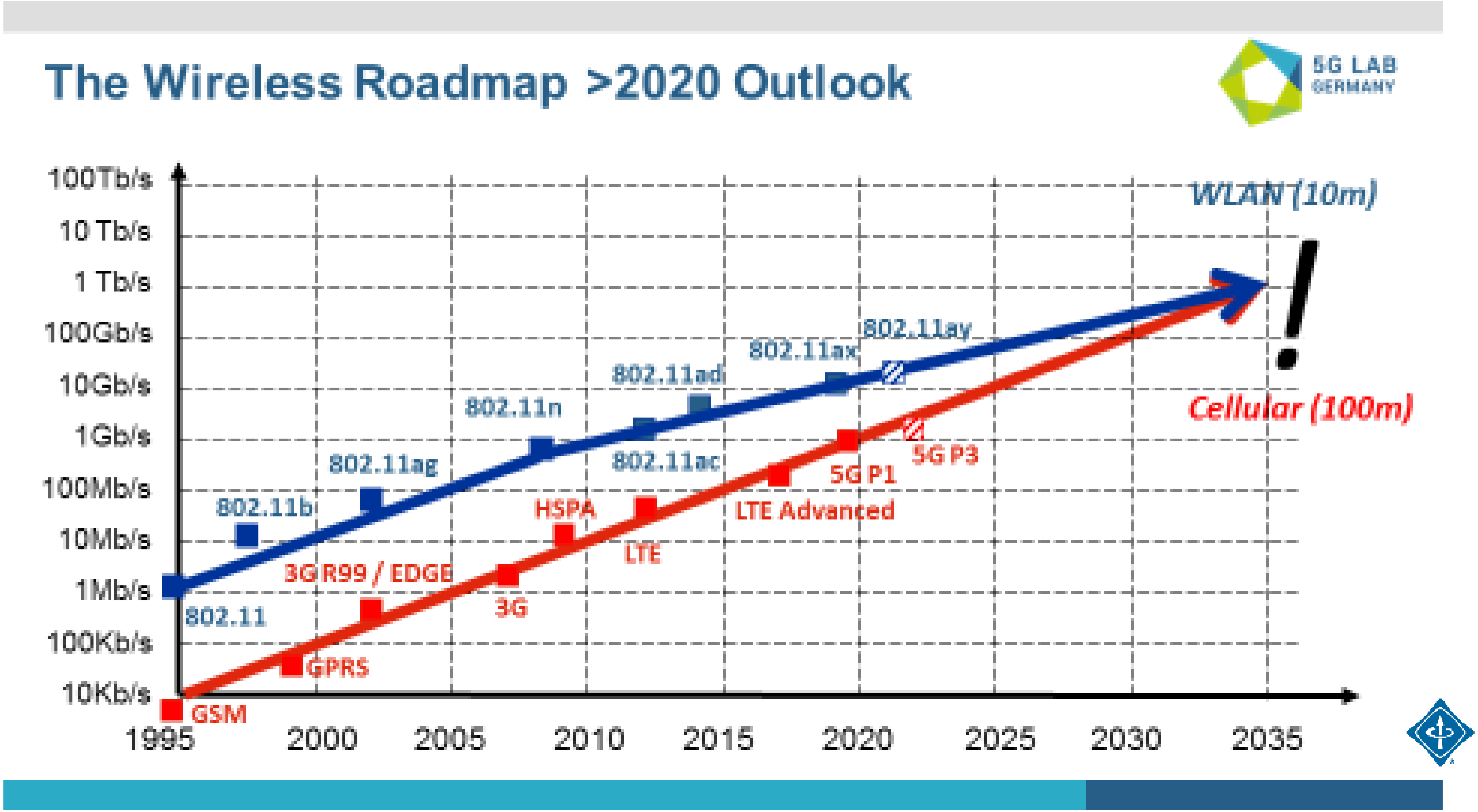
DS/CDMA T/CDMA
WCDMA
144 kb/s, 384 kb/s, 2 Mb/s
DS/CDMA T/CDMA
CDMA2000 NX
144 kb/s, 384 kb/s, 2 Mb/s

OFDM
IEEE 802.16
80 Mb/s (UL), 360 Mb/s
OFDM
802.20
80 Mb/s
EHSPA
42 Mb/s (DL), 22 Mb/s (UL)
OFDMA
UMB
280 Mb/s
OFDMA
LTE
80 UL, 360 DL

5G
10 Gbps DL Speed

1980
1990
1995
2000
2008
2020

Co-existence of IEEE and 3GPP Technologies



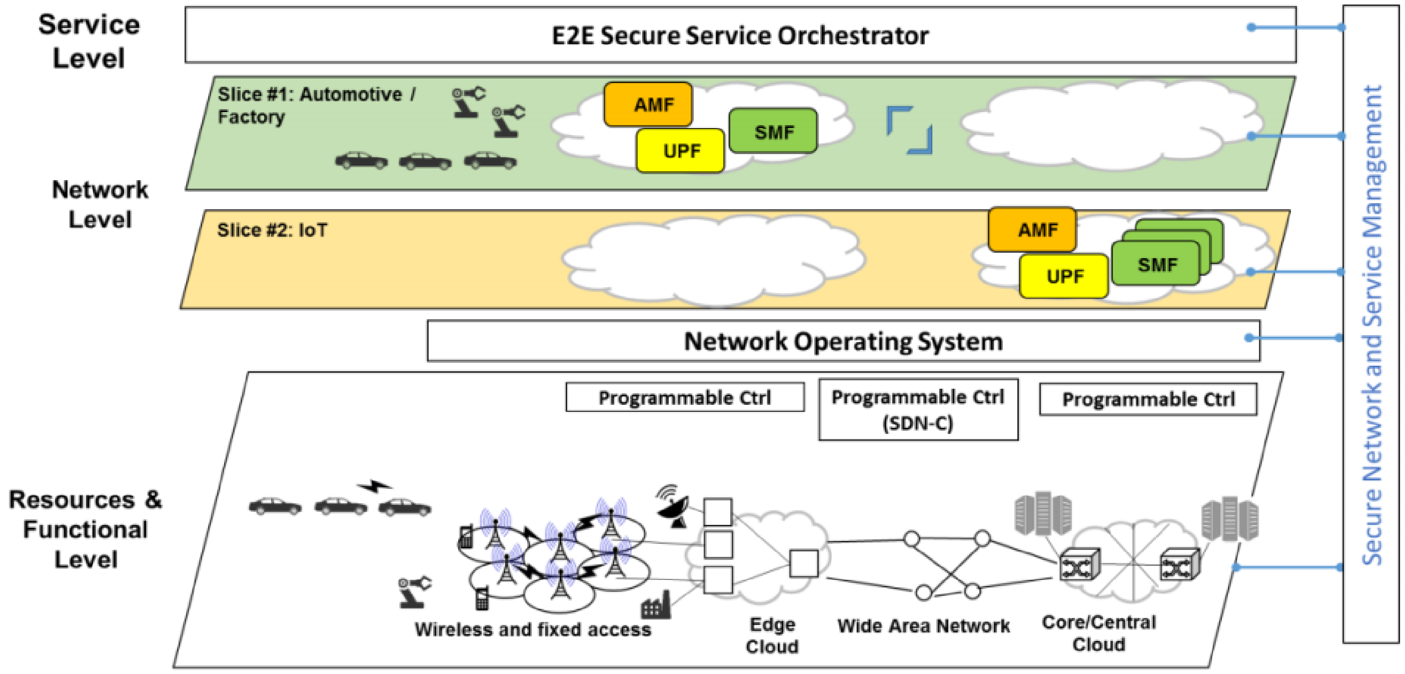
The Wireless Roadmap >2020 Outlook

Key Characteristics of 5G

- Massive MIMO
- RAN Transmission – Centimeter and Millimeter Waves
- New Waveforms
- Shared Spectrum Access
- Advanced Inter-Node Coordination
- Simultaneous Transmission Reception
- Multi-RAT Integration & Management
- D2D Communications
- Efficient Small Data Transmission
- Densification of Small Cells
- Wireless Backhaul / Access Integration
- Flexible Networks
- Flexible Mobility
- Context Aware Networking
- Information Centric Networking
- Moving Networks

5G – Emerging Architecture and Enabling Technologies

5G Architecture Themes: Flexibility, Scalability


Service Level
E2E Secure Service Orchestrator
Network Level
Slice #1: Automotive / Factory
AMF
SMF
UPF
Slice #2: IoT
AMF
UPF
SMF
Network Operating System
Resources & Functional Level
Programmable Ctrl
Programmable Ctrl (SDN-C)
Programmable Ctrl
Wireless and fixed access
Edge Cloud
Wide Area Network
Core/Central Cloud
Secure Network and Service Management

Source: 5G-PPP Architecture WG
View on 5G Architecture (Version 2.0)

5G New Radio

–Fiber-like performance

–However, 5G is Multi-RAT

- Network Function Virtualization
  - Network realized in software: Core and RAN
  - Cloud resources throughout the network
- Programmable Network
  - Flexible orchestration of network resources and infrastructure: RAN, core, transport, etc.
- Network Slicing
  - Self-contained, independent network partition including all segments: radio, core, transport, and edge.
  - Multi-domain, multi-tenant

5G Dimensions and Types of 5G Applications

Enhanced Mobile Broadband

- Mobile Broadband, UHD / Hologram, High-mobility, Virtual Presence, Virtual Reality

Critical Communications

- Interactive Game / Sports, Industrial Control, Drone / Robot / Vehicle, Emergency, Self-driving vehicles

Massive Machine Type Communications

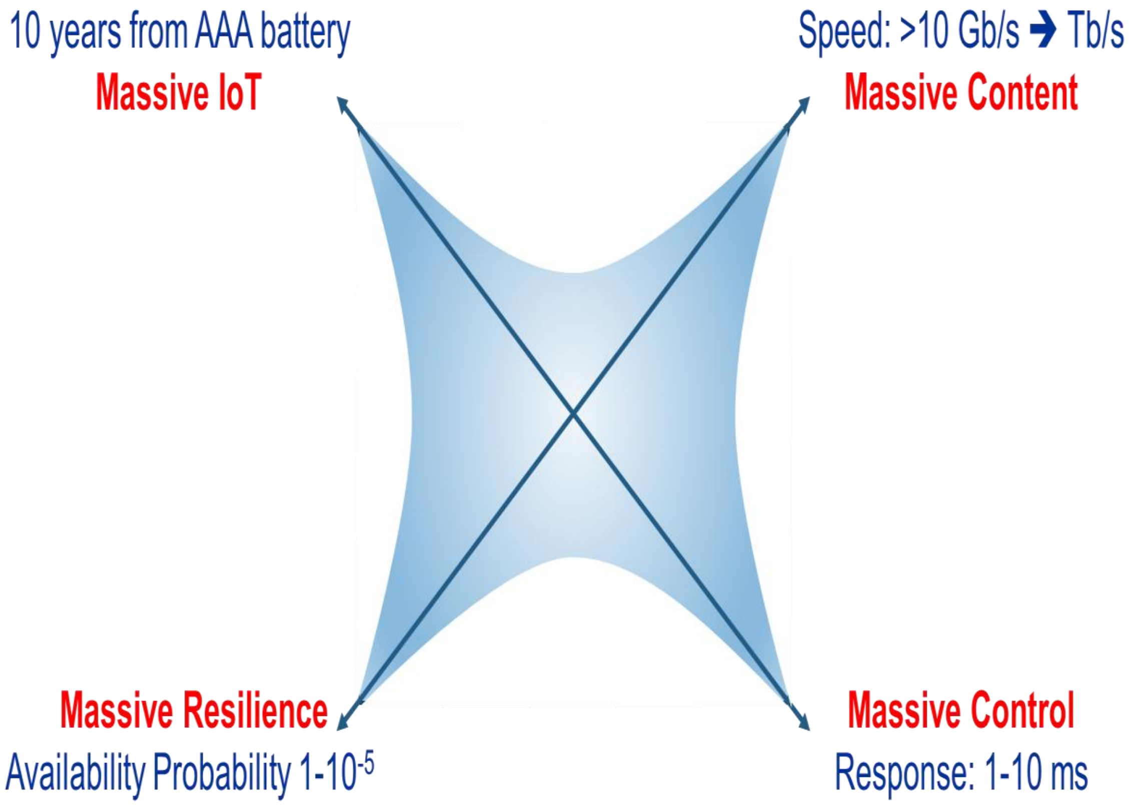
- Subway / Stadium Service, eHealth, Wearables, Inventory Control

Network Operation

- Network Slicing, Routing, Migration and Interworking, Energy Saving

Enhancement of Vehicle-to-Everything

- Autonomous Driving, safety and non-safety features

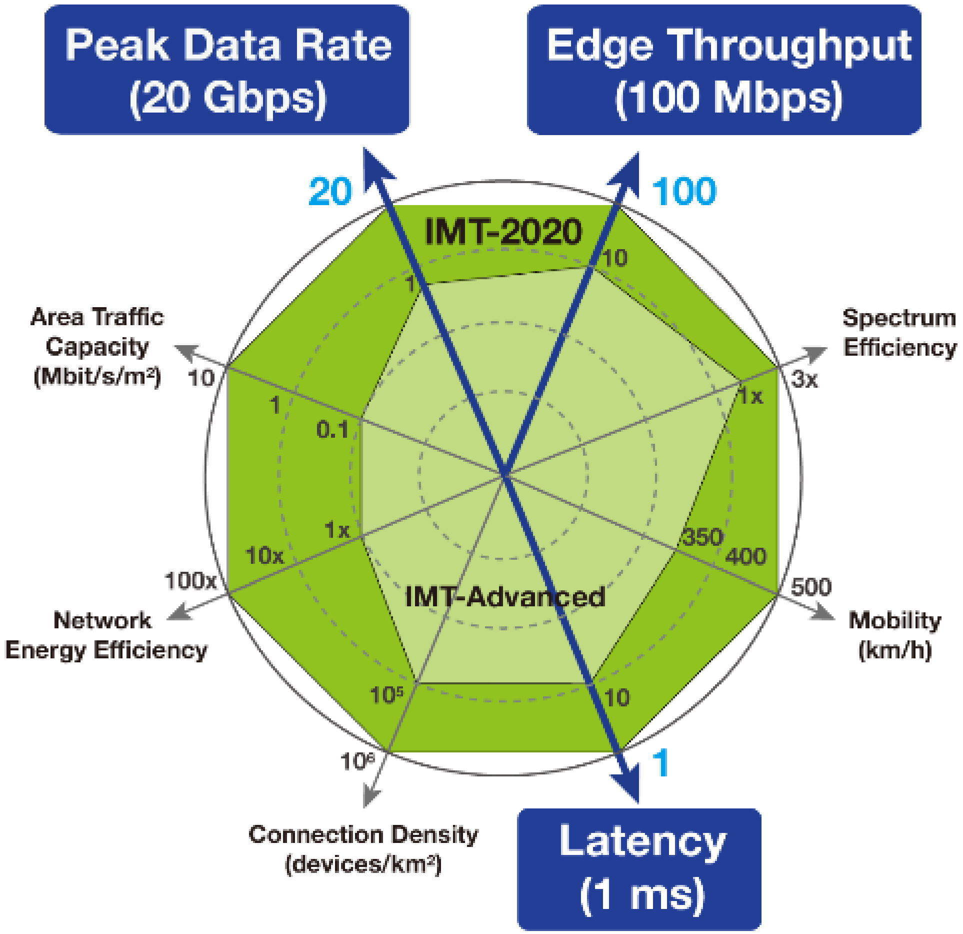


Courtesy: Gerhard Fettweis

Enhanced Mobile Broadband & UHRLLC Use Cases

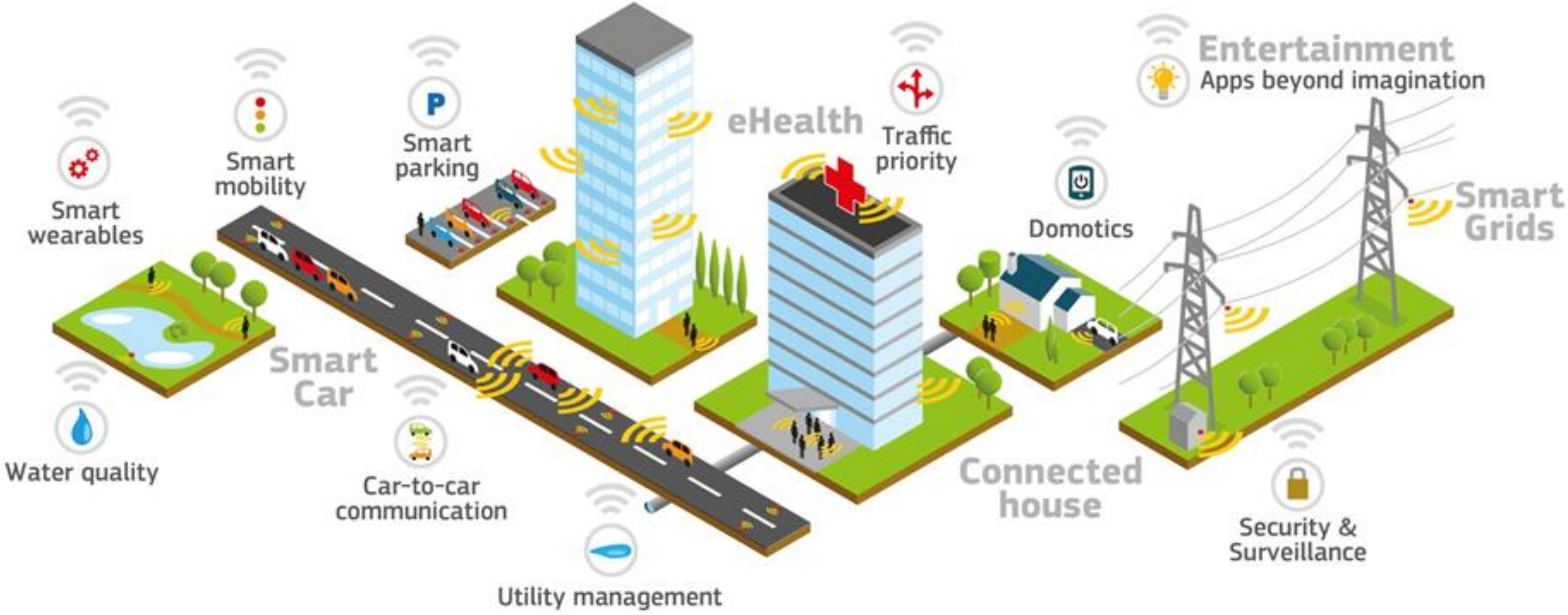
- Enhanced Mobile Broadband (eMBB)
  - Expected throughput of 5 Gbps +
  - UHD video (4k, 8k), 3D video (including broadcast services)
  - Virtual Reality
  - Augmented Reality
  - Tactile Internet
  - Cloud gaming
  - Broadband kiosks
  - Vehicular (cars, buses, trains, aerial stations, etc.)

- High reliability / low latency
  - Industrial control
  - Remote manipulation
  - Mission-critical applications e.g. ehealth, hazardous environments, rescue missions, etc.
  - Self-driving vehicles

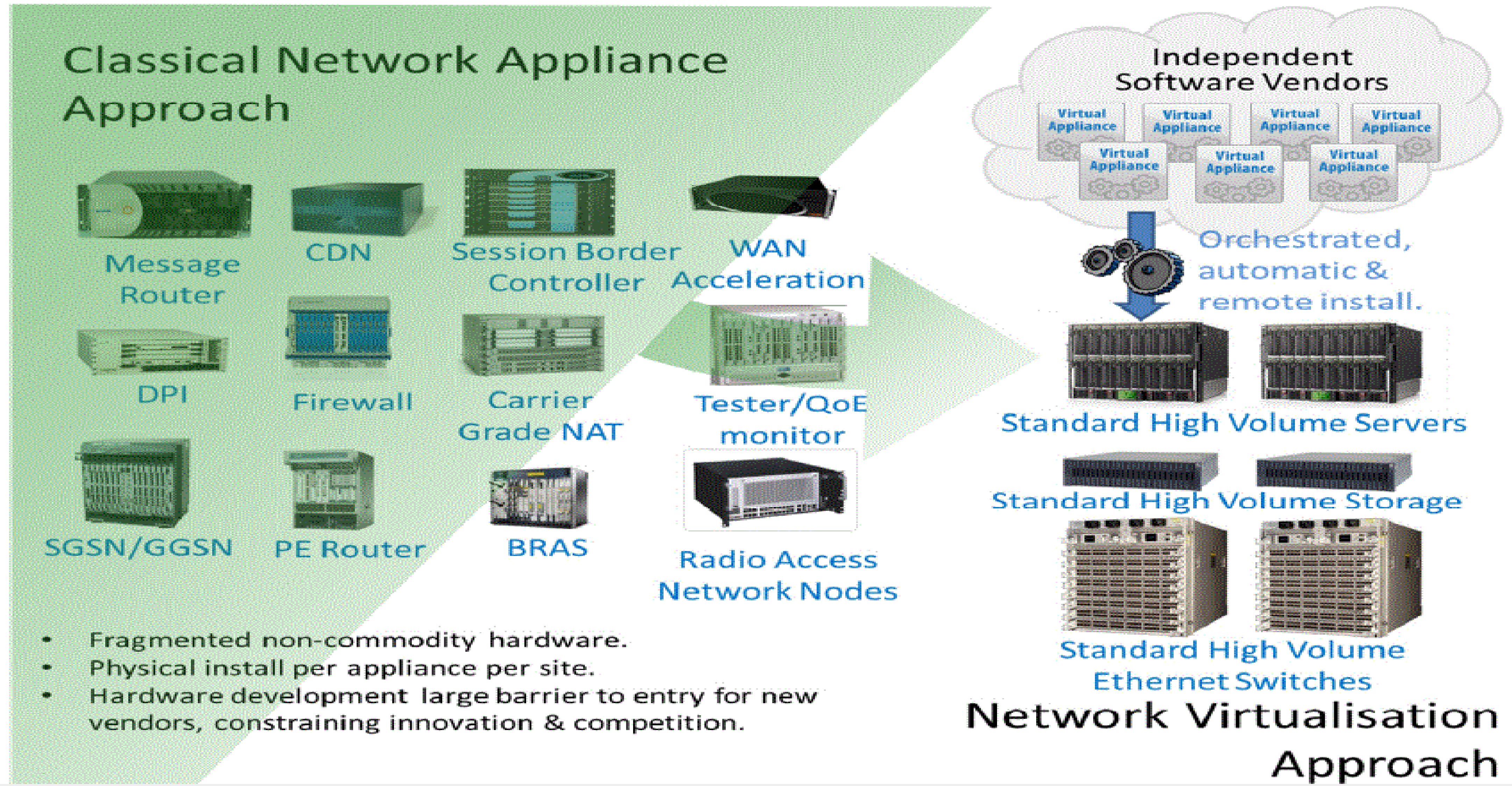


Source: ITU-R

What “5G and Advanced Communication Systems” is About

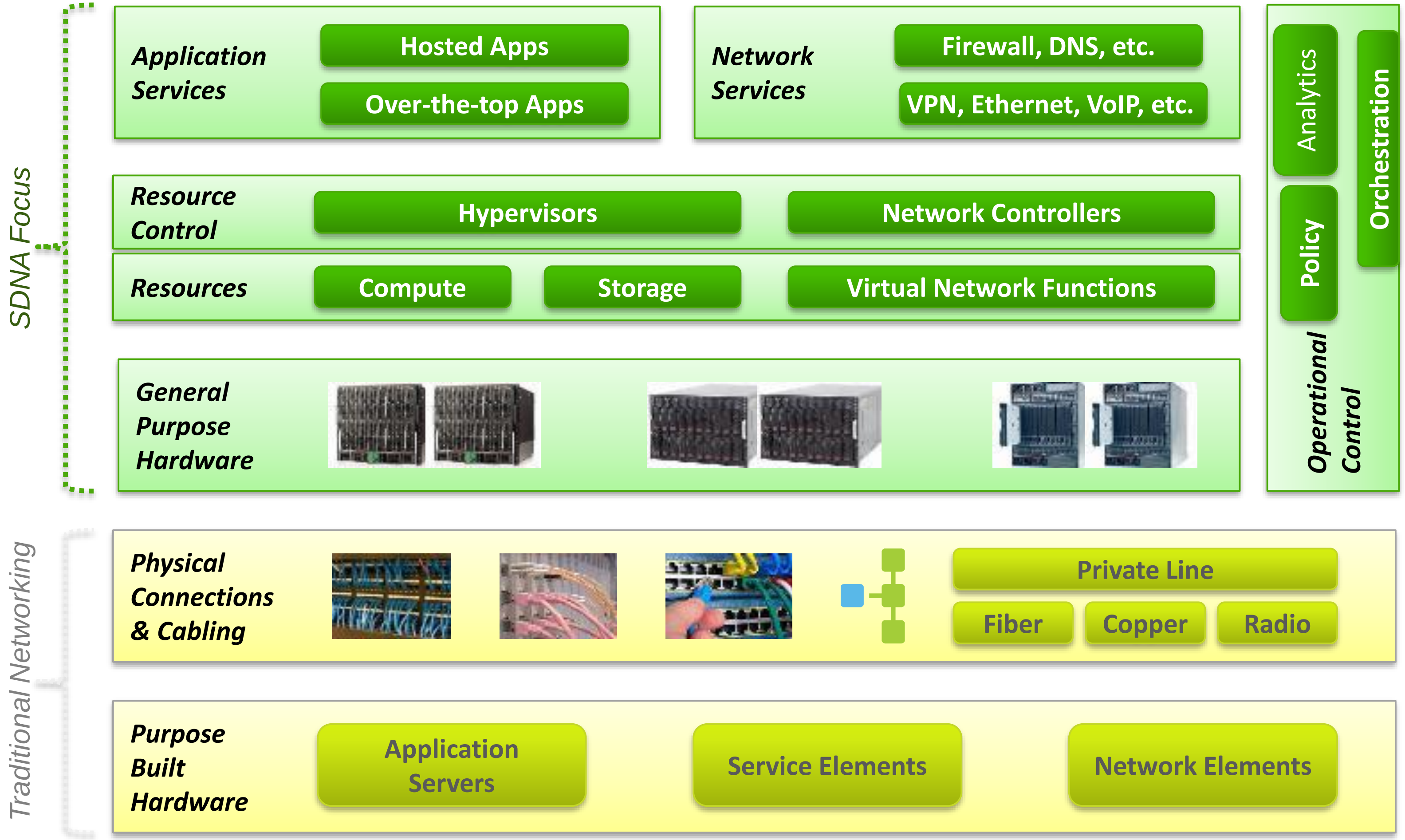


SDN/NFV is the Foundation of 5G Core Network


Classical Network Appliance Approach
Message Router
CDN
Session Border Controller
WAN Acceleration
DPI
Firewall
Carrier Grade NAT
Tester/QoE monitor
SGSN/GGSN
PE Router
BRAS
Radio Access Network Nodes
Independent Software Vendors
Virtual Appliance
Virtual Appliance
Virtual Appliance
Virtual Appliance
Virtual Appliance
Virtual Appliance
Virtual Appliance
Orchestrated, automatic & remote install.
Standard High Volume Servers
Standard High Volume Storage
Standard High Volume Ethernet Switches
Network Virtualisation Approach

- Fragmented non-commodity hardware.
- Physical install per appliance per site.
- Hardware development large barrier to entry for new vendors, constraining innovation & competition.

