IEEE Future Networks Webinar

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 Distinguished Lecturer
Email: ashutosh.dutta@ieee.org; Ashutosh.Dutta@jhuapl.edu
03/26/2019

Talk Outline

- Drivers for SDN/NFV and 5G
- 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

Part II: IEEE Future Networks Initiative Overview

Parts of this presentation have been discussed in various ETSI/NFV and IEEE Security and SDN/NFV Working Groups

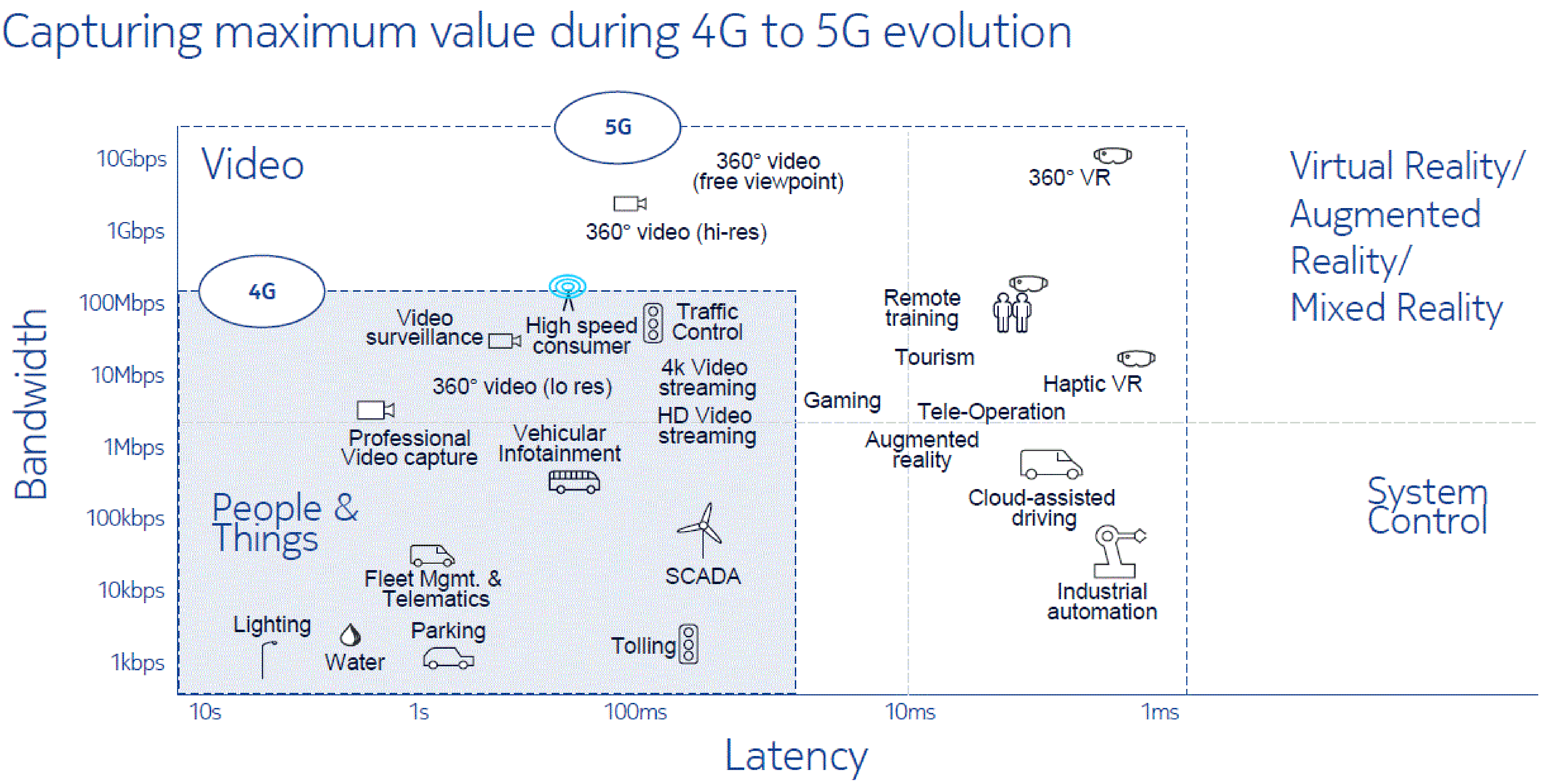