Traditional Network vs. SDN/NFV Network



SDNA Focus

Application Services
Hosted Apps
Over-the-top Apps

Network Services
Firewall, DNS, etc.
VPN, Ethernet, VoIP, etc.

Resource Control
Hypervisors
Network Controllers

Resources
Compute
Storage
Virtual Network Functions

General Purpose Hardware

Analytics
Policy
Orchestration
Operational Control

Traditional Networking

Physical Connections & Cabling
Private Line
Fiber
Copper
Radio

Purpose Built Hardware
Application Servers
Service Elements
Network Elements

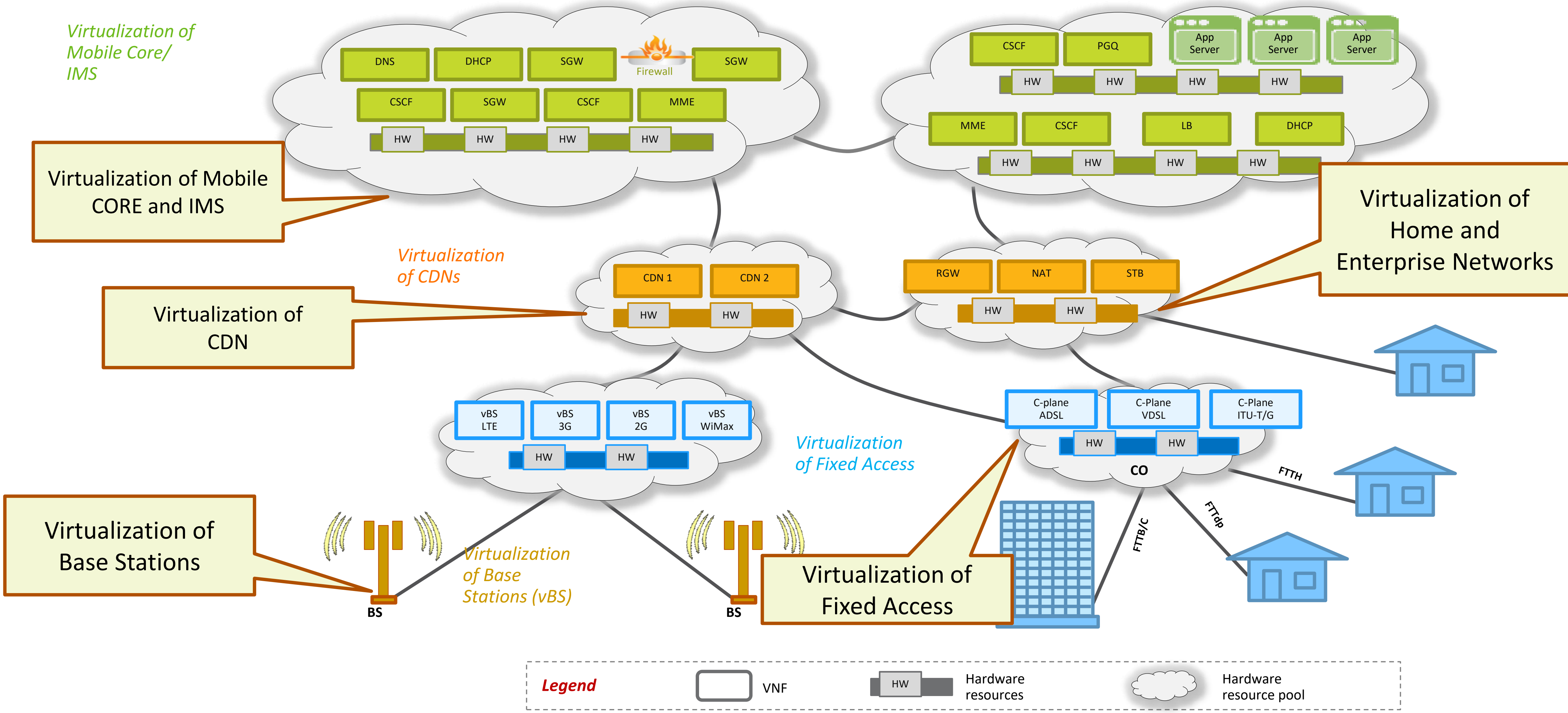
Virtualized Networks

- General purpose cloud-based hardware components
- Software-based virtual network components and services
- Dynamic real-time configuration to support internal or customer activity
- Programmable network management
  - Software Defined Network controls
  - Real-time analytics and policy driven orchestration of service, network and capacity requests

Traditional Networks

- Built using purpose-built hardware coupled with physical connectivity
- Control logic largely coordinated and implemented by layers of OSSs
- Control, Forward and Data Planes are tightly integrated in Network Elements
  - OA&M, inventory views and operational controls managed in OSSs to avoid negative impact to service performance

Overview of NFV (Network Function Virtualization) Sample Use cases



Virtualization of Mobile CORE and IMS

Virtualization of Home and Enterprise Networks

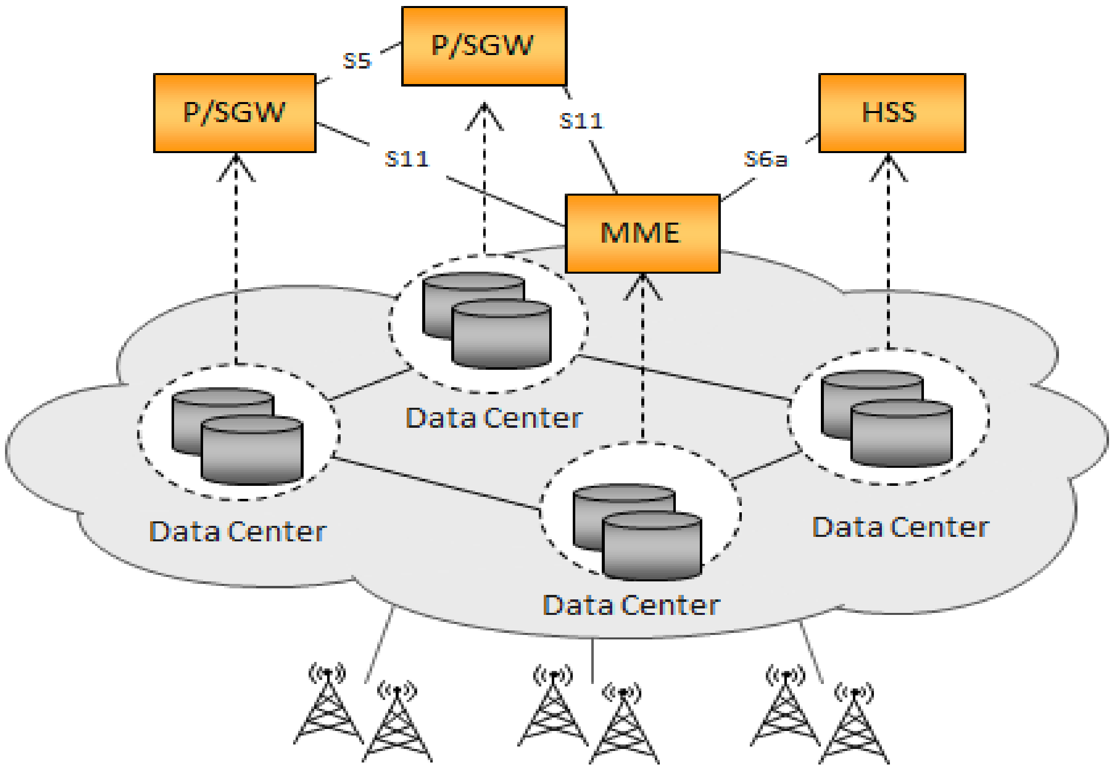
Virtualization of CDN

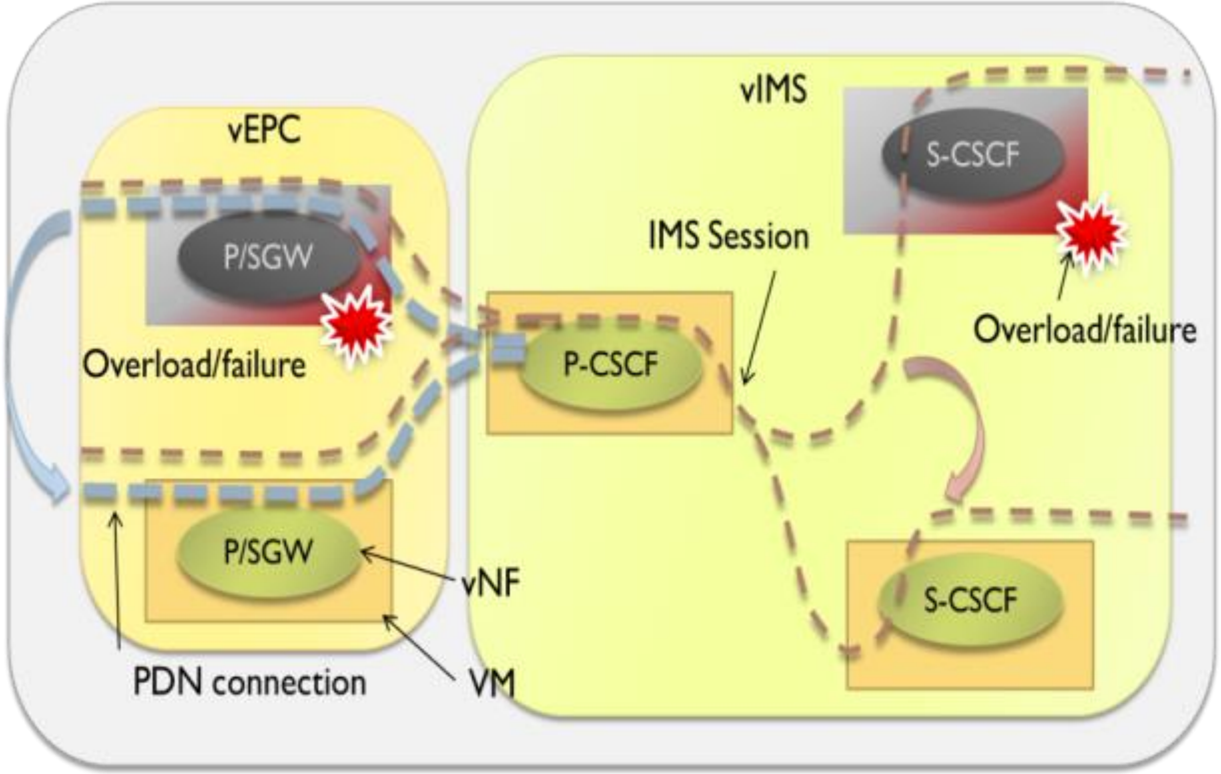
Virtualization of Base Stations

Virtualization of Fixed Access

NFV Use Case: Dynamic VNF Placement of Mobile Core Network (EPC) and IMS Elements

Network Operation





VNF Relocation

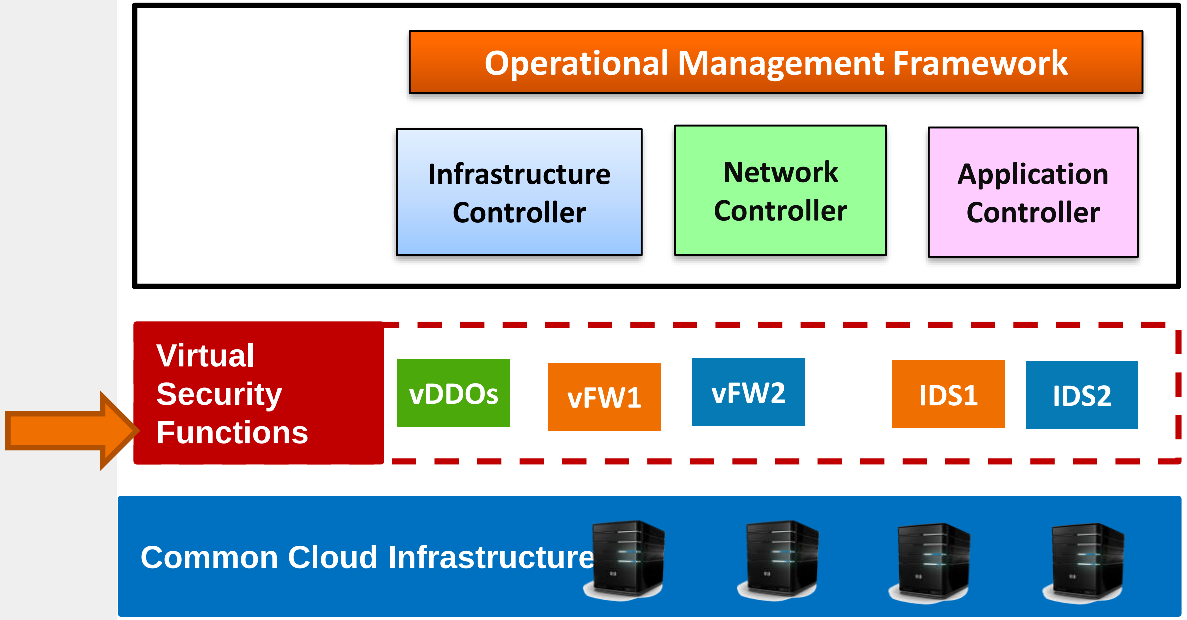
An Example - Security Transformation – Virtual Firewall/Virtual DDOS/Virtual IPS

Non-Virtualized Security

Intel Security
Tektronix
HP
f5
ARBOR NETWORKS
GUAVUS
ALLOT
A10 NETWORKS
NIKSUN
NETSCOUT
Check Point
paloalto networks
radware
Alcatel-Lucent
FORTINET
JUNIPER NETWORKS
sandvine
movik
FireEye

- Wide variety of vendor specific security hardware
- Requires vendor specific FW management platforms
- Requires hands-on customized physical work to install
- Multiple support organizations
- No single operations model or database of record

Virtualized Security Function



Operational Management Framework

Infrastructure Controller

Network Controller

Application Controller

Virtual Security Functions

vDDOs

vFW1

vFW2

IDS1

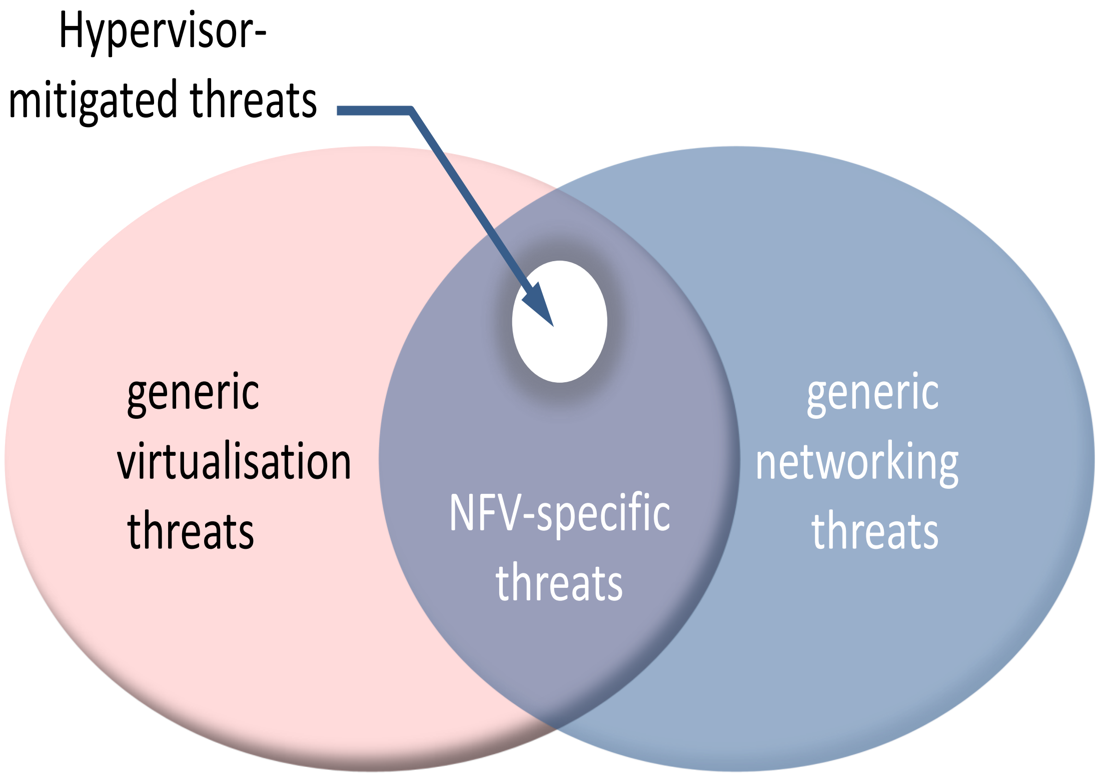
IDS2

Common Cloud Infrastructure

- Security functions will be cloud-based
- Security dynamically orchestrated in the cloud as needed
- Streamlined supplier integration
- Centralized common management platform
- Creates a standard operations/support model

Security Challenges in SDN/NFV Environment ETSI Problem Statement Draft

- Hypervisor Vulnerability
- API security
- Orchestration Vulnerability
- Virtual monitoring
  - Limited visibility to Mobility/EPC interfaces (e.g. S6a, S11, S8)
- Virtualized firewalls
- Secure boot
- Secure crash
- User/tenant authentication, authentication and accounting
- Topology validation and enforcement
- Performance isolation
- Authenticated Time Service
- Private Keys within Cloud Images
- Detection of attacks on resources in virtualization infrastructure
- Security monitoring across multiple administrative domains (i.e., Lawful Interception)


Hypervisor-mitigated threats
generic virtualisation threats
NFV-specific threats
generic networking threats

Key Pillars of SDN/NFV and 5G Security

Open Source Security

Network Slicing Security

Edge Security

Security Function Virtualization (Security-as-a-Service

Cloud RAN Security

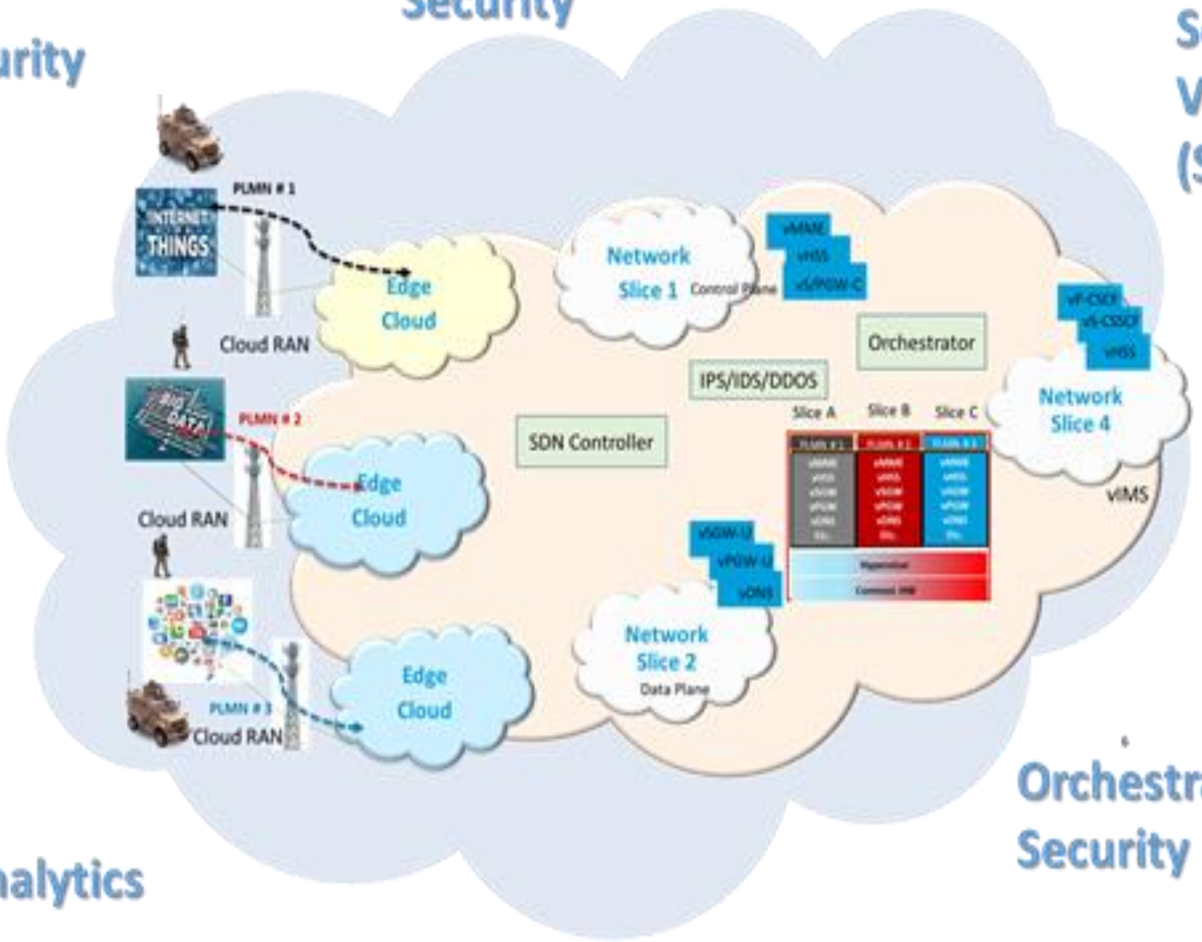
SDN Controller Security

Faster Authentication

Proactive Security Analytics

Orchestration Security

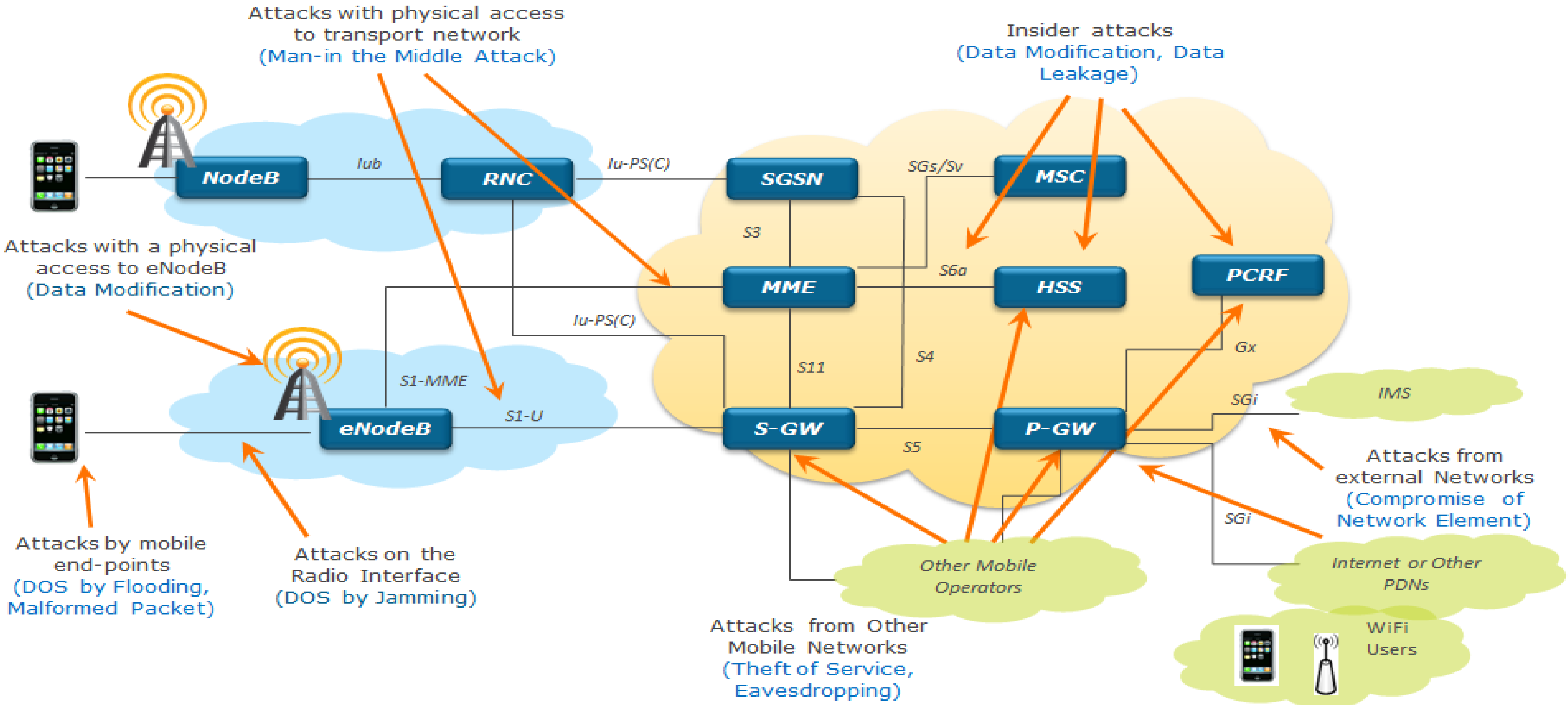
Hypervisor Security



May 7, 2019

General Threat Taxonomy (EPC) – Ref. ETSI/NFV Monitoring and Management (Draft 13)

LTE/EPC Security Threats Categories



Attacks with physical access to transport network (Man-in the Middle Attack)

Insider attacks (Data Modification, Data Leakage)

Attacks with a physical access to eNodeB (Data Modification)

Attacks from external Networks (Compromise of Network Element)

Attacks by mobile end-points (DOS by Flooding, Malformed Packet)

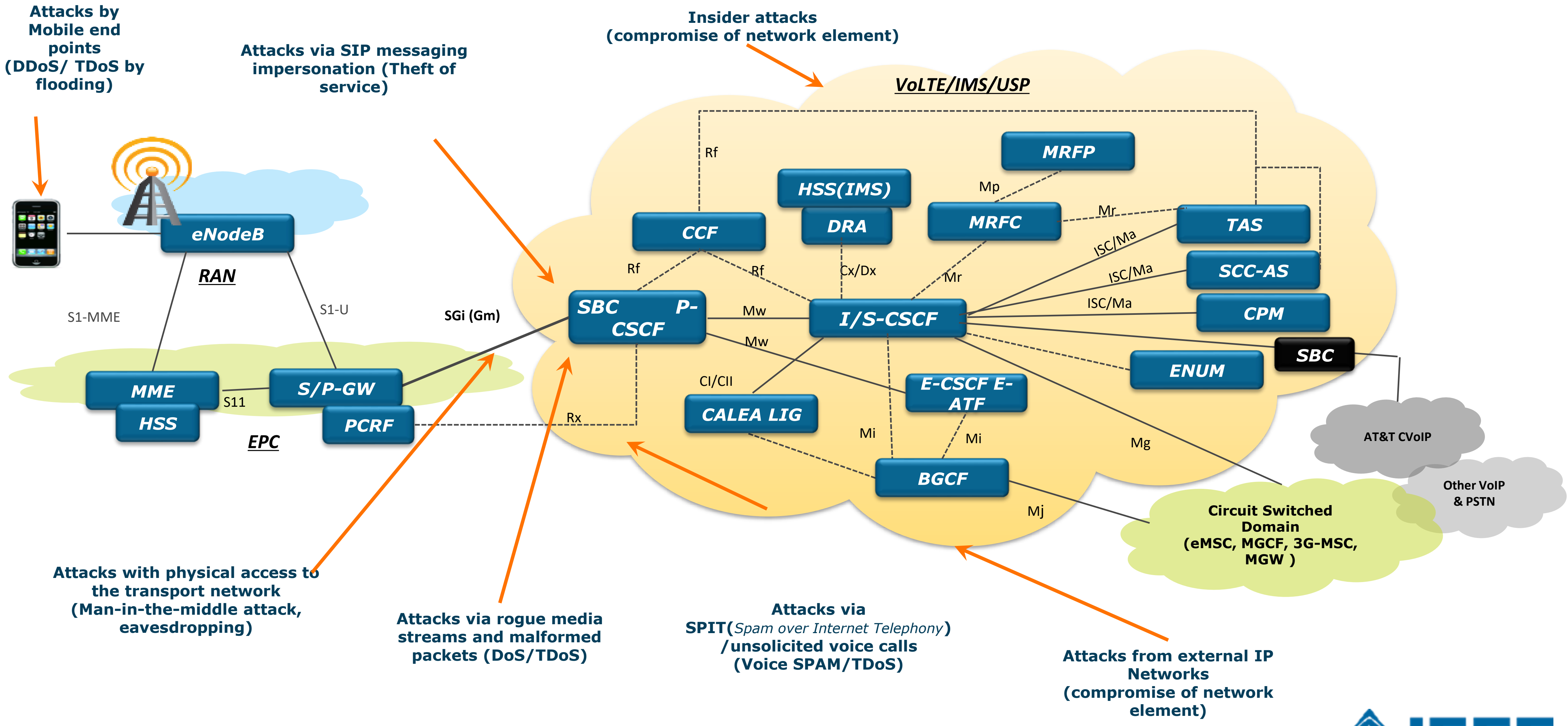
Attacks on the Radio Interface (DOS by Jamming)

Attacks from Other Mobile Networks (Theft of Service, Eavesdropping)

Mobile Network Security - EPC
Threat Categories

	Category	Threat	Description
T1	Loss of Availability	Flooding an interface	Attackers flood an interface resulting in DoS condition (e.g. multiple authentication failure on s6a, DNS lookup)
T2		Crashing a network element	Attackers crash a network element by sending malformed packets
T3	Loss of Confidentiality	Eavesdropping	Attackers eavesdrop on sensitive data on control and bearer plane
T4		Data leakage	Unauthorized access to sensitive data on the server (HSS profile, etc.)
T5	Loss of Integrity	Traffic modification	Attackers modify information during transit (DNS redirection, etc.)
T6		Data modification	Attackers modify data on network element (change the NE configurations)
T7	Loss of Control	Control the network	Attackers control the network via protocol or implementation flaw
T8		Compromise of network element	Attackers compromise of network element via management interface
T9	Malicious Insider	Insider attacks	Insiders make data modification on network elements, make unauthorized changes to NE configuration, etc.
T10	Theft of Service	Service free of charge	Attackers exploits a flaw to use services without being charged

Attacks Taxonomy – VoLTE/IMS/USP

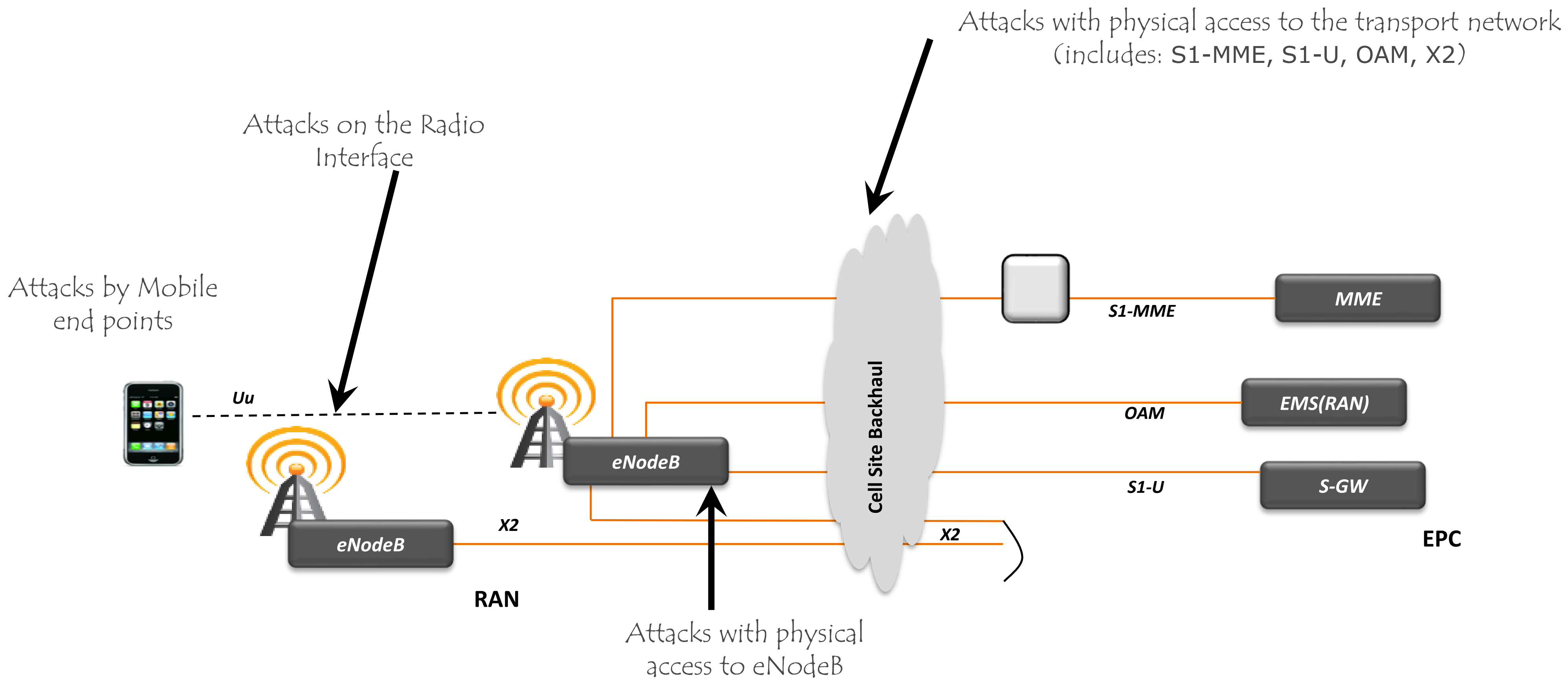


Attacks by Mobile end points (DDoS/ TDoS by flooding)
Attacks via SIP messaging impersonation (Theft of service)
Insider attacks (compromise of network element)
VoLTE/IMS/USP
eNodeB
RAN
S1-MME
S1-U
MME
HSS
S11
S/P-GW
PCRF
EPC
SGi (Gm)
Rx
SBC P-CSCF
CCF
Rf
Rf
Rf
HSS(IMS)
DRA
Cx/Dx
MRFP
Mp
MRFC
Mr
Mr
TAS
SCC-AS
CPM
ISC/Ma
ISC/Ma
ISC/Ma
Mw
Mw
I/S-CSCF
SBC
ENUM
CI/CII
CALEA LIG
E-CSCF E-ATF
Mi
Mi
BGCF
Mg
Mj
AT&T CVoIP
Other VoIP & PSTN
Circuit Switched Domain (eMSC, MGCF, 3G-MSC, MGW)
Attacks with physical access to the transport network (Man-in-the-middle attack, eavesdropping)
Attacks via rogue media streams and malformed packets (DoS/TDoS)
Attacks via SPIT(*Spam over Internet Telephony*) /unsolicited voice calls (Voice SPAM/TDoS)
Attacks from external IP Networks (compromise of network element)

IMS Threat Categories

	Category	**Threat**	**Description**
T1	Loss of Availability	Flooding an interface	DDoS/TDoS via Mobile end-points
T2		Crashing a network element	DoS/TDoS via rogue media streams and malformed packets
T3	Loss of Confidentiality	Eavesdropping	Eavesdropping via sniffing the SGi(Gm) interface
T4		Data leakage	Unauthorized access to sensitive data on the IMS-HSS
T5	Loss of Integrity	Traffic modification	Man-in-the-middle attack on SGi(Gm) interface
T6		Data modification	SIP messaging impersonation via spoofed SIP messages
T7	Loss of Control	Control the network	SPIT(Spam over Internet Telephony) / unsolicited voice calls resulting in Voice-SPAM/TDoS
T8		Compromise of network element	Compromise of network element via attacks from external IP networks
T9	Malicious Insider	Insider attacks	Malicious Insider makes unauthorized changes to IMS-HSS, SBC, P/I/S-CSCF configurations
T10	Theft of Service	Service free of charge	Theft of Service via SIP messaging impersonation

Attacks on LTE-RAN



Attacks with physical access to the transport network (includes: S1-MME, S1-U, OAM, X2)

Attacks on the Radio Interface

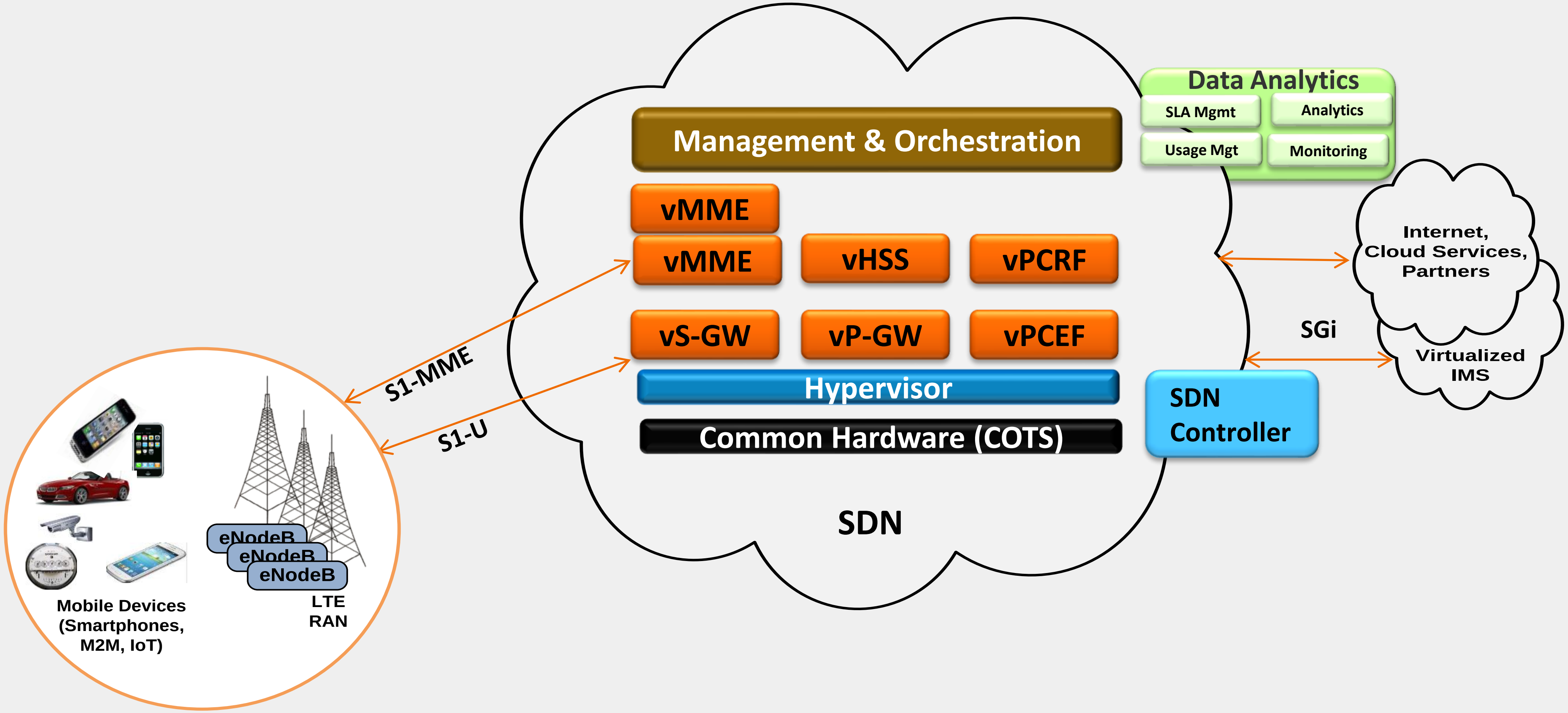
Attacks by Mobile end points

Attacks with physical access to eNodeB

RAN Threat Categories

	Category	Threat	Description
T1	Loss of Availability	Flooding an interface	DOS on eNodeB via RF Jamming
T2		Crashing a network element	DDOS on eNodeB via UE Botnets
T3	Loss of Confidentiality	Eavesdropping	Eavesdropping on S1-MME/S1-U interfaces
T4		Data leakage	Unauthorized access to sensitive data on the eNodeB
T5	Loss of Integrity	Traffic modification	Man-in-the-Middle attack on UE via false eNodeB
T6		Data modification	Malicious modification of eNodeB configuration data
T7	Loss of Control	Control the network	Attackers control the eNodeB via protocol or implementation flaw
T8		Compromise of network element	Attackers compromise the eNodeB via management interface
T9	Malicious Insider	Insider attacks	Malicious Insider makes unauthorized changes to eNodeB configuration
T10	Theft of Service	Service free of charge	Theft of Service via Spoofing/Cloning a UE

SDN/NFV-based Evolved Packet Core



Security Advantages of SDN/NFV

A Comprehensive View of SDN/NFV Security Advantages

Performance Improvements:

Streamline and Reduce Incident Response Cycle Time

Streamline and Reduce Patching Cycle Time

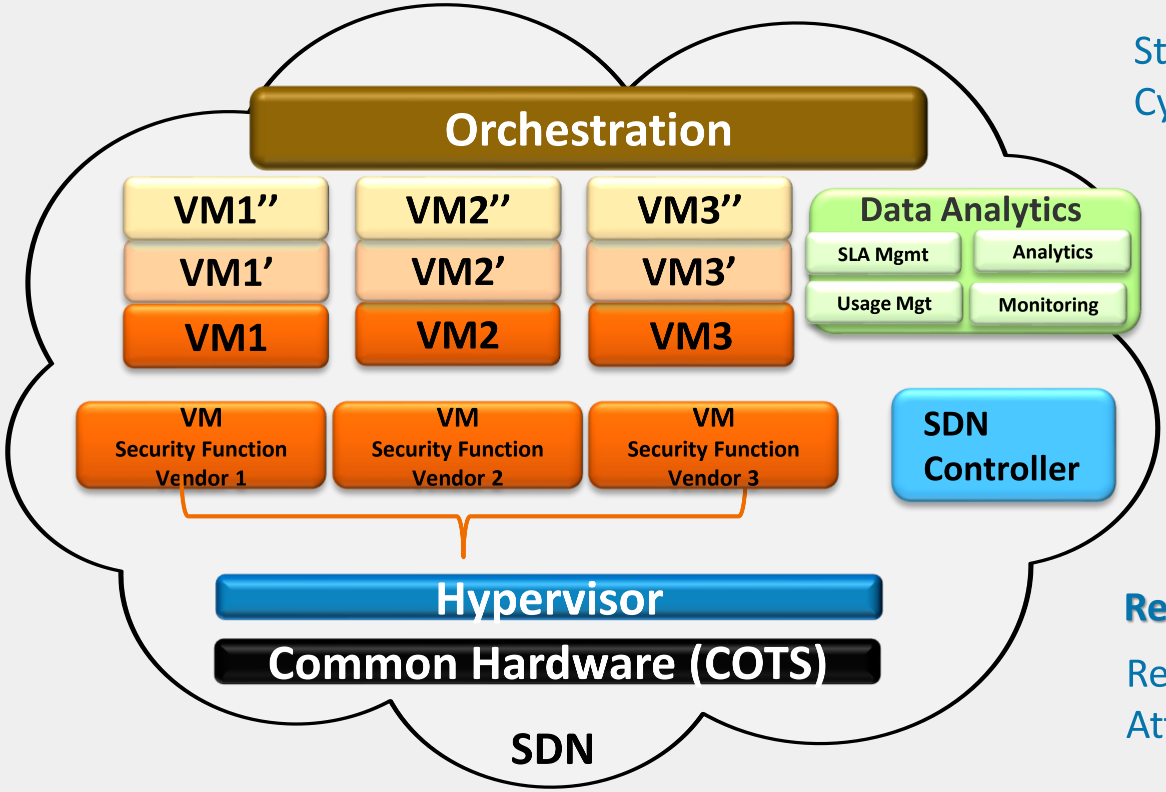
Design Enhancements:

Centralize Control and Management Functions

Security Embedded at Design Time

Security that Exceeds Existing Perimeter

Multivendor Security Service



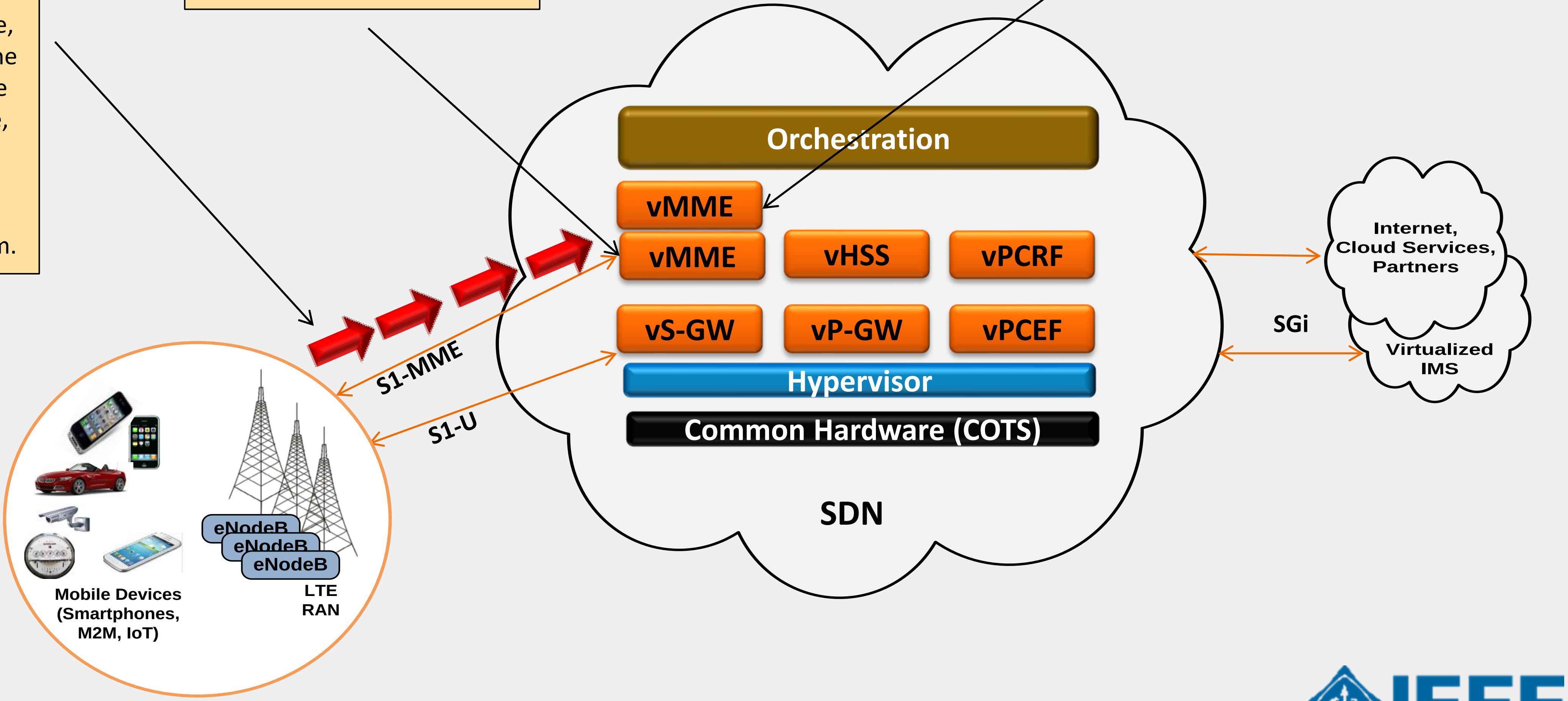
Real-Time capabilities:

Real-Time Scaling to Absorb DDOS Attacks

Real-Time Integration of "Add-on" Security Functions

Security Opportunities from Virtualization

DDoS Attack Resiliency – Control Plane



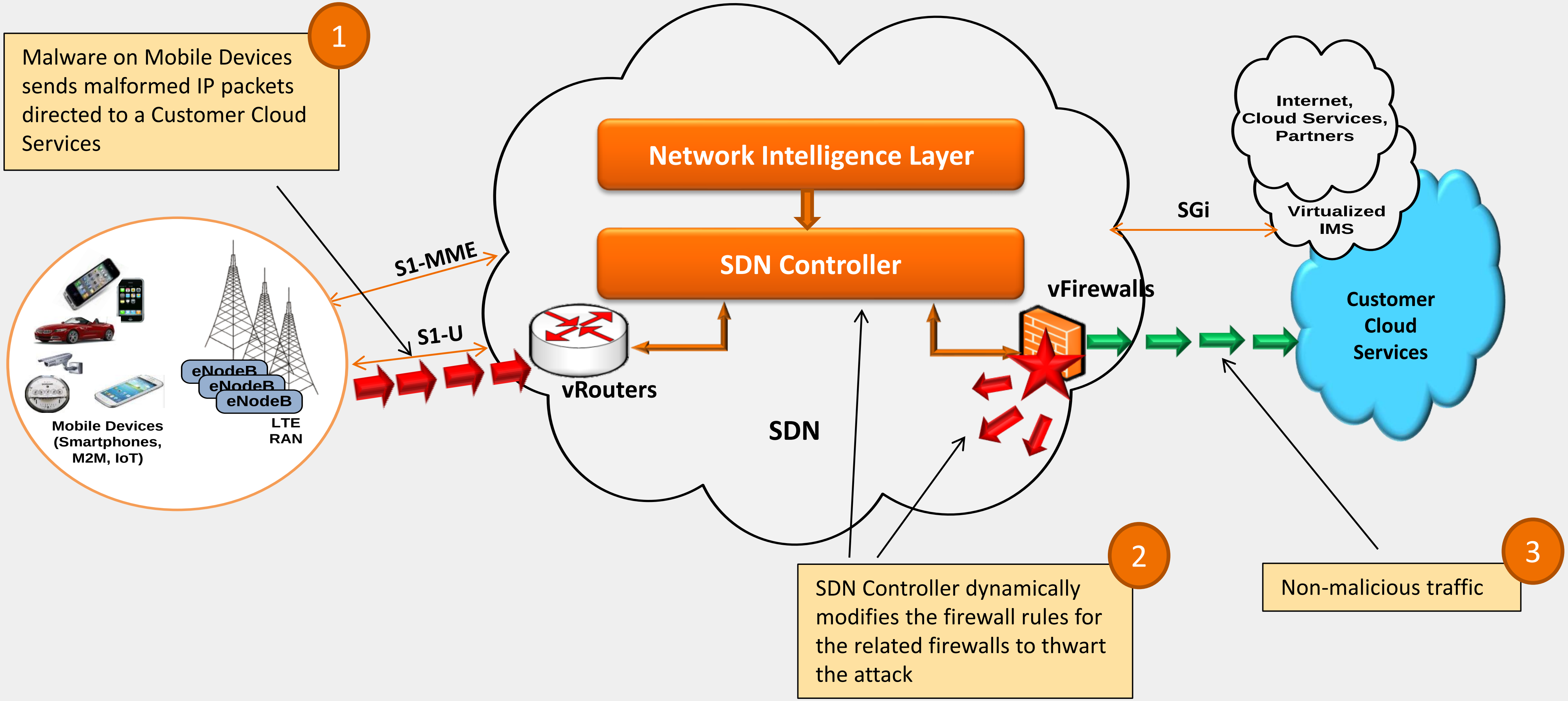
1 Attacker creates a Botnet army by infecting many Mobile devices with a ‘remote-reboot’ malware, attacker then instructs the malware to reboot all the devices at the same time, this will cause excessive malicious Attach Requests, creating a Malicious Signaling Storm.