IEEE

Emerging Services and Applications

A Driver for Network Evolution

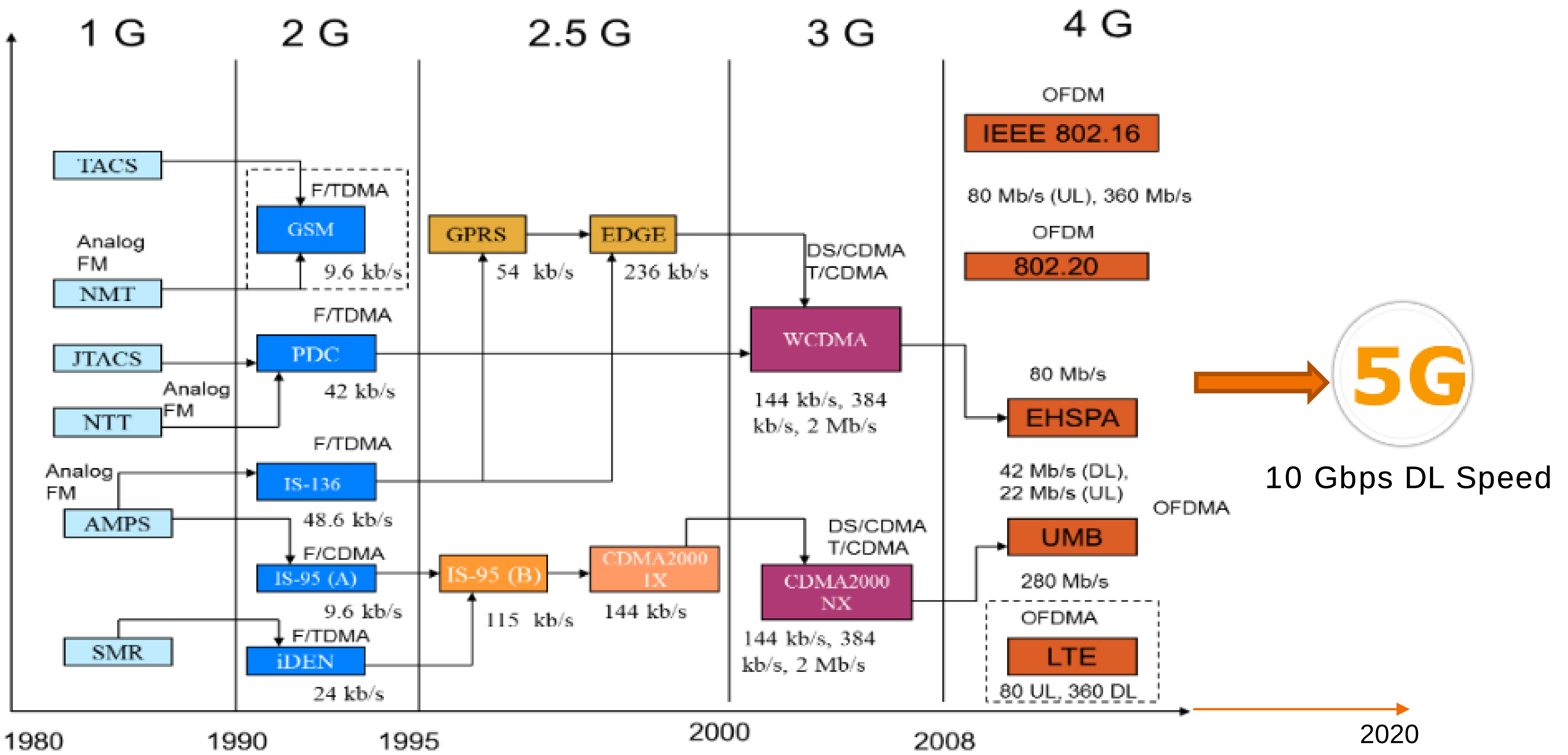
Smart Workplace
Asset Tracking
Internet of Things
Security
WebTV
Video
Smart Meter
Digital Content
Smart City
Robotics
Mobilize Everything
Semantic Web
Big Data
SmartGrid
Augmented Reality
M2M
Digital Learning
Sensor Network
Wearable Computing
BYOD
Voice Recognition
Digital Life
Virtualization
Gesture 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