2 vMME is under DDoS attack

3 Orchestrator instantiates new VM to scale-out vMME function to sustain the higher traffic load while we investigate.

Security Opportunities from Virtualization

SDN Controller Dynamic Security Control – Data Plane



1 Malware on Mobile Devices sends malformed IP packets directed to a Customer Cloud Services

2 SDN Controller dynamically modifies the firewall rules for the related firewalls to thwart the attack

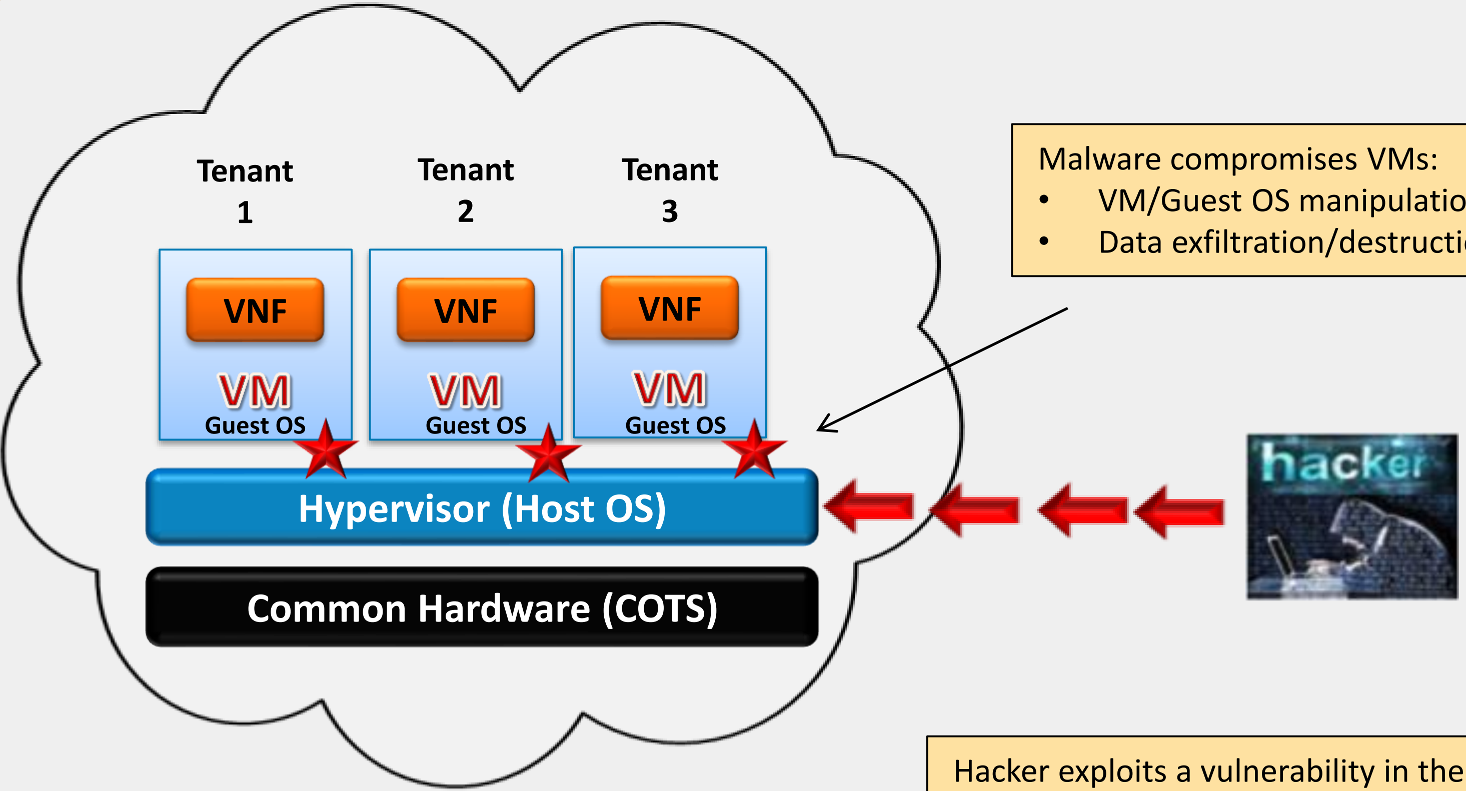
3 Non-malicious traffic

Security Challenges from Virtualization

Hypervisor Vulnerabilities

3

To prevent this type of attack, we must:
- ✓ Conduct security scans and apply security patches
- ✓ Ensure the Hypervisor is hardened and minimized (close vulnerable ports)
- ✓ Ensure the access to the Hypervisor is controlled via User Access Management,



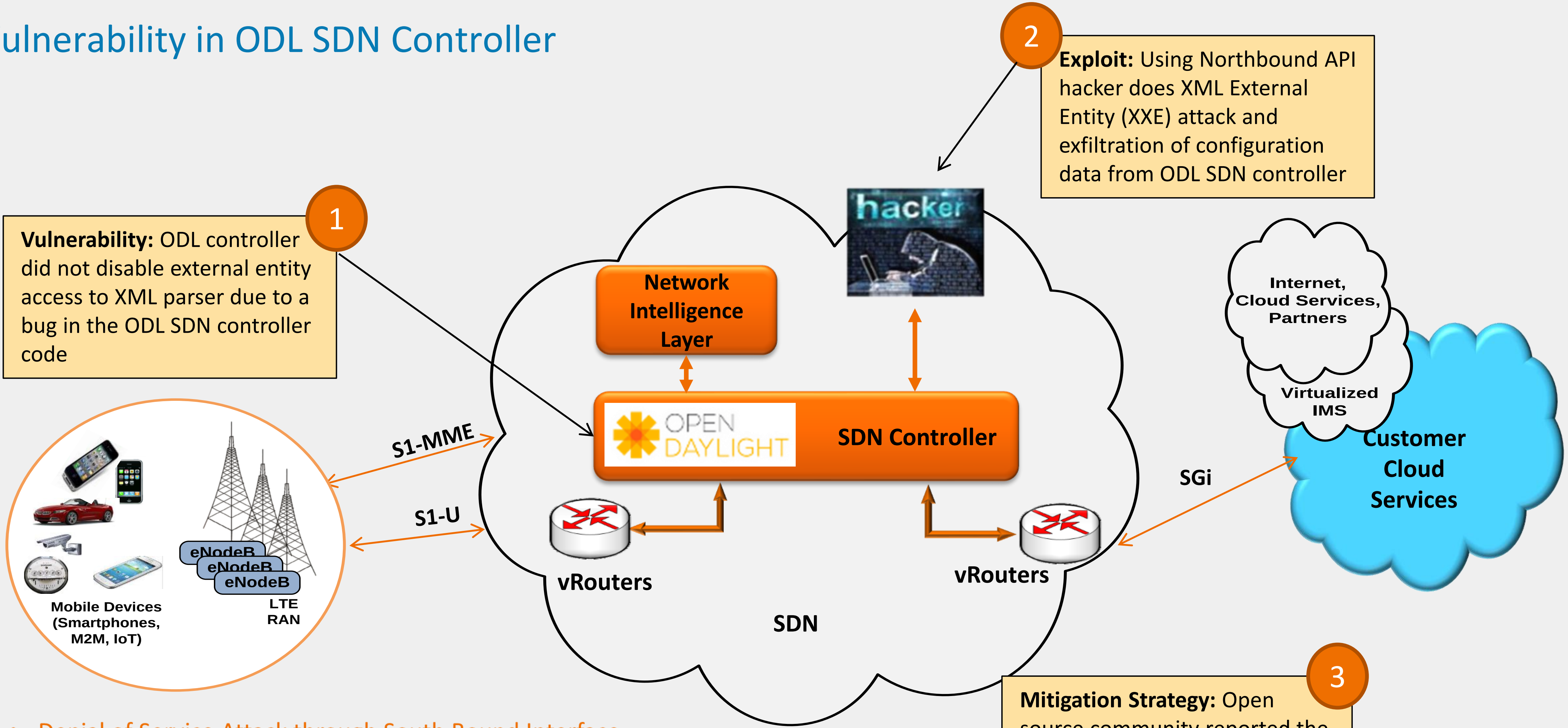
2

Malware compromises VMs:
- VM/Guest OS manipulation
- Data exfiltration/destruction

1

Hacker exploits a vulnerability in the Open Source code and infects the Hypervisor with a Malware

Security Vulnerability in ODL SDN Controller


1

Vulnerability: ODL controller did not disable external entity access to XML parser due to a bug in the ODL SDN controller code

2

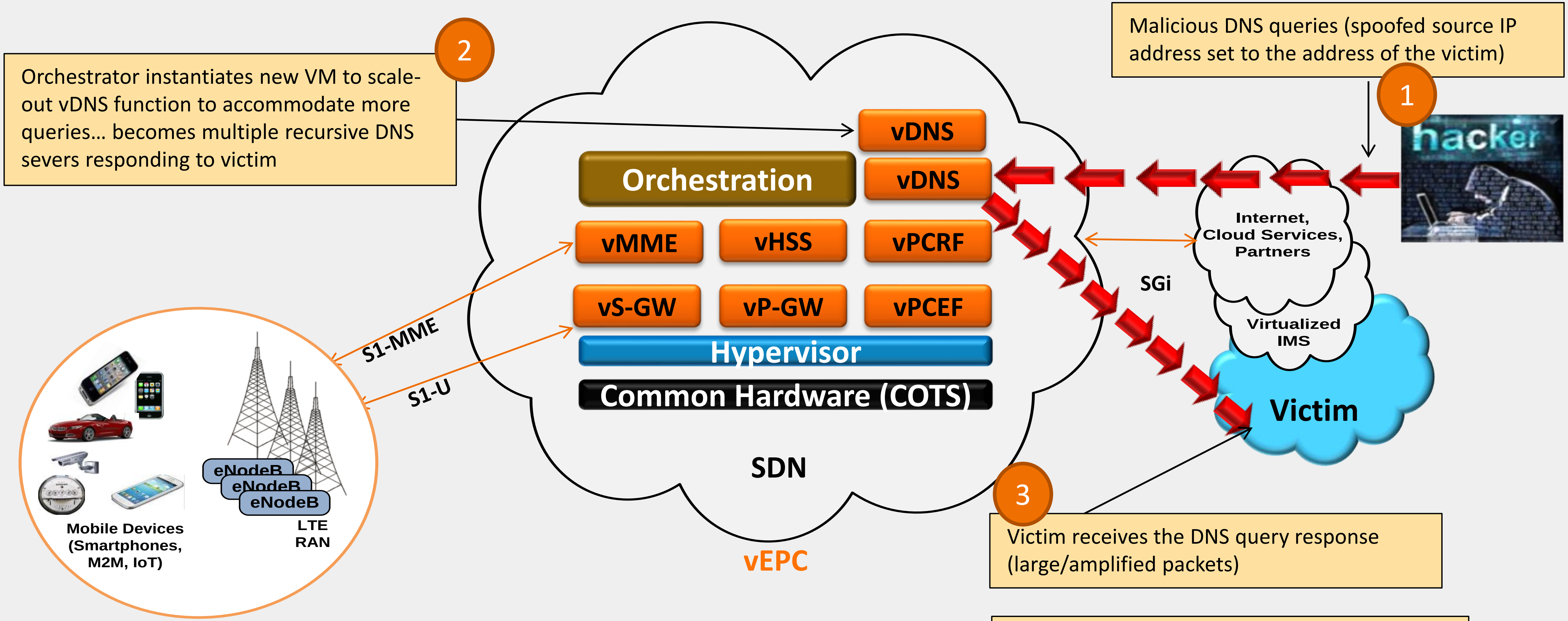
Exploit: Using Northbound API hacker does XML External Entity (XXE) attack and exfiltration of configuration data from ODL SDN controller

3

Mitigation Strategy: Open source community reported the problem, Patch was applied that disabled external entity access and fixed the problem.

- Denial of Service Attack through South Bound Interface
- REST API Parameter Exploitation – North Bound API
- North Bound API Flood Attack
- MAN-IN-THE MIDDLE ATTACK/Spoofing
- Protocol Fuzzing – South Bound
- Controller Impersonation – South Bound

DNS Amplification Attacks Enhanced by Elasticity Function



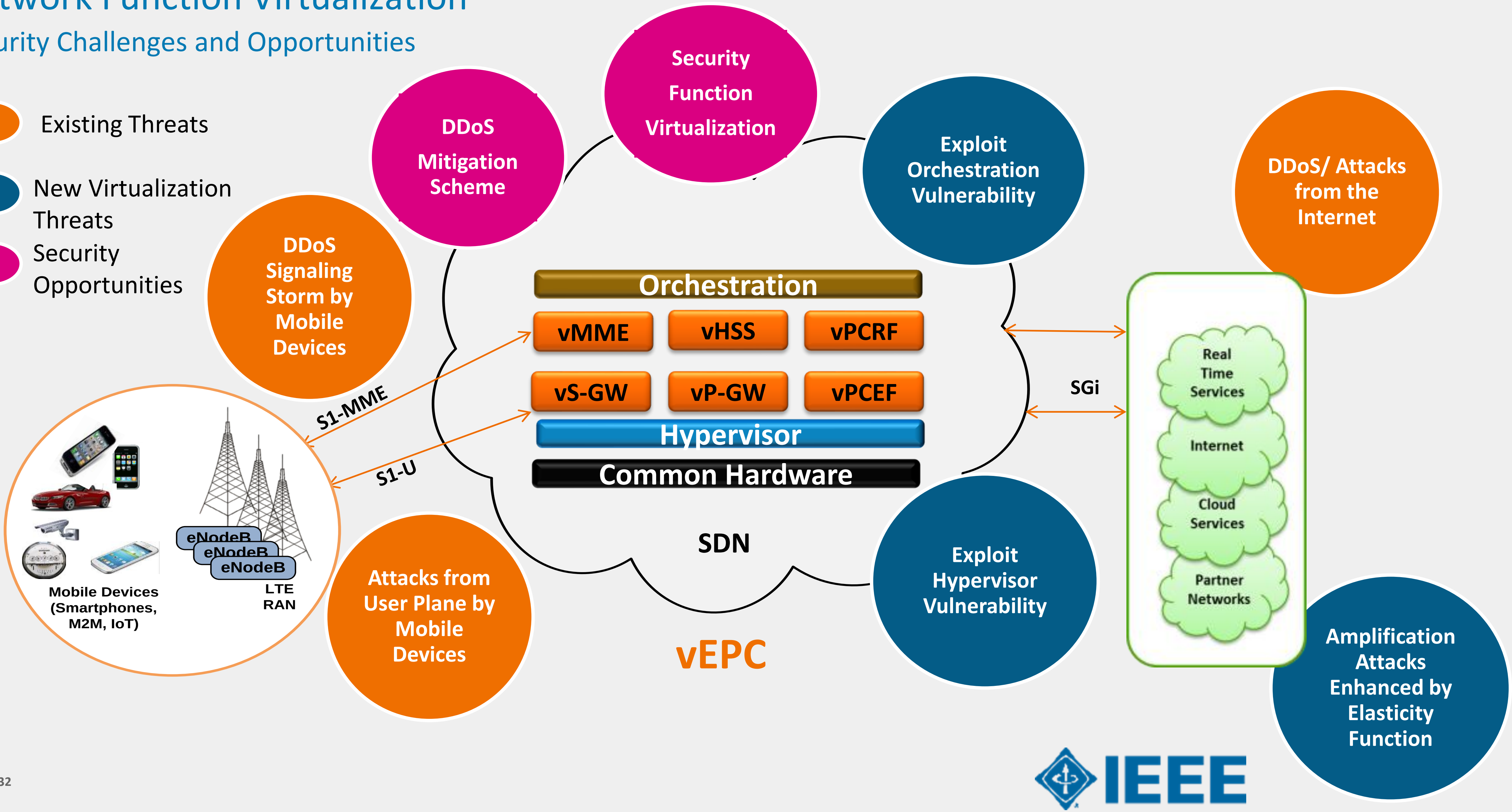
2
Orchestrator instantiates new VM to scale-out vDNS function to accommodate more queries… becomes multiple recursive DNS severs responding to victim
1
Malicious DNS queries (spoofed source IP address set to the address of the victim)
hacker
vDNS
vDNS
Orchestration
vMME
vHSS
vPCRF
vS-GW
vP-GW
vPCEF
Hypervisor
Common Hardware (COTS)
SDN
vEPC
S1-MME
S1-U
SGi
Internet, Cloud Services, Partners
Virtualized IMS
Victim
eNodeB
eNodeB
eNodeB
LTE RAN
Mobile Devices (Smartphones, M2M, IoT)
3
Victim receives the DNS query response (large/amplified packets)

NOTE: we must implement vIDS/vIPS & vFirewalls to mitigate these types of attacks

Network Function Virtualization

Security Challenges and Opportunities

- 🟠 Existing Threats
- 🔵 New Virtualization Threats
- 🟣 Security Opportunities



DDoS Mitigation Scheme

Security Function Virtualization

Exploit Orchestration Vulnerability

DDoS/ Attacks from the Internet

DDoS Signaling Storm by Mobile Devices

Orchestration

vMME | vHSS | vPCRF

vS-GW | vP-GW | vPCEF

Hypervisor

Common Hardware

SDN

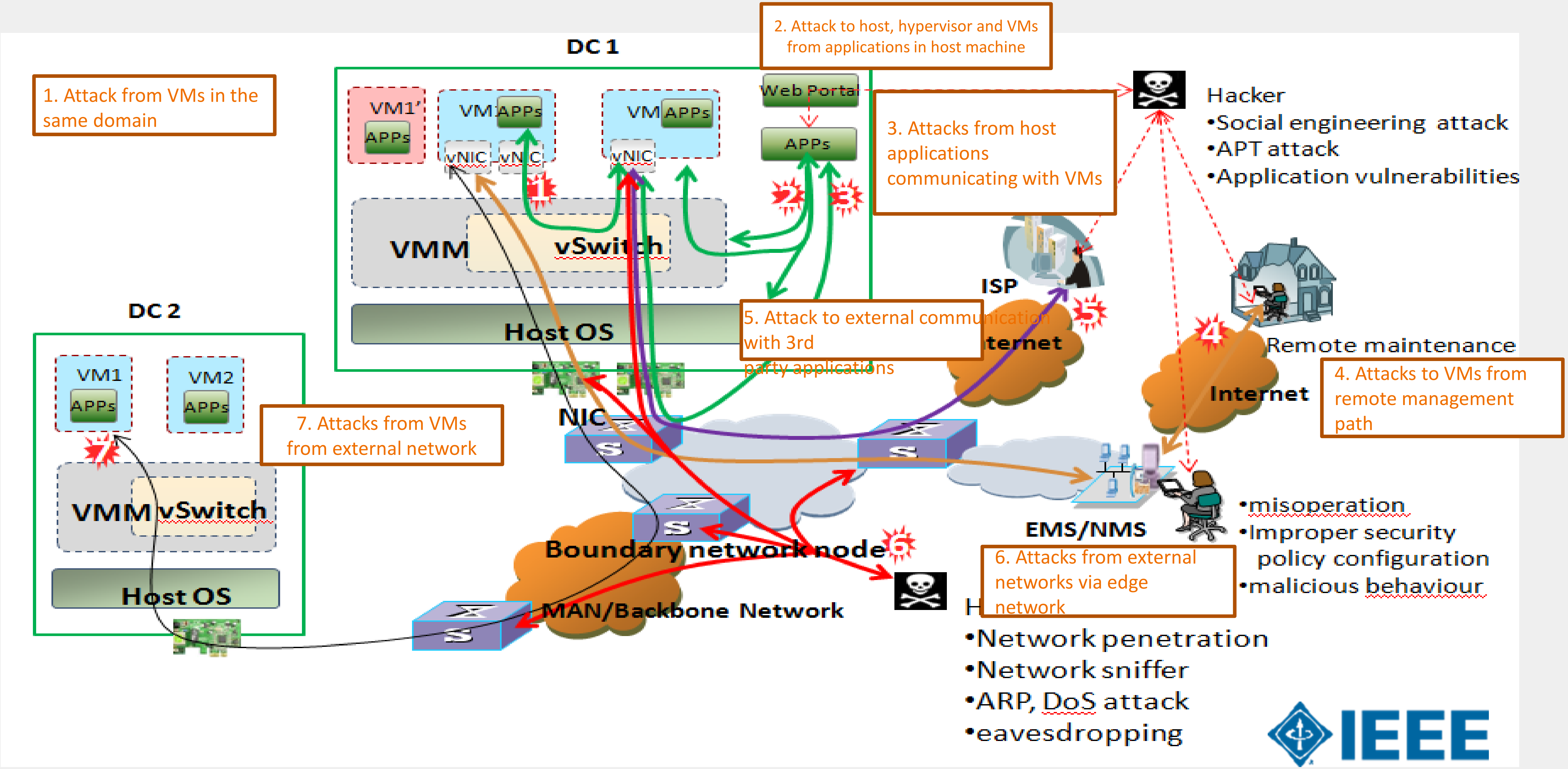
vEPC

Attacks from User Plane by Mobile Devices

Exploit Hypervisor Vulnerability

Amplification Attacks Enhanced by Elasticity Function

Threat Scenarios in NFV - Enterprise Networks(Reference - ETSI NFV)



1. Attack from VMs in the same domain

2. Attack to host, hypervisor and VMs from applications in host machine

3. Attacks from host applications communicating with VMs

4. Attacks to VMs from remote management path

5. Attack to external communication with 3rd party applications

6. Attacks from external networks via edge network

7. Attacks from VMs from external network

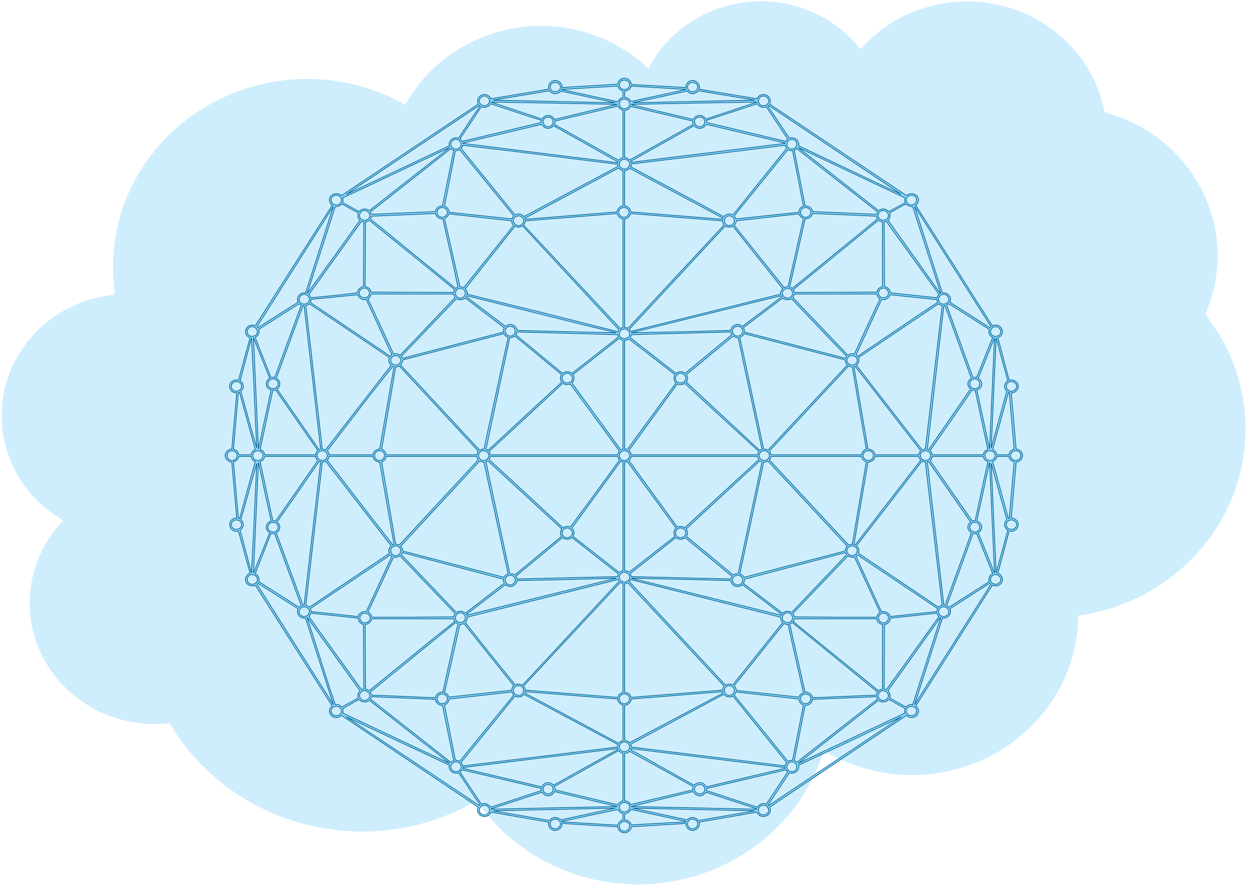
Hacker
- Social engineering attack
- APT attack
- Application vulnerabilities

- misoperation
- Improper security policy configuration
- malicious behaviour

H
- Network penetration
- Network sniffer
- ARP, DoS attack
- eavesdropping

IEEE

Security Pillars for 5G Core



RAN

(Cloud RAN / vRAN)

Network Slicing

Mobile Edge

Security Use Cases for 5G RAN

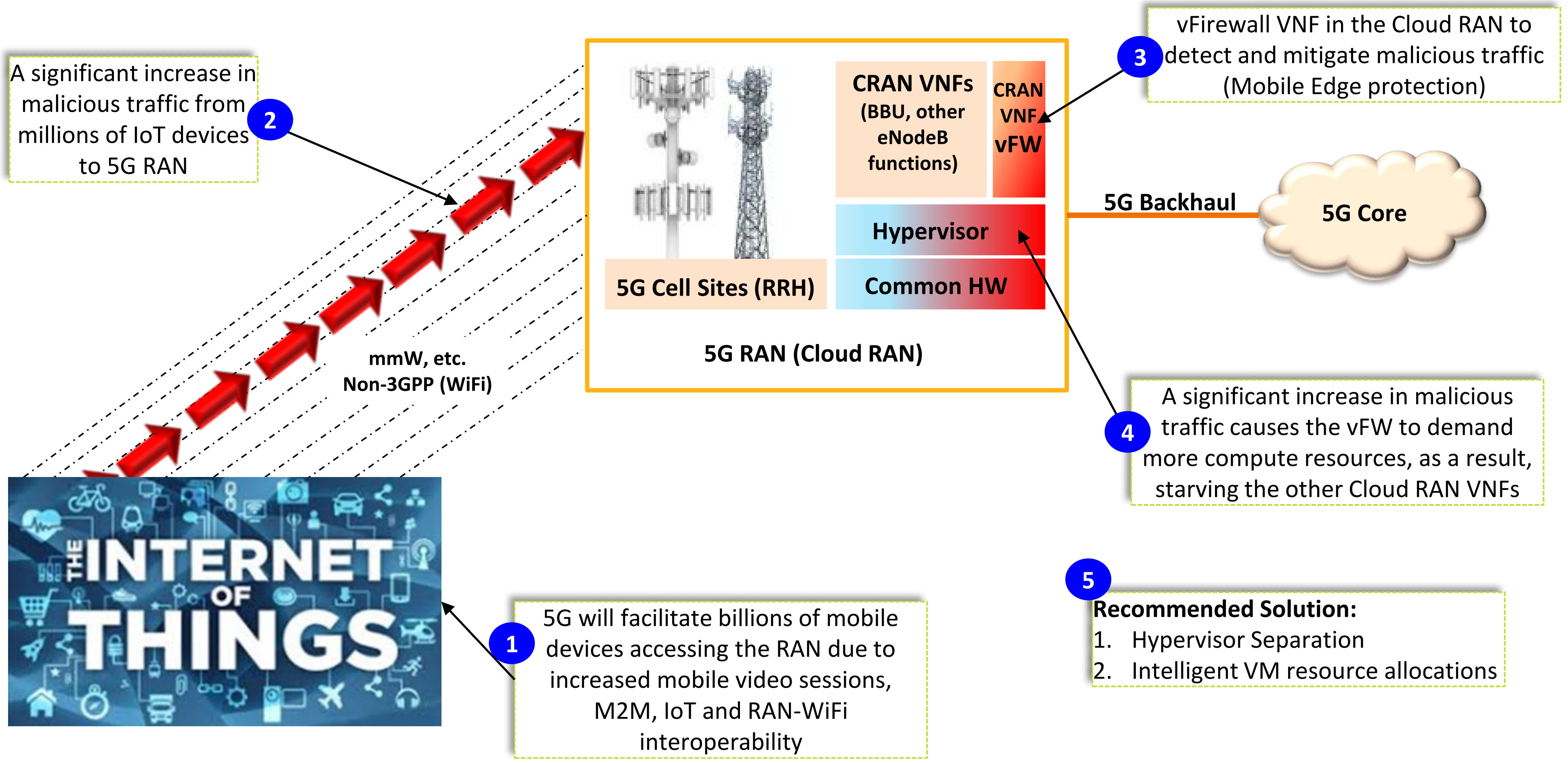
DDOS attacks against Network Infrastructure

- Overload of the signaling plane by a huge number of infected M2M/IOT devices that attempt to gain access
- Overload of the signaling plane by a huge number of infected M2M/IOT devices that transmit intermittently and simultaneously
- Resource Starvation at cRAN vFW
- Leverage IOT for Distributed Denial of Service
- Resource Sharing by multiple service providers at cRAN
- Deliberate triggering of network and overload mechanisms
- Bulk configuration

Virtualization (NFV and SDN) is the Foundation upon which 5G will be Built

Opportunities and Risks associated with Virtualization will apply to 5G VNFs

Use Case: CRAN (Cloud RAN) Resource Starvation due to 5G RAN Firewall Functions



1 5G will facilitate billions of mobile devices accessing the RAN due to increased mobile video sessions, M2M, IoT and RAN-WiFi interoperability

2 A significant increase in malicious traffic from millions of IoT devices to 5G RAN

mmW, etc.
Non-3GPP (WiFi)

5G Cell Sites (RRH)

CRAN VNFs (BBU, other eNodeB functions)

CRAN VNF vFW

Hypervisor

Common HW

5G RAN (Cloud RAN)

5G Backhaul

5G Core

3 vFirewall VNF in the Cloud RAN to detect and mitigate malicious traffic (Mobile Edge protection)

4 A significant increase in malicious traffic causes the vFW to demand more compute resources, as a result, starving the other Cloud RAN VNFs

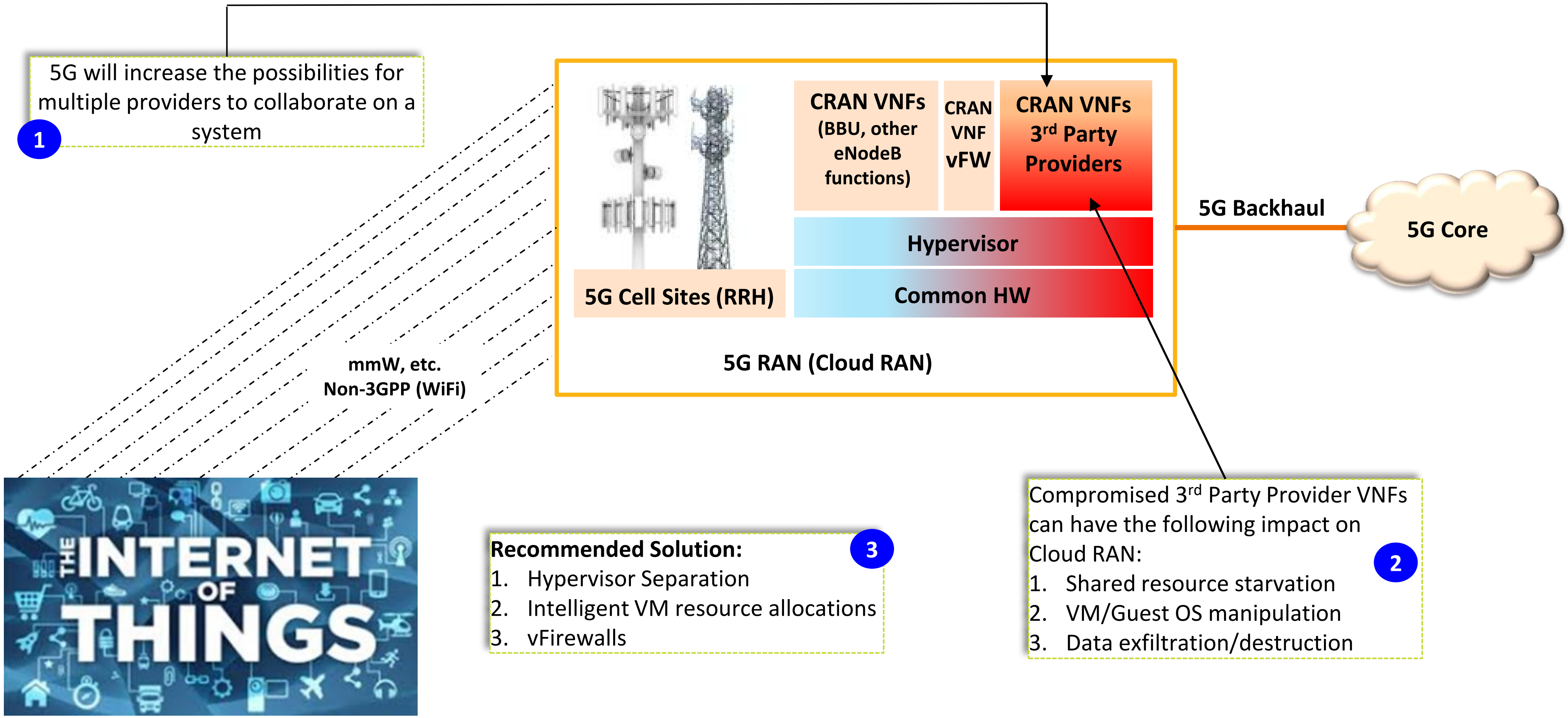
5 **Recommended Solution:**

1. Hypervisor Separation
2. Intelligent VM resource allocations

5G will Increase the Possibilities for Multiple Providers to Collaborate on a System

Increase the Risk of Compromise Shared Resources

Use Case: Compromise Shared Resources



① 5G will increase the possibilities for multiple providers to collaborate on a system

CRAN VNFs (BBU, other eNodeB functions)

CRAN VNF vFW

CRAN VNFs 3rd Party Providers

Hypervisor

Common HW

5G Cell Sites (RRH)

5G RAN (Cloud RAN)

5G Backhaul

5G Core

mmW, etc.
Non-3GPP (WiFi)

Recommended Solution: ③

1. Hypervisor Separation
2. Intelligent VM resource allocations
3. vFirewalls

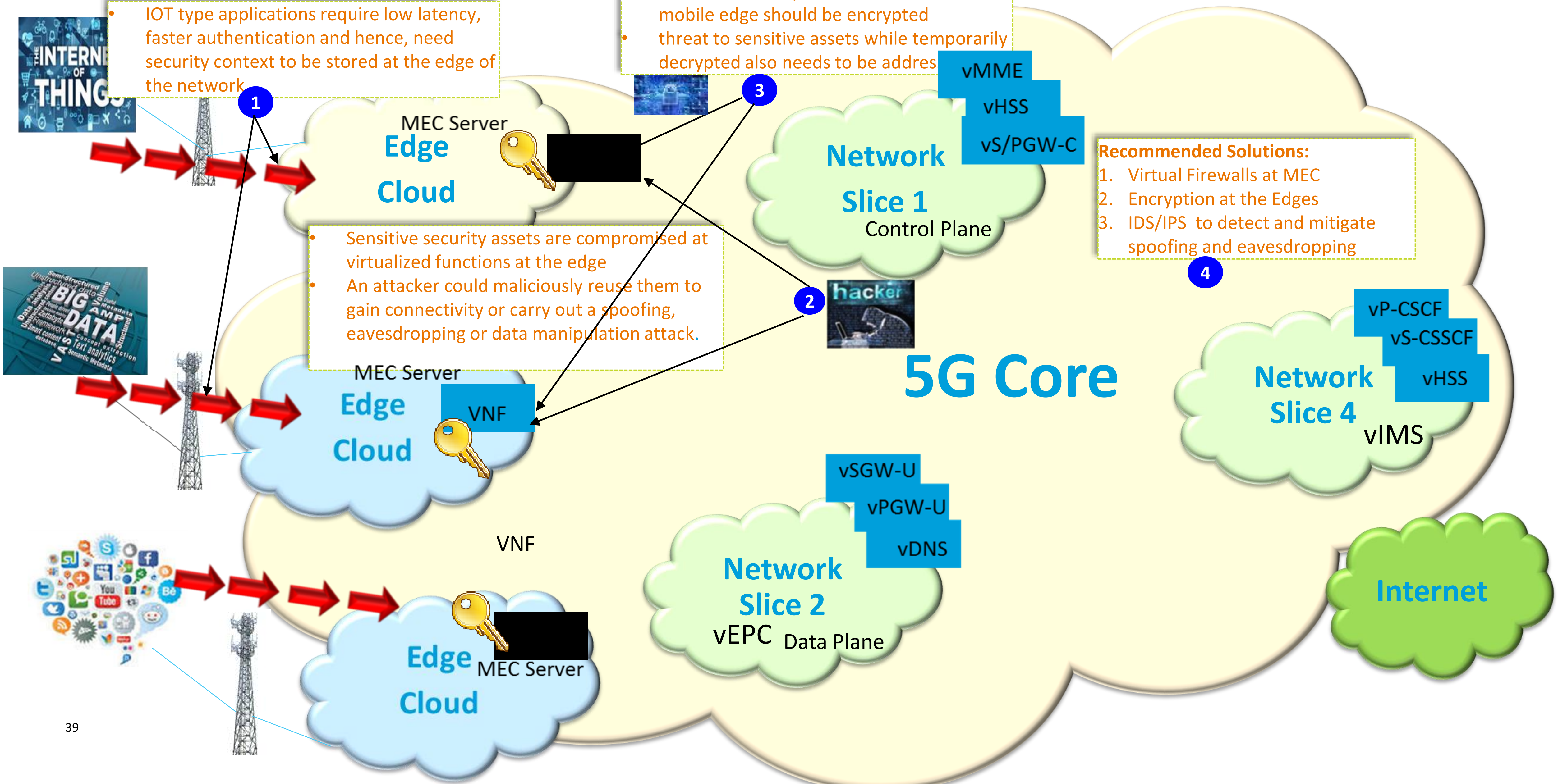
Compromised 3rd Party Provider VNFs can have the following impact on Cloud RAN: ②

1. Shared resource starvation
2. VM/Guest OS manipulation
3. Data exfiltration/destruction

Security Use Cases for Mobile Edge Computing

- Storage of Sensitive Security Assets at the Edge
- Third party applications on the same platform as network functions
- User Plane attacks in Mobile Edge Computing Environment
- Exchange of Sensitive Security Assets between core and Mobile Edge
- Trust establishment between functions at the core and at the edge
- Subscriber authentication within the visited network
- Secure storage of credentials to access IMS network
- Access to 5G core over non-3GPP network access
- User plane data security over less trusted 3GPP network accesses
- Management of credentials to access non-3GPP network access

Mobile Edge Computing – Use Case
Storage of Sensitive Security Context at the Mobile Edge



- IOT type applications require low latency, faster authentication and hence, need security context to be stored at the edge of the network

- Sensitive Security Assets stored at the mobile edge should be encrypted
- threat to sensitive assets while temporarily decrypted also needs to be addres

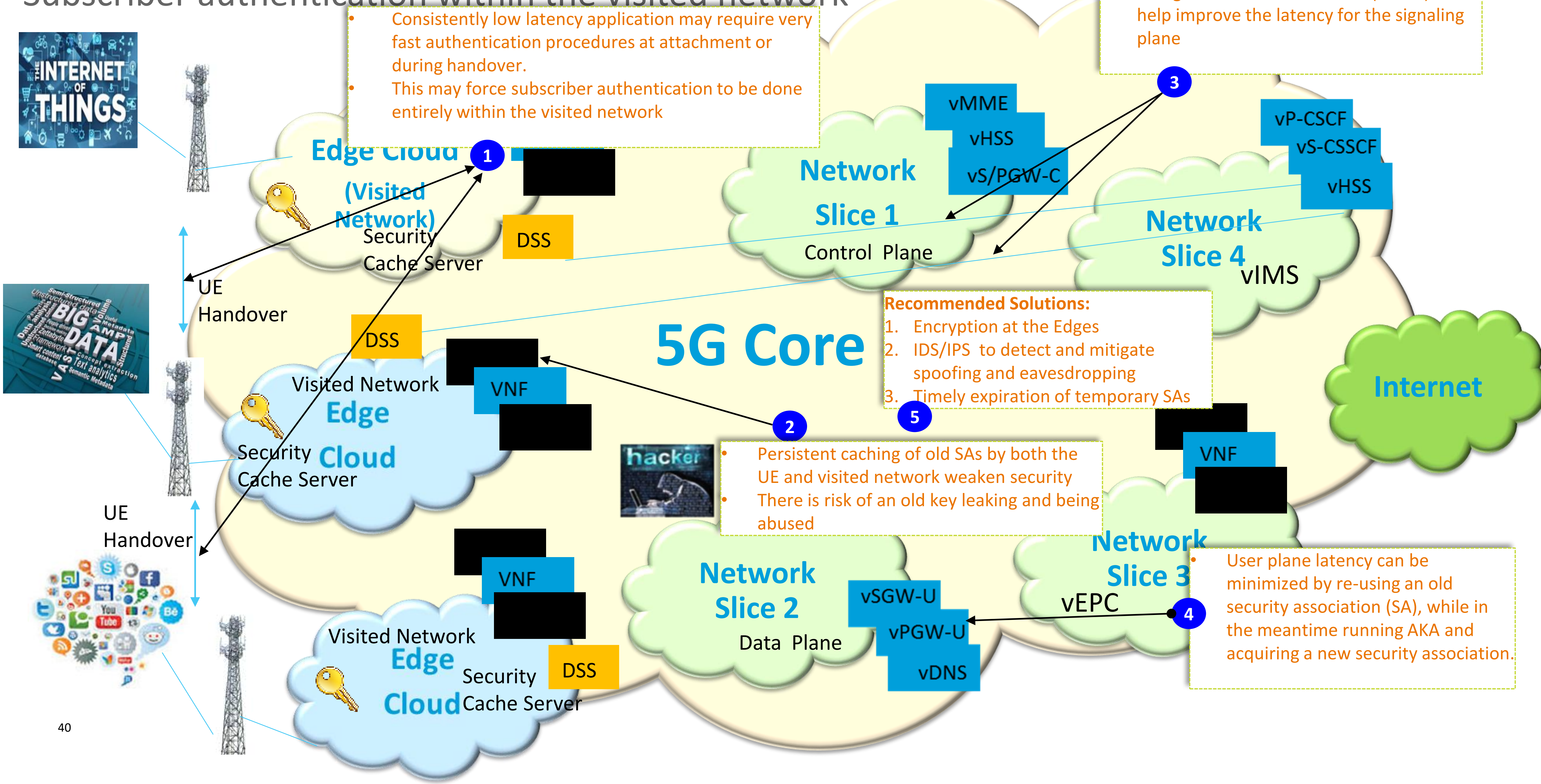
- Sensitive security assets are compromised at virtualized functions at the edge
- An attacker could maliciously reuse them to gain connectivity or carry out a spoofing, eavesdropping or data manipulation attack.

Recommended Solutions:
1. Virtual Firewalls at MEC
2. Encryption at the Edges
3. IDS/IPS to detect and mitigate spoofing and eavesdropping

Mobile Edge Computing – Low Latency during Handover

Subscriber authentication within the visited network

- Combine low latency on the user plane with high latency on the signaling plane.
- Delegated Subscriber Servers (DSSes) will help improve the latency for the signaling plane



- Consistently low latency application may require very fast authentication procedures at attachment or during handover.
- This may force subscriber authentication to be done entirely within the visited network

Recommended Solutions:

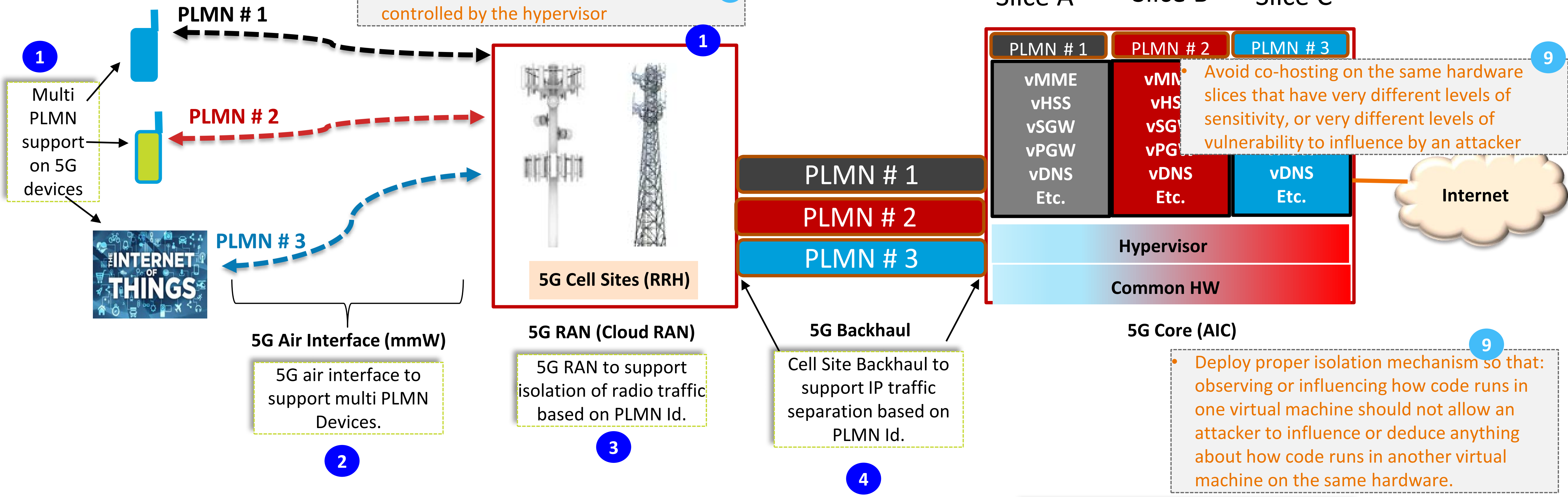
1. Encryption at the Edges
2. IDS/IPS to detect and mitigate spoofing and eavesdropping
3. Timely expiration of temporary SAs

- Persistent caching of old SAs by both the UE and visited network weaken security
- There is risk of an old key leaking and being abused

- User plane latency can be minimized by re-using an old security association (SA), while in the meantime running AKA and acquiring a new security association.

Network Slicing Use Case

Side channel attacks across Network slices



- Each slice is dedicated for a specific operator.
- These slices run on the same hardware controlled by the hypervisor

6

- If an attacker can observe or influence how code runs in functions in slice A, she/he may be able to affect the running of code in functions in the slice B machine, or extract information about the running of code in slice B.

7

- This may allow side channel attacks – in particular, timing attacks – that extract information about cryptographic keys or other secrets in slice B.

8

9

- Avoid co-hosting on the same hardware slices that have very different levels of sensitivity, or very different levels of vulnerability to influence by an attacker

5G air interface to support multi PLMN Devices.

2

5G RAN to support isolation of radio traffic based on PLMN Id.

3

Cell Site Backhaul to support IP traffic separation based on PLMN Id.

4

9

- Deploy proper isolation mechanism so that: observing or influencing how code runs in one virtual machine should not allow an attacker to influence or deduce anything about how code runs in another virtual machine on the same hardware.

5

1. All required core network elements (VNFs) are configured for each slice; i.e. PLMN id via VNFs in AIC.
2. CBB (MPLS) network to support separation of core network IP traffic based on PLMN Id for each slide.

Public Land Mobile Network Identity (PLMN-ID) = three digit mobile country code (MCC) + a two or three digit mobile network code (MNC

Security Use Cases for Network Slicing

- Controlling Inter-Network Communications
- Instantiation time Impersonation attacks against Network Slice Manager
- Impersonation attacks against a Network Slice instance within an Operator Network
- Impersonation attacks against different Network Slice managers within an Operator Network
- Different Security Protocols or Policies in different slices
- Denial of Service to other slices
- Exhaustion of security resources in other slices
- Side Channel Attacks Across Slices
- Hybrid Deployment Model
- Sealing between slices when UE is attached to several slices

Relevant SDN/NFV/5G Standards

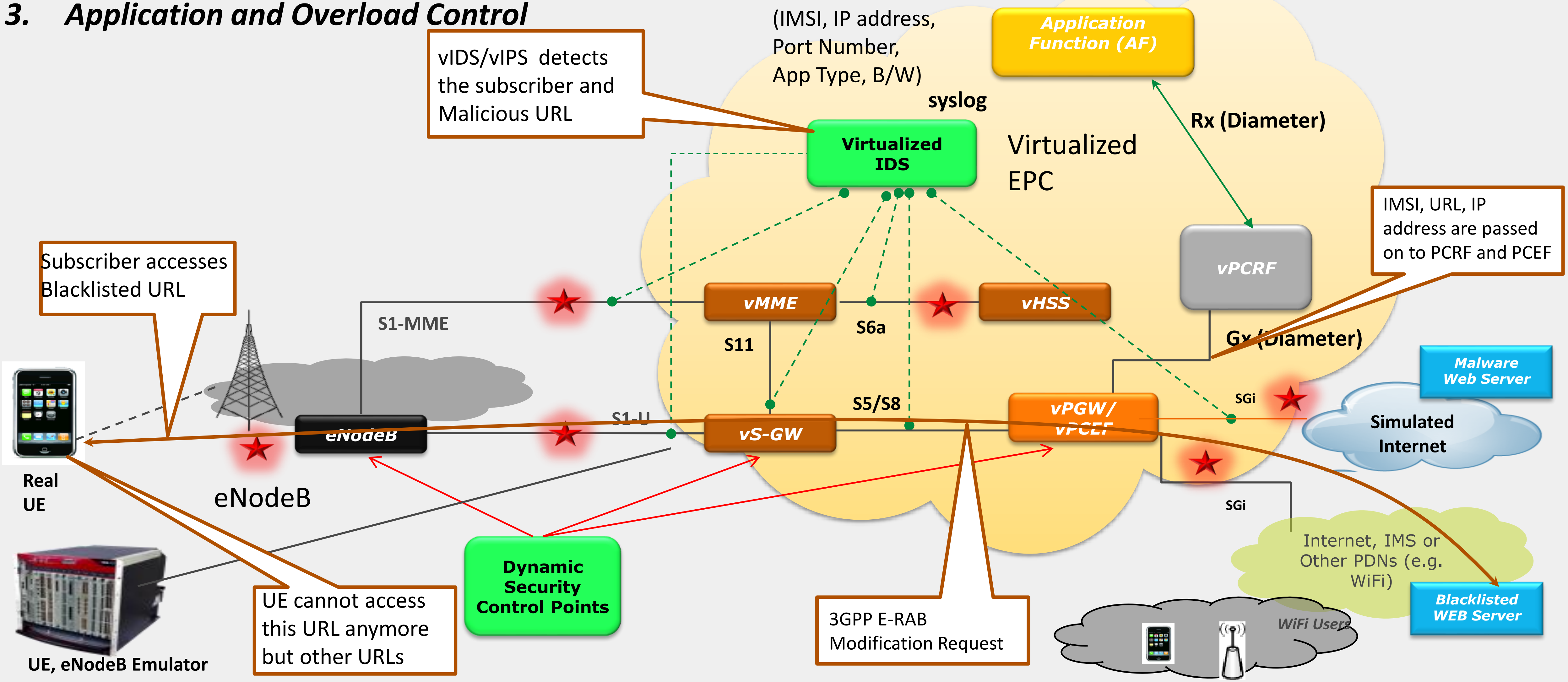
Forum	Focus
IETF	Network Virtualization Overlay, Dynamic Service Chaining, Network Service Header
3GPP	Mobility and Security Architecture and Specification
ETSI ISG NFV	NFV Platform/Deployment Standards – Security, Architecture/Interfaces, Reliability, Evolution, Performance
IEEE	Develop Technologies for that can be used by other Standards Bodies. There are 42 societies to contribute to 5G Eco System
ONF	OpenFlow SDN Controller Standards
OPNFV	NFV Open Platform/eCOMP/OPNFV Community TestLabs
Openstack	Cloud Orchestrator Open Source
OpenDaylight	Brownfield SDN Controller Open Source
ONOS	OpenFlow SDN Controller Open Source
DPDK/ODP	CPU/NIC HW API – Data Plane Development Kit
KVM Forum	Hypervisor
OVS	Open Source vSwitch
Linux	Operating System, Container Security
ATIS/NIST/FCC/CSA	Regulatory Aspects of SDN/NFV

ETSI/NFV Security Expert Group work Items

Work Items	Scope
NFV Security Problem Statement Document	Identifies and proposes solutions to any new vulnerabilities that result from the introduction of NFV
Security and Trust Guidance	Describes the security and trust guidance that is unique to NFV development, architecture and operation
Cataloguing Security Features in Management Software	Catalogue security features in management software relevant to NFV - OpenStack as the first case study.
Lawful Interception Implications	Identify the security and architecture pre-conditions for the provision of LI in an NVF based network
Certificate Management	Looks at various certificate deployment scenarios and describe certificate specific use cases
Report on Security Aspects and Regulatory Concerns	Addresses the security aspects and regulatory concerns of NFV related documents and applications
Report on Attestation Technologies and Practices for Secure Deployments	Identifies gaps in existing attestation technologies and practice
Security Monitoring – Report on Use Cases and Requirements	Investigate the security monitoring requirements and deployment use cases in an NFV environment
Use cases for multi-layer host administration	Addresses provision of multi-layer administration issues within a single host.

Virtual IDS Prototype for Mobility CORE

1. ***Malicious URL Detection and Mitigation***
2. ***Malware Detection and Mitigation***
3. ***Application and Overload Control***



vIDS/vIPS detects the subscriber and Malicious URL

(IMSI, IP address, Port Number, App Type, B/W)

syslog

Application Function (AF)

Rx (Diameter)

Virtualized IDS

Virtualized EPC

IMSI, URL, IP address are passed on to PCRF and PCEF

vPCRF

Gx (Diameter)

Subscriber accesses Blacklisted URL

S1-MME

vMME

S6a

vHSS

S11

S5/S8

S1-U

eNodeB

vS-GW

vPGW/ vPCEF

SGi

Malware Web Server

Simulated Internet

Real UE

eNodeB

SGi

Internet, IMS or Other PDNs (e.g. WiFi)

Blacklisted WEB Server

WiFi Users

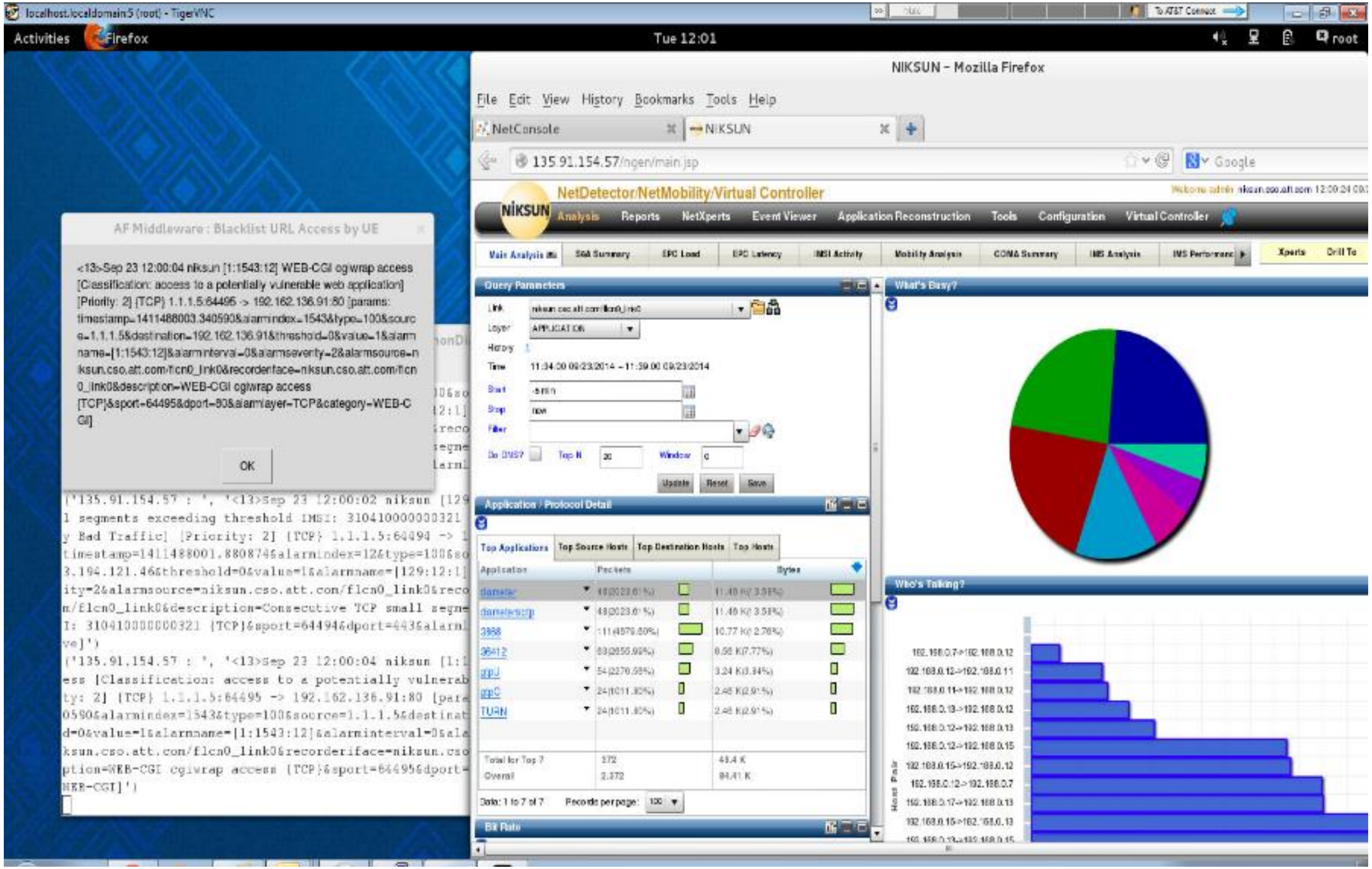
UE, eNodeB Emulator

UE cannot access this URL anymore but other URLs

Dynamic Security Control Points

3GPP E-RAB Modification Request

Blacklist Detection for DSC



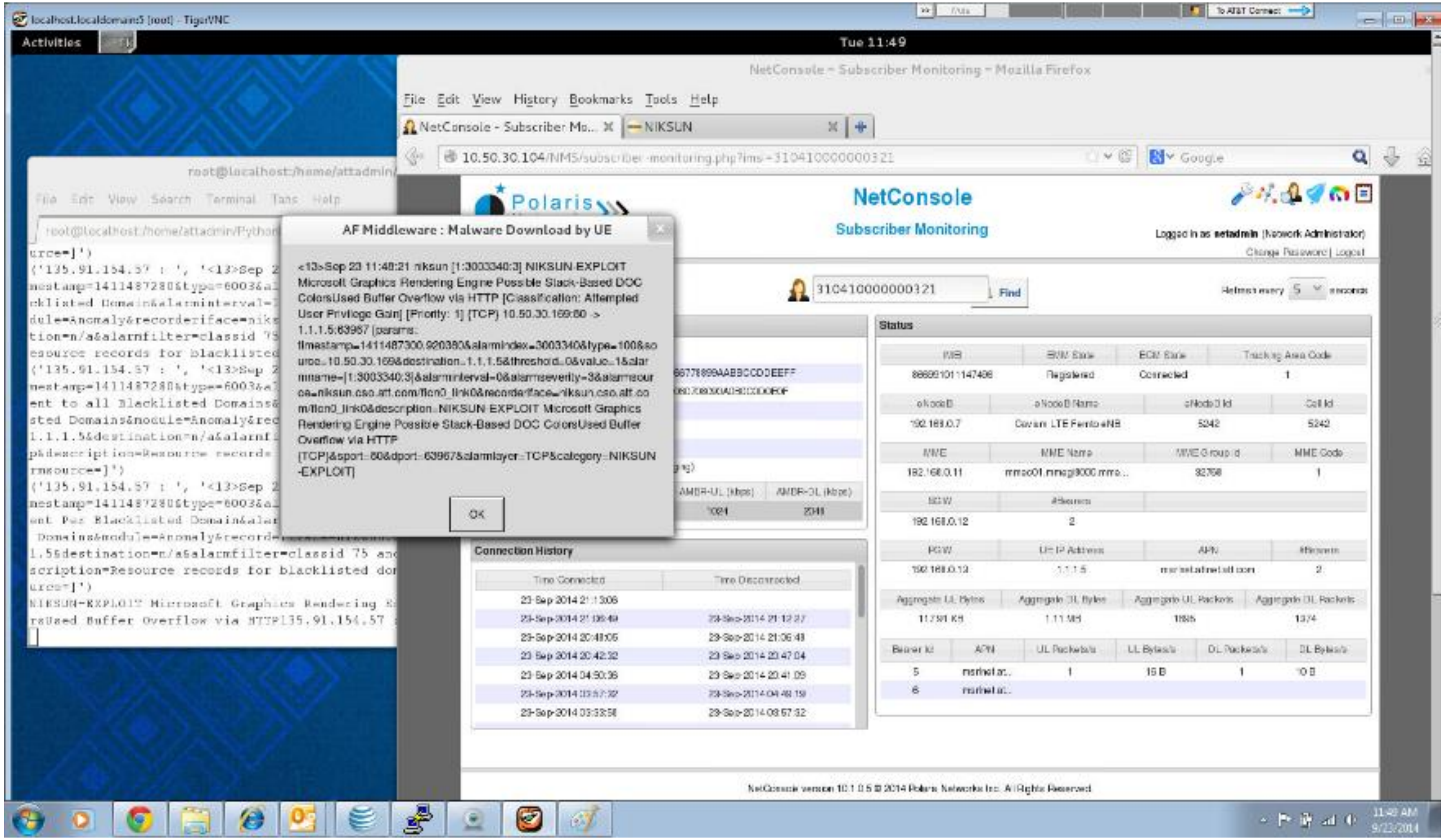
AF Middleware : Blacklist URL Access by UE

```
<13>Sep 23 12:00:04 niksun [1:1543:12] WEB-CGI cgiwrap access
[Classification: access to a potentially vulnerable web application]
[Priority: 2] {TCP} 1.1.1.5:64495 -> 192.162.136.91:80 [params:
timestamp=1411488003.340590&alarmindex=1543&type=100&sourc
e=1.1.1.5&destination=192.162.136.91&threshold=0&value=1&alarm
name=[1:1543:12]&alarminterval=0&alarmseverity=2&alarmsource=n
iksun.cso.att.com/flcn0_link0&recorderiface=niksun.cso.att.com/flcn
0_link0&description=WEB-CGI cgiwrap access
{TCP}&sport=64495&dport=80&alarmlayer=TCP&category=WEB-C
GI]
```

OK

```
('135.91.154.57 : ', '<13>Sep 23 12:00:02 niksun [129
1 segments exceeding threshold IMSI: 310410000000321
y Bad Traffic] [Priority: 2] {TCP} 1.1.1.5:64494 -> 1
timestamp=1411488001.880874&alarmindex=12&type=100&so
3.194.121.46&threshold=0&value=1&alarmname=[129:12:1]
ity=2&alarmsource=niksun.cso.att.com/flcn0_link0&reco
m/flcn0_link0&description=Consecutive TCP small segme
I: 310410000000321 {TCP}&sport=64494&dport=443&alarml
ve]')
('135.91.154.57 : ', '<13>Sep 23 12:00:04 niksun [1:1
ess [Classification: access to a potentially vulnerab
ty: 2] {TCP} 1.1.1.5:64495 -> 192.162.136.91:80 [para
0590&alarmindex=1543&type=100&source=1.1.1.5&destinat
d=0&value=1&alarmname=[1:1543:12]&alarminterval=0&ala
ksun.cso.att.com/flcn0_link0&recorderiface=niksun.cso
ption=WEB-CGI cgiwrap access {TCP}&sport=64495&dport=
WEB-CGI]')
```

Malware Download Detection for GDSC


localhost.localdomain:5 (root) - TigerVNC
Activities
Tue 11:49
NetConsole - Subscriber Monitoring - Mozilla Firefox
File Edit View History Bookmarks Tools Help
NetConsole - Subscriber Mo...
NIKSUN
10.50.30.104/NMS/subscriber-monitoring.php?imsi=310410000000321
Google
Polaris
root@localhost:/home/attadmin/
File Edit View Search Terminal Tabs Help
root@localhost:/home/attadmin/Python

```
urce=]')
('135.91.154.57 : ', '<13>Sep 2
mestamp=1411487280&type=6003&a
cklisted Domain&alarminterval=
dule=Anomaly&recorderiface=niks
tion=n/a&alarmfilter=classid 75
esource records for blacklisted
('135.91.154.57 : ', '<13>Sep 2
mestamp=1411487280&type=6003&a
ent to all Blacklisted Domains&
sted Domains&module=Anomaly&rec
1.1.1.5&destination=n/a&alarmf
p&description=Resource records
rmsource=]')
('135.91.154.57 : ', '<13>Sep 2
mestamp=1411487280&type=6003&a
ent Per Blacklisted Domain&alar
 Domains&module=Anomaly&record=
1.5&destination=n/a&alarmfilter=classid 75 and
scription=Resource records for blacklisted dom
urce=]')
NIKSUN-EXPLOIT Microsoft Graphics Rendering E
rsUsed Buffer Overflow via HTTP135.91.154.57 :
```

AF Middleware : Malware Download by UE

```
<13>Sep 23 11:48:21 niksun [1:3003340:3] NIKSUN-EXPLOIT
Microsoft Graphics Rendering Engine Possible Stack-Based DOC
ColorsUsed Buffer Overflow via HTTP [Classification: Attempted
User Privilege Gain] [Priority: 1] {TCP} 10.50.30.169:80 ->
1.1.1.5:63967 [params:
timestamp=1411487300.920380&alarmindex=3003340&type=100&so
urce=10.50.30.169&destination=1.1.1.5&threshold=0&value=1&alar
mname=[1:3003340:3]&alarminterval=0&alarmseverity=3&alarmsour
ce=niksun.cso.att.com/ifcn0_link0&recorderiface=niksun.cso.att.co
m/ifcn0_link0&description=NIKSUN-EXPLOIT Microsoft Graphics
Rendering Engine Possible Stack-Based DOC ColorsUsed Buffer
Overflow via HTTP
{TCP}&sport=80&dport=63967&alarmlayer=TCP&category=NIKSUN
-EXPLOIT]
```

NetConsole

Subscriber Monitoring

Logged in as **netadmin** (Network Administrator)

Change Password | Logout

310410000000321 Find

Refresh every 5 seconds

66778899AABBCCDDEEFF

AMBR-UL (kbps): 1024 | AMBR-DL (kbps): 2048

Status

IMEI	EMM State	ECM State	Tracking Area Code
86699101147406	Registered	Connected	1

eNodeB	eNodeB Name	eNodeB Id	Cell Id
192.168.0.7	Cavium LTE FemtoeNB	5242	5242

MME	MME Name	MME Group Id	MME Code
192.168.0.11	mmec01.mmegi8000.mme...	32768	1

SGW	#Bearers
192.168.0.12	2

PGW	UE IP Address	APN	#Bearers
192.168.0.13	1.1.1.5	msrnet.afnet.att.com	2

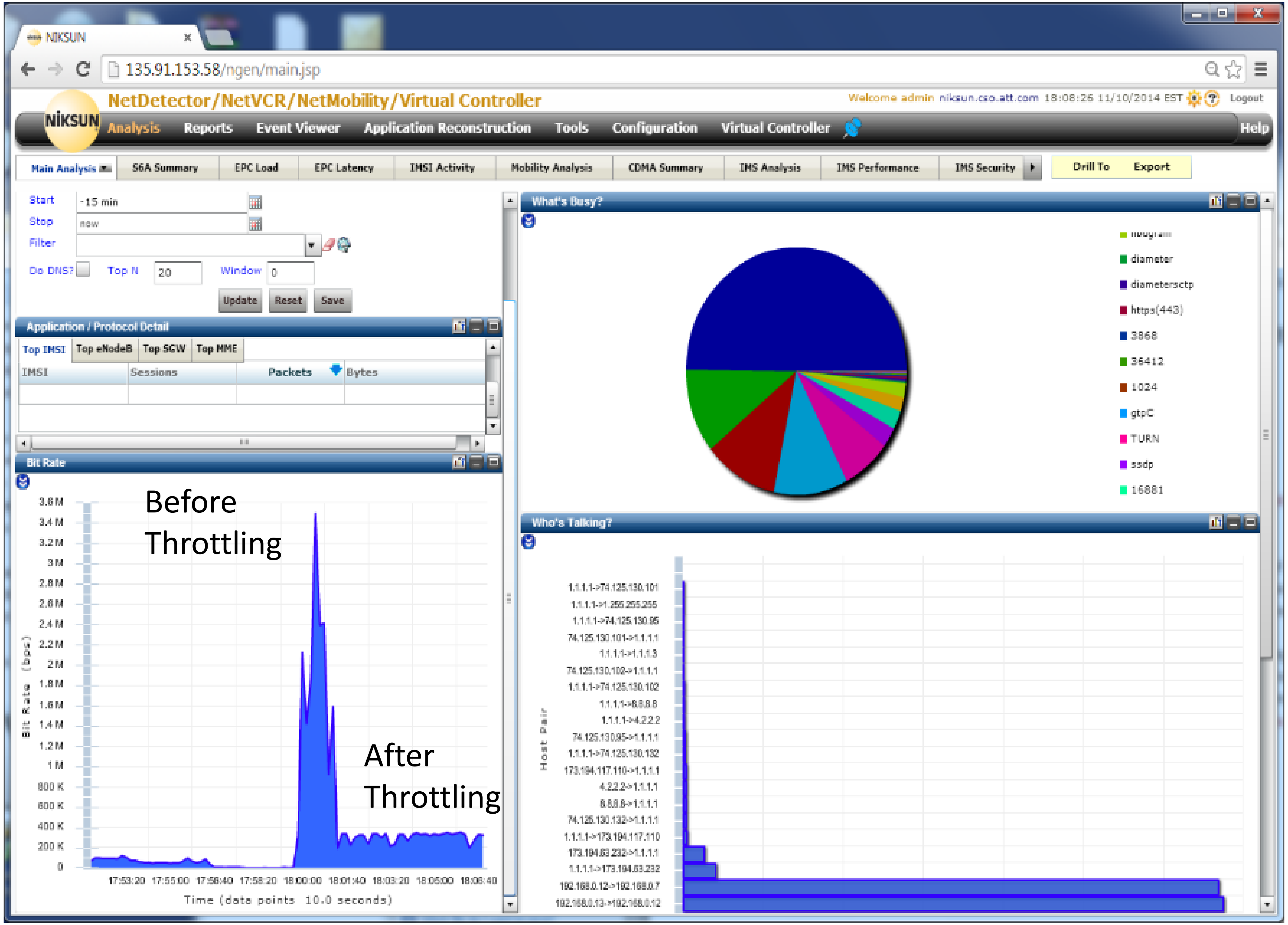
Aggregate UL Bytes	Aggregate DL Bytes	Aggregate UL Packets	Aggregate DL Packets
117.91 KB	1.11 MB	1885	1374

Bearer Id	APN	UL Packets/s	UL Bytes/s	DL Packets/s	DL Bytes/s
5	msrnet.at...	1	16 B	1	10 B
6	msrnet.at...				

Connection History

Time Connected	Time Disconnected
23-Sep-2014 21:13:06	
23-Sep-2014 21:06:49	23-Sep-2014 21:12:27
23-Sep-2014 20:48:05	23-Sep-2014 21:06:48
23-Sep-2014 20:42:32	23-Sep-2014 20:47:04
23-Sep-2014 04:50:36	23-Sep-2014 20:41:09
23-Sep-2014 03:57:32	23-Sep-2014 04:48:19
23-Sep-2014 03:33:58	23-Sep-2014 03:57:32

NetConsole version 10.1.0.5 © 2014 Polaris Networks Inc. All Rights Reserved.



Start: -15 min
Stop: now
Filter:
Do DNS? ☐
Top N: 20
Window: 0

Before Throttling

After Throttling

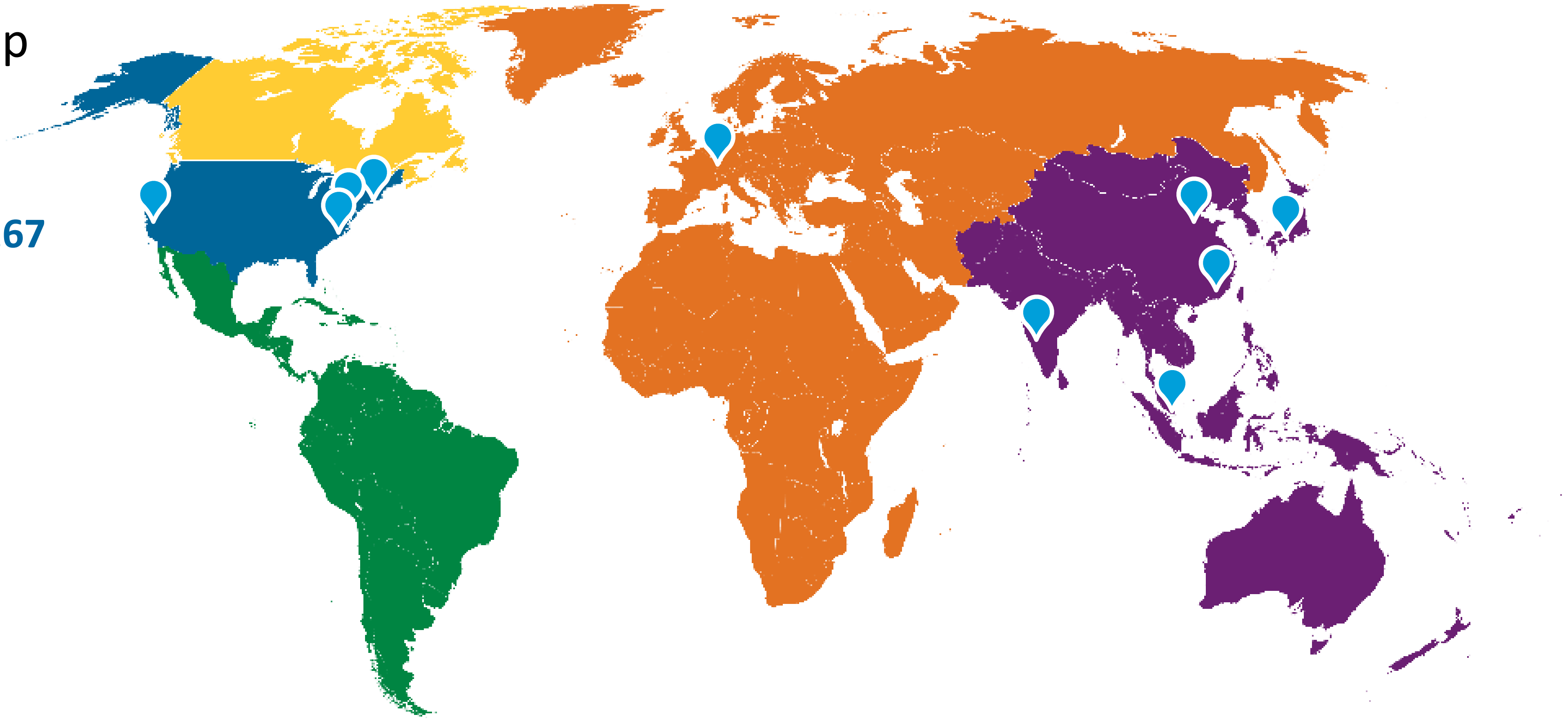
Summary

- Emerging services are evolving rapidly
- Network needs to be designed to be adaptable, resilient, and flexible
- Operators need to reduce Capex and Opex
- SDN/NFV is an enabler for 5G
- Opportunities and Challenges in this new virtualized environment
- 5G-specific application adds new security requirements
- Comprehensive security architecture is essential to take care of security challenges
- Operators and vendors need to work together to form a security ecosystem
- Standards, Testbeds and POCs act as catalyst for Virtualization

IEEE Membership By Region

Total Membership

421,355



🟦 R1 to 6 — **194,167**

🟨 R7 — **17,163**

🟧 R8 — **77,883**

🟩 R9 — **18,569**

🟪 R10 — **113,573**

📍 IEEE Offices

2018 FDC Initiatives & Activities

Small Projects

Environmental Engineering

Roadmaps Strategy and Governance (IRSG)

Quantum Computing

IEEE BLOCKCHAIN™

✓ IEEE Future NETWORKS™

IEEE brain

IEEE rebooting COMPUTING

IEEE DigitalReality

IEEE SYMBIOTIC AUTONOMOUS SYSTEMS™

IEEE TECHNOLOGY TIME MACHINE

Graduated Initiatives

IEEE BigData

IEEE Smart Cities

IEEE CLOUD COMPUTING

IEEE SMARTGRID

IEEE CYBER SECURITY

IEEE SOFTWARE DEFINED NETWORKS

IEEE Internet of Things

IEEE lifesciences

IEEE TRANSPORTATION ELECTRIFICATION COMMUNITY

IEEE SUSTAINABLEICT™

ieee.org/futuredirections

Key Stakeholders

IEEE Societies (22 so far)

IEEE PES Power & Energy Society®

SSCS

IEEE Technology and Engineering Management Society

A P S

IEEE Consumer Electronics Society

IEEE ComSoc™ IEEE Communications Society

IEEE VTS Connecting the Mobile World

IEEE Instrumentation & Measurement Society®

IEEE Standards Association

MTT-S®

AESS Aerospace and Electronic Systems Society

IEEE Photonics Society

IEEE Signal Processing Society®

ITSS Intelligent Transportation Systems Society IEEE

EMC Society

CEDA® IEEE Council on Electronic Design Automation

Electron Devices Society®

IEEE TEMS Technology & Engineering Management Society

IEEE Electronics Packaging Society

IEEE computer society

EMB

RFID IEEE Council on RFID Bridging the physical to the digital

Industry

Academia, Students

IEEE OUs

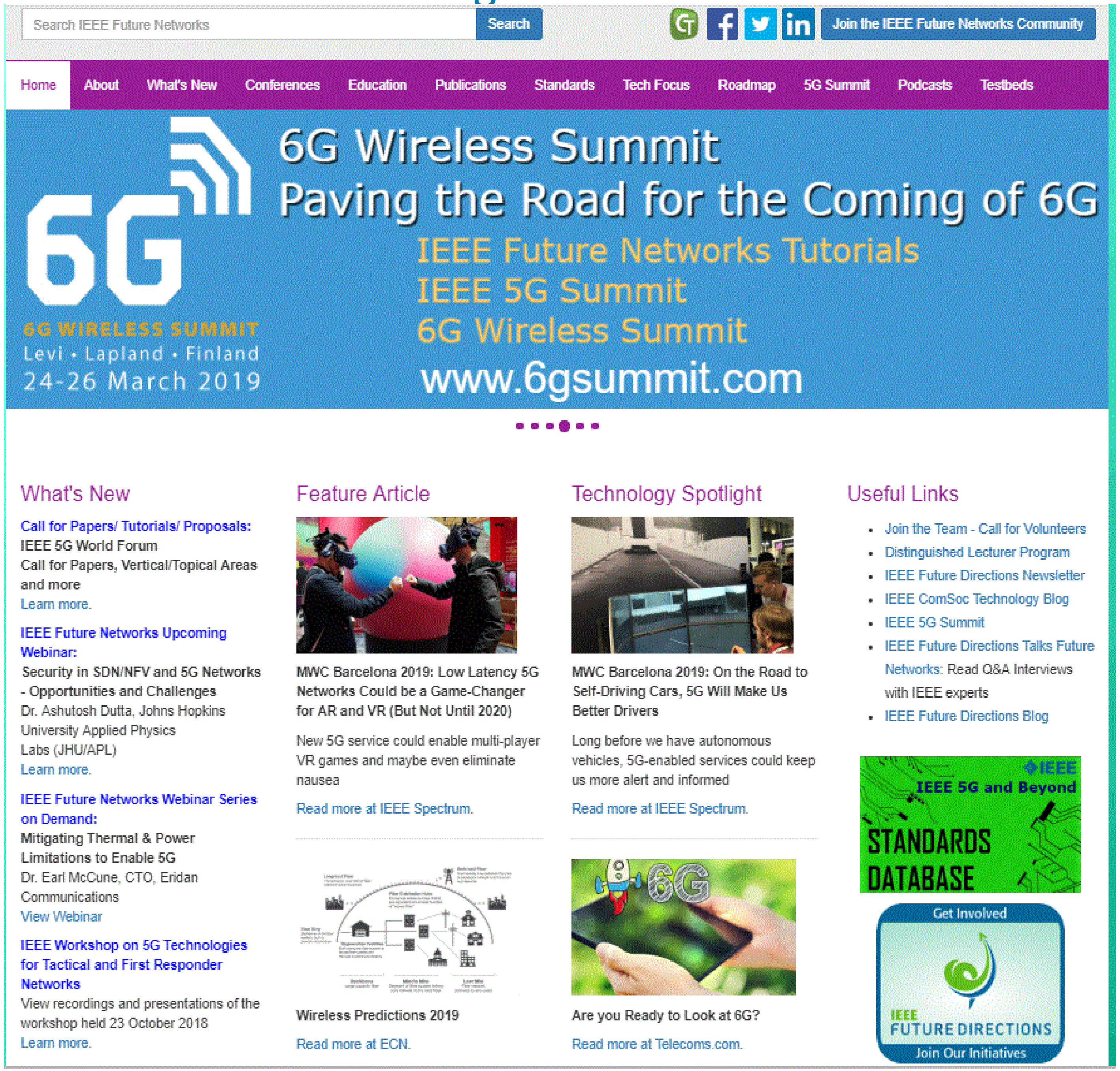
IEEE STANDARDS ASSOCIATION

IEEE EDUCATIONAL ACTIVITIES

Initiative Profile

- Launched August 2016
- Technical Activities Board Funded
- 20+ Participating Societies/OUs

Futurenetworks.IEEE.org



6G Wireless Summit
Paving the Road for the Coming of 6G
IEEE Future Networks Tutorials
IEEE 5G Summit
6G Wireless Summit
www.6gsummit.com

What's New

Call for Papers/ Tutorials/ Proposals:
IEEE 5G World Forum
Call for Papers, Vertical/Topical Areas and more
Learn more.

IEEE Future Networks Upcoming Webinar:
Security in SDN/NFV and 5G Networks - Opportunities and Challenges
Dr. Ashutosh Dutta, Johns Hopkins University Applied Physics Labs (JHU/APL)
Learn more.

IEEE Future Networks Webinar Series on Demand:
Mitigating Thermal & Power Limitations to Enable 5G
Dr. Earl McCune, CTO, Eridan Communications
View Webinar

IEEE Workshop on 5G Technologies for Tactical and First Responder Networks
View recordings and presentations of the workshop held 23 October 2018
Learn more.

Feature Article

MWC Barcelona 2019: Low Latency 5G Networks Could be a Game-Changer for AR and VR (But Not Until 2020)

New 5G service could enable multi-player VR games and maybe even eliminate nausea

Read more at IEEE Spectrum.

Wireless Predictions 2019

Read more at ECN.

Technology Spotlight

MWC Barcelona 2019: On the Road to Self-Driving Cars, 5G Will Make Us Better Drivers

Long before we have autonomous vehicles, 5G-enabled services could keep us more alert and informed

Read more at IEEE Spectrum.

Are you Ready to Look at 6G?

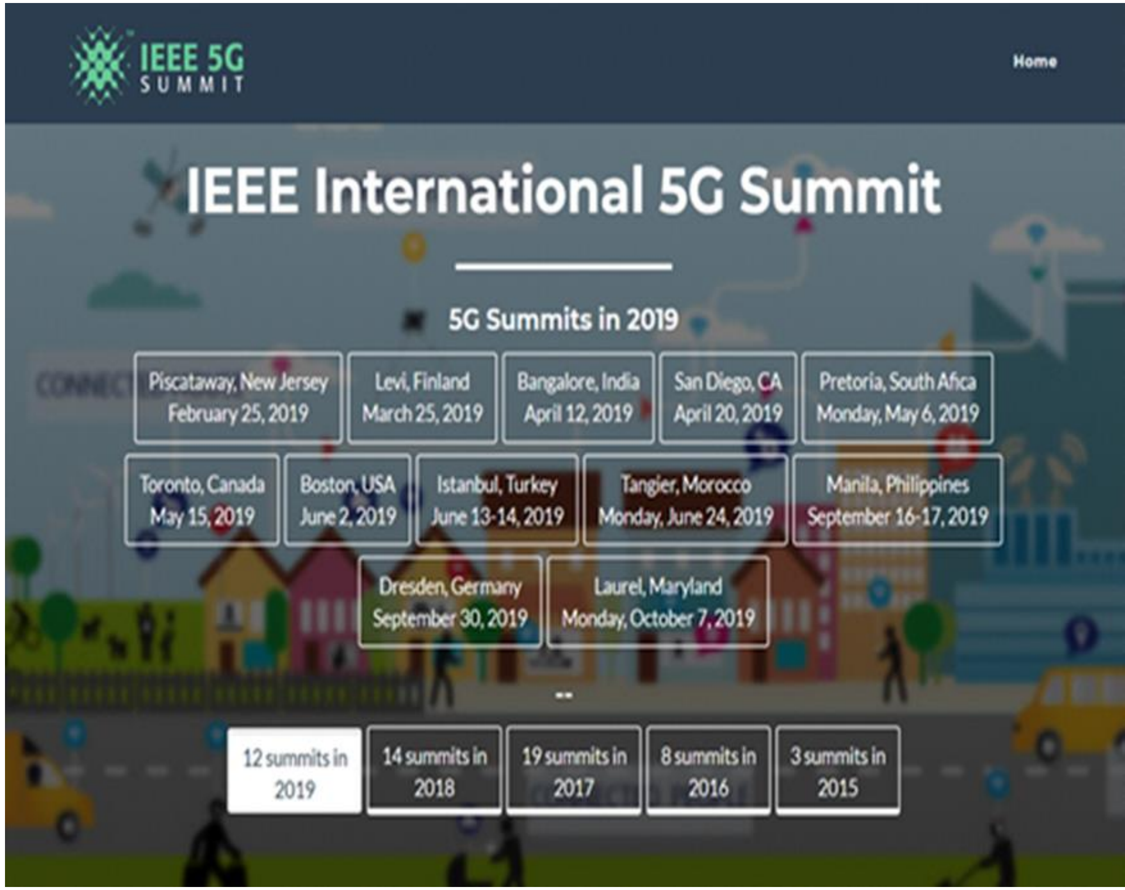
Read more at Telecoms.com.

Useful Links

- Join the Team - Call for Volunteers
- Distinguished Lecturer Program
- IEEE Future Directions Newsletter
- IEEE ComSoc Technology Blog
- IEEE 5G Summit
- IEEE Future Directions Talks Future Networks: Read Q&A Interviews with IEEE experts
- IEEE Future Directions Blog

Click here to view the Special Report on 5G in The Institute

5G The New Wireless Frontier



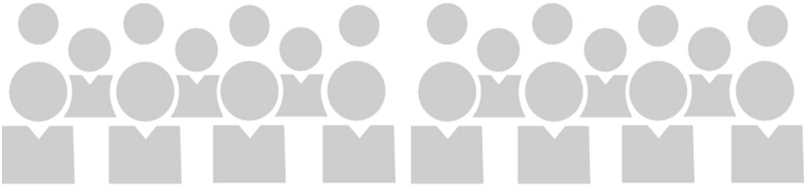
IEEE International 5G Summit

5G Summits in 2019

Piscataway, New Jersey February 25, 2019	Levi, Finland March 25, 2019	Bangalore, India April 12, 2019	San Diego, CA April 20, 2019	Pretoria, South Afica Monday, May 6, 2019
Toronto, Canada May 15, 2019	Boston, USA June 2, 2019	Istanbul, Turkey June 13-14, 2019	Tangier, Morocco Monday, June 24, 2019	Manila, Philippines September 16-17, 2019
Dresden, Germany September 30, 2019	Laurel, Maryland Monday, October 7, 2019			

12 summits in 2019	14 summits in 2018	19 summits in 2017	8 summits in 2016	3 summits in 2015

Led by a steering committee of 30 leaders from a diverse set of Future Networks-related IEEE Societies



The global team of experts involved in IEEE Future Networks are producing programs and activities including…

The Future Networks Roadmap

short-term (~3 years), mid-term (~5 years), and long-term (~10 years) research, innovation, and technology trends

Standards

Global, open, and collaborative

Conferences & Events

IEEE 5G Summits

IEEE 5G World Forums

Future Networks-related IEEE conferences

Education

IEEE Future Networks Learning Series

IEEE Live Online Courses, Webinar series

Videos from IEEE 5G Summits

Expert Articles

Published on IEEE Future Networks web portal and in industry media

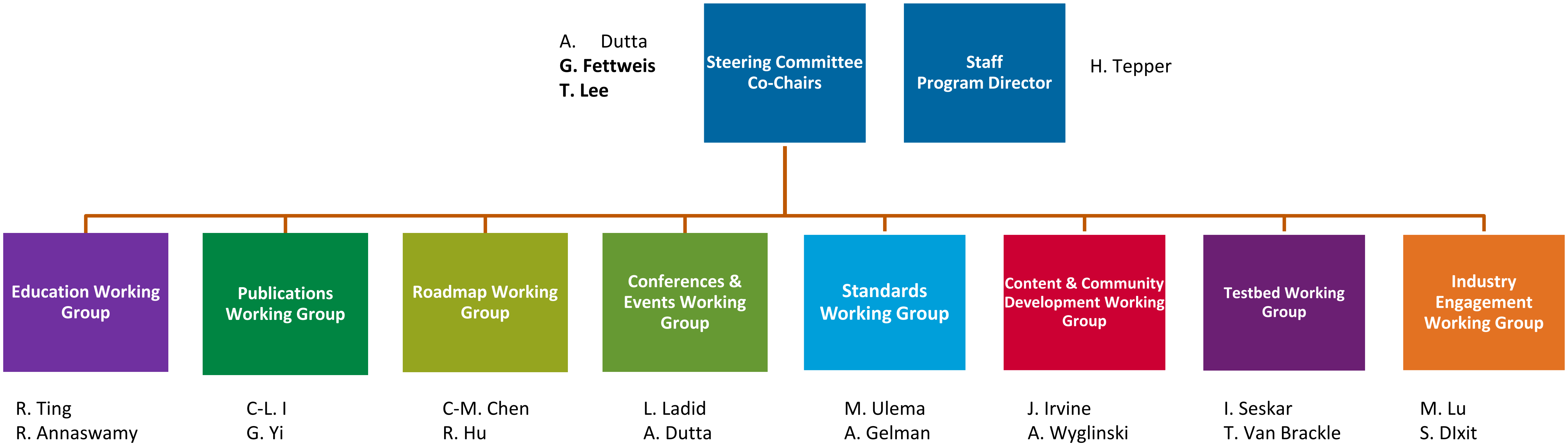
Publications

IEEE Future Networks Transmissions podcast series

IEEE Future Networks Tech Focus Newsletter

IEEE Future Directions Talks Future Networks Q&A article series

IEEE Future Networks Initiative Organization Structure



A. Dutta
G. Fettweis
T. Lee

Steering Committee Co-Chairs

Staff Program Director

H. Tepper

Education Working Group
R. Ting
R. Annaswamy

Publications Working Group
C-L. I
G. Yi

Roadmap Working Group
C-M. Chen
R. Hu

Conferences & Events Working Group
L. Ladid
A. Dutta

Standards Working Group
M. Ulema
A. Gelman

Content & Community Development Working Group
J. Irvine
A. Wyglinski

Testbed Working Group
I. Seskar
T. Van Brackle

Industry Engagement Working Group
M. Lu
S. DIxit

Roadmap Structure – Leadership and Working Group Co-chairs

Standardization Building Blocks
Paul Nikolich
Alex Gelman
Purva Rajkotia
Mehmet Ulema
mmWave and Signal Processing
Timothy Lee
Harish Krishnaswamy
Earl McCune
Hardware
Dylan Williams

Massive MIMO
Rose Quingyang Hu
Dongming Wang
Chris Ng
Chi Ming Chen
Haijian Sun
Applications and Services
Ravi Annaswamy
Narendra Mangra
Testbed
Ivan Seskar
Tracy Van Brakle

Security
Ashutosh Dutta
Ana Nieto
Ahmad Cheema
Satellite
Sastri Kota
Prashant Pillai
Giovanni Giambene
Edge Automation Platform
Meryem Simsek
Cagatay Buyukkoc
Kaniz Mahdi
Paul Littlewood

NEW FOR 2019
Systems Optimization
Ashutosh Dutta
Kaniz Mahdi
Optics
Feras Abou-Galala
Paul Littlewood
Deployment
David Witkowski

Connecting the Unconnected
Sudhir Dixit, Ashutosh Dutta

Ecosystem Stakeholders

- End users
- Application developers
- Service providers
- Equipment manufacturers
- Component suppliers
- Technology innovators
- Governments
- Standards and guidelines producing bodies

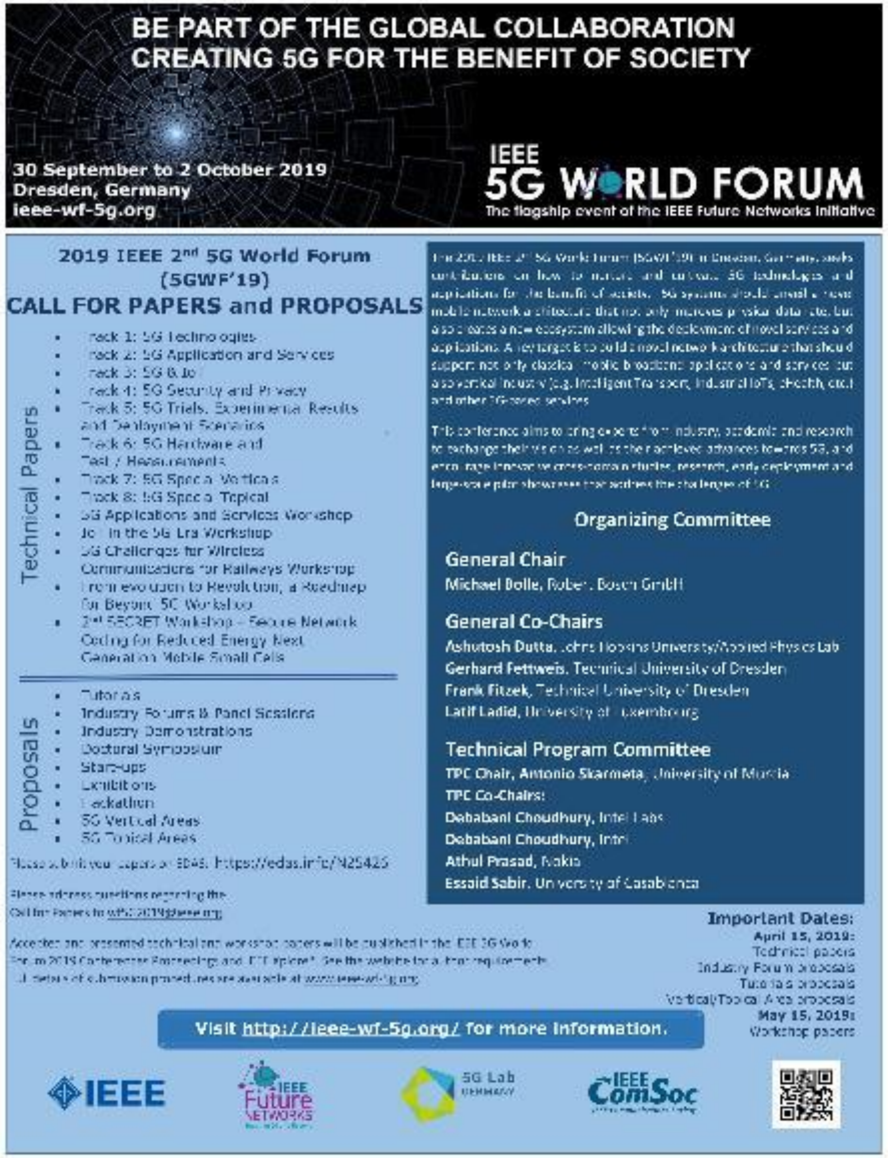
IEEE-SA
3GPP
ITU

Industry Interaction at Large

- The Roadmap effort will also include a series of meetings to gather additional inputs and feedback on trends related to:
- Business
- Technology
- Societal
- New fields
- Other industries

IEEE 5G World Forum 2019 and 2020

5G World Forum 2019 – Dresden, Germany



BE PART OF THE GLOBAL COLLABORATION
CREATING 5G FOR THE BENEFIT OF SOCIETY

30 September to 2 October 2019
Dresden, Germany
ieee-wf-5g.org

IEEE
5G WORLD FORUM
The flagship event of the IEEE Future Networks Initiative

2019 IEEE 2nd 5G World Forum (5GWF'19)
CALL FOR PAPERS and PROPOSALS

Technical Papers
- Track 1: 5G Technologies
- Track 2: 5G Application and Services
- Track 3: 5G & IoT
- Track 4: 5G Security and Privacy
- Track 5: 5G Trials, Experimental Results and Deployment Scenarios
- Track 6: 5G Hardware and Test / Measurements
- Track 7: 5G Special Verticals
- Track 8: 5G Special Topical
- 5G Applications and Services Workshop
- IoT in the 5G Era Workshop
- 5G Challenges for Wireless Communications for Railways Workshop
- From evolution to Revolution, a Roadmap for Beyond 5G Workshop
- 2nd SECRET Workshop – Secure Network Coding for Reduced Energy Next Generation Mobile Small Cells

Proposals
- Tutorials
- Industry Forums & Panel Sessions
- Industry Demonstrations
- Doctoral Symposium
- Start-ups
- Exhibitions
- Hackathon
- 5G Vertical Areas
- 5G Topical Areas

Please submit your papers on EDAS: https://edas.info/N25425

Please address questions regarding the Call for Papers to wf5g2019@ieee.org

Accepted and presented technical and workshop papers will be published in the IEEE 5G World Forum 2019 Conference Proceedings and IEEE Xplore®. See the website for author requirements. Full details of submission procedures are available at www.ieee-wf-5g.org

The 2019 IEEE 2nd 5G World Forum (5GWF'19) in Dresden, Germany, seeks contributions on how to nurture and cultivate 5G technologies and applications for the benefit of society. 5G systems should unveil a novel mobile network architecture that not only improves physical data rate, but also creates a new ecosystem allowing the deployment of novel services and applications. A key target is to build a novel network architecture that should support not only classical mobile broadband applications and services but also vertical industry (e.g. Intelligent Transport, Industrial IoTs, eHealth, etc.) and other 5G-based services.

This conference aims to bring experts from industry, academic and research to exchange their vision as well as their achieved advances towards 5G, and encourage innovative cross-domain studies, research, early deployment and large-scale pilot showcases that address the challenges of 5G.

Organizing Committee

General Chair
Michael Bolle, Robert Bosch GmbH

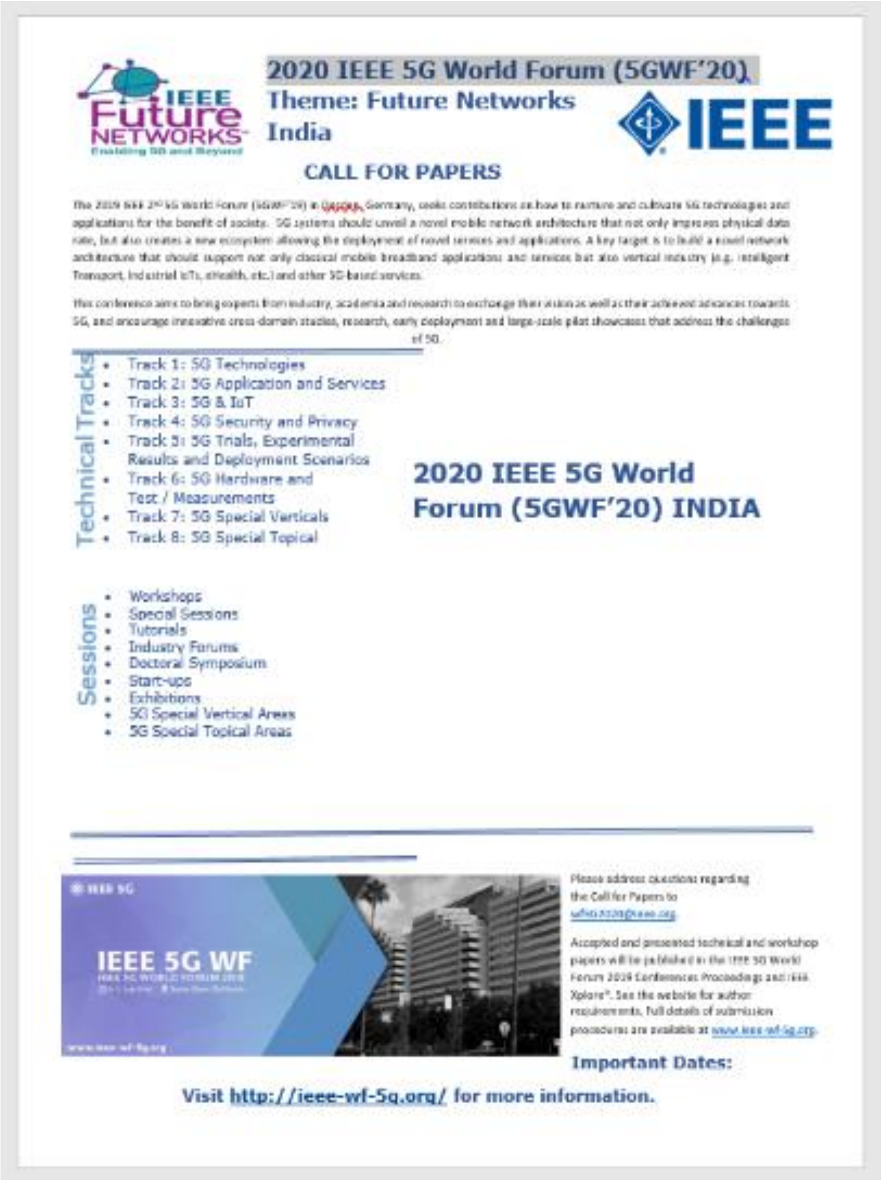
General Co-Chairs
Ashutosh Dutta, Johns Hopkins University/Applied Physics Lab
Gerhard Fettweis, Technical University of Dresden
Frank Fitzek, Technical University of Dresden
Latif Ladid, University of Luxembourg

Technical Program Committee
TPC Chair, Antonio Skarmeta, University of Murcia
TPC Co-Chairs:
Debabani Choudhury, Intel Labs
Debabani Choudhury, Intel
Athul Prasad, Nokia
Essaid Sabir, University of Casablanca

Important Dates:
April 15, 2019:
Technical papers
Industry Forum proposals
Tutorials proposals
Vertical/Topical Area proposals
May 15, 2019:
Workshop papers

Visit http://ieee-wf-5g.org/ for more information.

5G World Forum 2020, India



2020 IEEE 5G World Forum (5GWF'20)
Theme: Future Networks
India

CALL FOR PAPERS

The 2019 IEEE 2nd 5G World Forum (5GWF'20) in [illegible], Germany, seeks contributions on how to nurture and cultivate 5G technologies and applications for the benefit of society. 5G systems should unveil a novel mobile network architecture that not only improves physical data rate, but also creates a new ecosystem allowing the deployment of novel services and applications. A key target is to build a novel network architecture that should support not only classical mobile broadband applications and services but also vertical industry (e.g. Intelligent Transport, Industrial IoTs, eHealth, etc.) and other 5G-based services.

This conference aims to bring experts from industry, academia and research to exchange their vision as well as their achieved advances towards 5G, and encourage innovative cross-domain studies, research, early deployment and large-scale pilot showcases that address the challenges of 5G.

Technical Tracks
- Track 1: 5G Technologies
- Track 2: 5G Application and Services
- Track 3: 5G & IoT
- Track 4: 5G Security and Privacy
- Track 5: 5G Trials, Experimental Results and Deployment Scenarios
- Track 6: 5G Hardware and Test / Measurements
- Track 7: 5G Special Verticals
- Track 8: 5G Special Topical

2020 IEEE 5G World Forum (5GWF'20) INDIA

Sessions
- Workshops
- Special Sessions
- Tutorials
- Industry Forums
- Doctoral Symposium
- Start-ups
- Exhibitions
- 5G Special Vertical Areas
- 5G Special Topical Areas

IEEE 5G WF

Please address questions regarding the Call for Papers to wf5g2020@ieee.org

Accepted and presented technical and workshop papers will be published in the IEEE 5G World Forum 2019 Conferences Proceedings and IEEE Xplore®. See the website for author requirements. Full details of submission procedures are available at www.ieee-wf-5g.org.

Important Dates:

Visit http://ieee-wf-5g.org/ for more information.

GLOBAL

IS

WHAT IS NEEDED

LOCALLY EVERYWHERE

More than 50 Summits
IEEE 5G Summit Series – 2015 - 2019 (www.5gsummit.org)

50+ 5G Summits, More than 7500 attendees (onsite and online), 600 Speakers, Streaming and Recording Archived

7
1-6
9
8
8
10
10

HAWAII

PRINCETON
TORONTO
MONTREAL
SANTA CLARA
AUSTIN
LAUREL
SEATTLE
RESTON
BOULDER
PHILADELPHIA
DALLAS
BRAZIL

TUNISIA
MOROCCO
CASABLANCA
ISTANBUL
PRETORIA

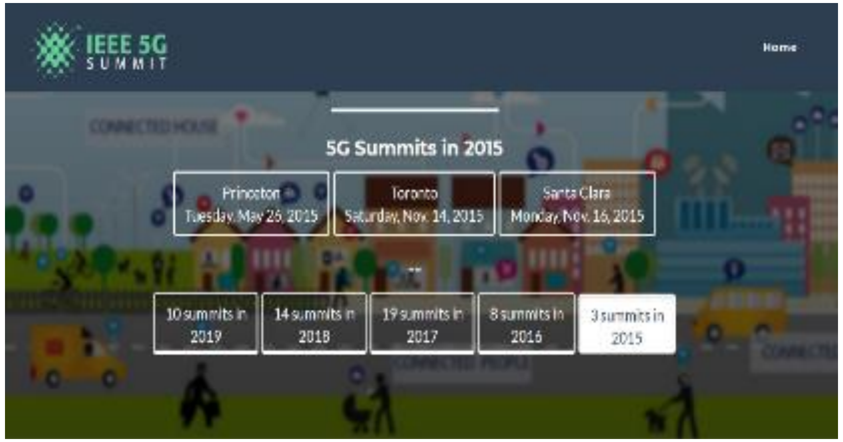
AALBORG
BERLIN
THESSOLONIKI
HELSINKI
TRENTO
LEVI

DRESDEN
LISBON

SHANGHAI
PATNA
TIANJIN
TOKYO
NANJING
TAIPEI
NEW DELHI
KOLKATA
BHUBANESWAR
TRIVANDRUM
CHENNAI

Number of Summits
2015 – 3
2016 – 8
2017 – 19
2018 – 14
2019– 12+ (Planning underway)
Soliciting other chapters

5G Summits at a Glance 5gsummit.org



5G Summits in 2015

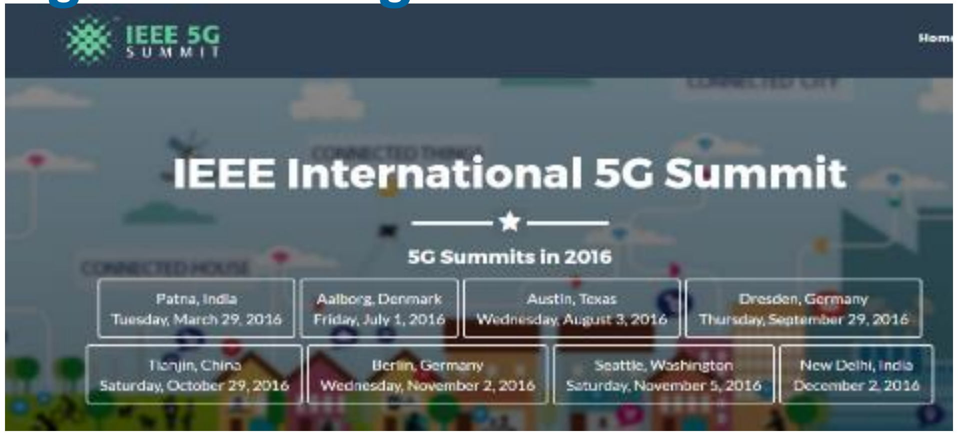
Princeton
Tuesday, May 26, 2015

Toronto
Saturday, Nov. 14, 2015

Santa Clara
Monday, Nov. 16, 2015

10 summits in 2019
14 summits in 2018
19 summits in 2017
8 summits in 2016
3 summits in 2015

3 IEEE 5G Summits in 2015



IEEE International 5G Summit

5G Summits in 2016

Patna, India
Tuesday, March 29, 2016

Aalborg, Denmark
Friday, July 1, 2016

Austin, Texas
Wednesday, August 3, 2016

Dresden, Germany
Thursday, September 29, 2016

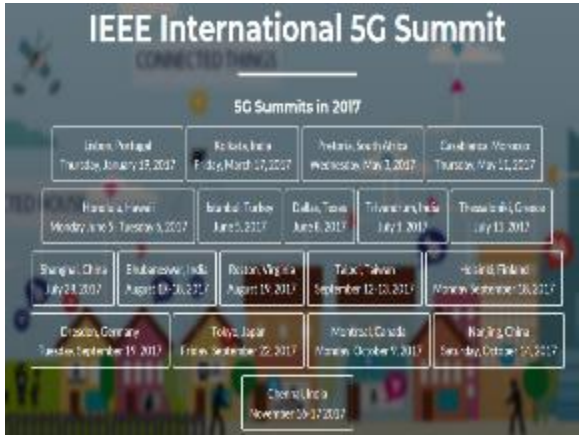
Tianjin, China
Saturday, October 29, 2016

Berlin, Germany
Wednesday, November 2, 2016

Seattle, Washington
Saturday, November 5, 2016

New Delhi, India
December 2, 2016

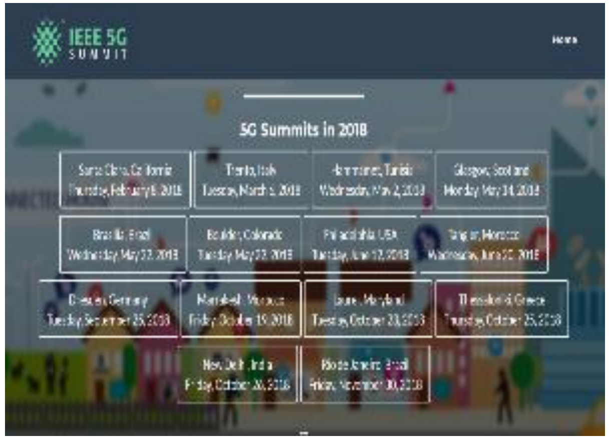
8 IEEE 5G Summits in 2016



IEEE International 5G Summit

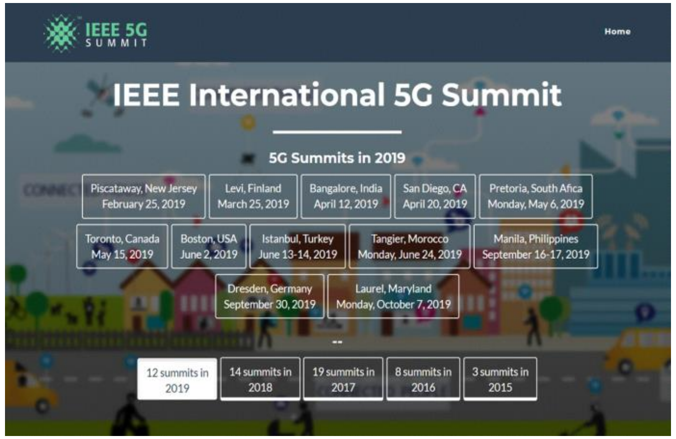
5G Summits in 2017

19 IEEE 5G Summits in 2017



5G Summits in 2018

14 IEEE 5G Summits in 2018



IEEE International 5G Summit

5G Summits in 2019

Piscataway, New Jersey
February 25, 2019

Levi, Finland
March 25, 2019

Bangalore, India
April 12, 2019

San Diego, CA
April 20, 2019

Pretoria, South Afica
Monday, May 6, 2019

Toronto, Canada
May 15, 2019

Boston, USA
June 2, 2019

Istanbul, Turkey
June 13-14, 2019

Tangier, Morocco
Monday, June 24, 2019

Manila, Philippines
September 16-17, 2019

Dresden, Germany
September 30, 2019

Laurel, Maryland
Monday, October 7, 2019

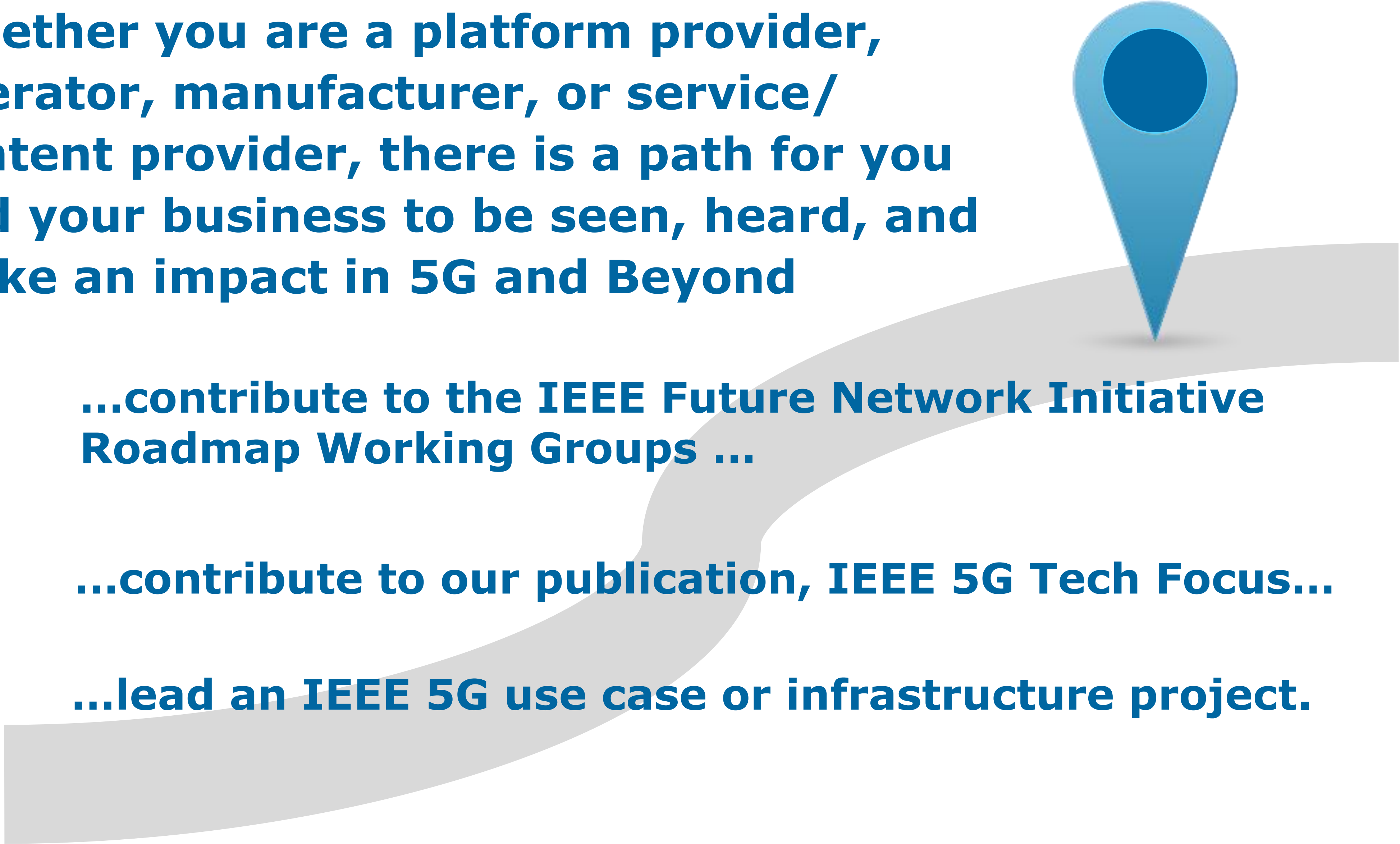
--

12 summits in 2019
14 summits in 2018
19 summits in 2017
8 summits in 2016
3 summits in 2015

12 IEEE 5G Summits Planned in 2019

IEEE
Advancing Technology for Humanity

Whether you are a platform provider, operator, manufacturer, or service/content provider, there is a path for you and your business to be seen, heard, and make an impact in 5G and Beyond



…contribute to the IEEE Future Network Initiative Roadmap Working Groups …

…contribute to our publication, IEEE 5G Tech Focus…

…lead an IEEE 5G use case or infrastructure project.

THANK YOU

and

JOIN US FOR THE INNOVATION REVOLUTION

LEARN MORE AT
5G.IEEE.ORG

Backup Slides

Attack Types in NFV (Ref- ETSI/NFV)

Threat 1: Attack from VMs in the same domain

- VM would be manipulated by attackers and potentially extend the attack to other VMs
- Buffer overflow, DOS, ARP, Hypervisor, vswitch

Threat 2: Attack to host, hypervisor and VMs from applications in host machine

- Poor design of hypervisors, improper configuration
- Attackers inject malicious software to virtual memory and control VM
- Malformed packet attacks to hypervisors

Threat 3: Attack from host applications communicating with VMs

- Host applications being attacked can initiate monitoring, tampering or DOS attack to communications going through host vSwitch
- Improper network isolation, Improper configuration to application privileges of host machine
- Lack of restriction to services or application

Attack Types in NFV (Ref-ETSI/NFV)(Contd.)

Threat 4: Attack to VMs from remote management path

- Outside attackers could initiate communication by eavesdropping, tampering, DOS attack, and Man-in-the-Middle attack
- Gain illegal access of the system and access OS without authorization, tamper and obtain sensitive and important information of a system
- Poor design and development of the application may lead to many known attacks (e.g., buffer overflow attacks)

Threat 5: Attack to external communication with 3rd party applications

- The API interface accessed by 3rd party applications in the untrusted domains is easily subject to malicious attack. Such attack includes illegal access to API, DOS attack to API platform
- Logical bugs in APIs, API authentication/authorization mechanism problems and security policy configuration problems.

Threat 6: Attack from external network via network edge node

- Virtualized Firewalls, Residential gateways

Threat 7: Attack from host machines or VMs of external network domain

- VNF migration, VNF scaling (Scale in- Scale out)

Hypervisor Vulnerability (Example)

Use Case: Hypervisor gets compromised somehow by the attacker. Attacker uses hypervisor privilege to install kernel root kit in VNF's OS and thereby controls and modifies the VNF.

Mitigation Techniques:

- Hypervisor Introspection schemes can use the Hypervisor's higher privilege to secure the guest VMs.
- A Hypervisor-based introspection scheme can detect guest OS rootkit that got installed by the attacker.
- Adoption of Hypervisor hardening mechanisms can protect hypervisor's code and data from unauthorized modification and can guard against bugs and misconfigurations in the hardened hypervisors.
- Use Software vulnerability management procedure to make sure the hypervisor is secured from attack

Orchestration Vulnerability (Example)

Use Case: An attacker uses legitimate access to the orchestrator and manipulates its configuration in order to run a modified VNF or alter the behavior of the VNF through changing its configuration through the orchestrator. This will compromise the VNF separation as the administrator of one VNF can get admin privilege of another VNF and the separation between the VNFs cannot be maintained.

Mitigation Techniques:

- Deploy some of the inherent best current practices for orchestration security by way of detection mechanism when the separation is violated, provide secure logging for access, automated system or configuration auditing.
- Deploy security monitoring system that will detect the compromised VNF separation, any kind of anomaly in the system or provide alert mechanism when some critical configuration data in the orchestrator is altered.
- Access Control, File system protection, system integrity protection
- Hardening of separation policy through proper configuration management