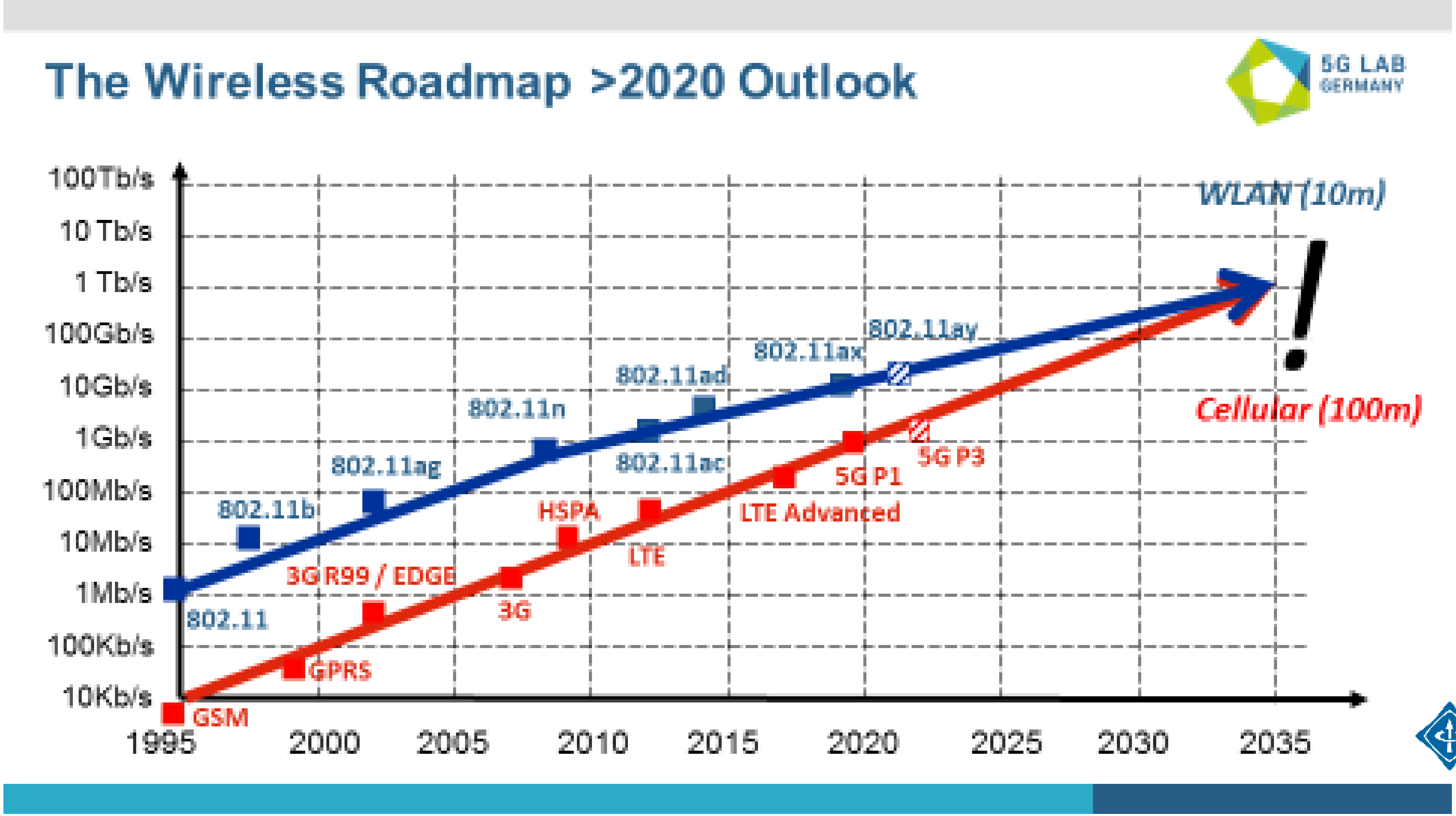


Source Nokia

Evolution of wireless access technologies



Co-existence of IEEE and 3GPP Technologies

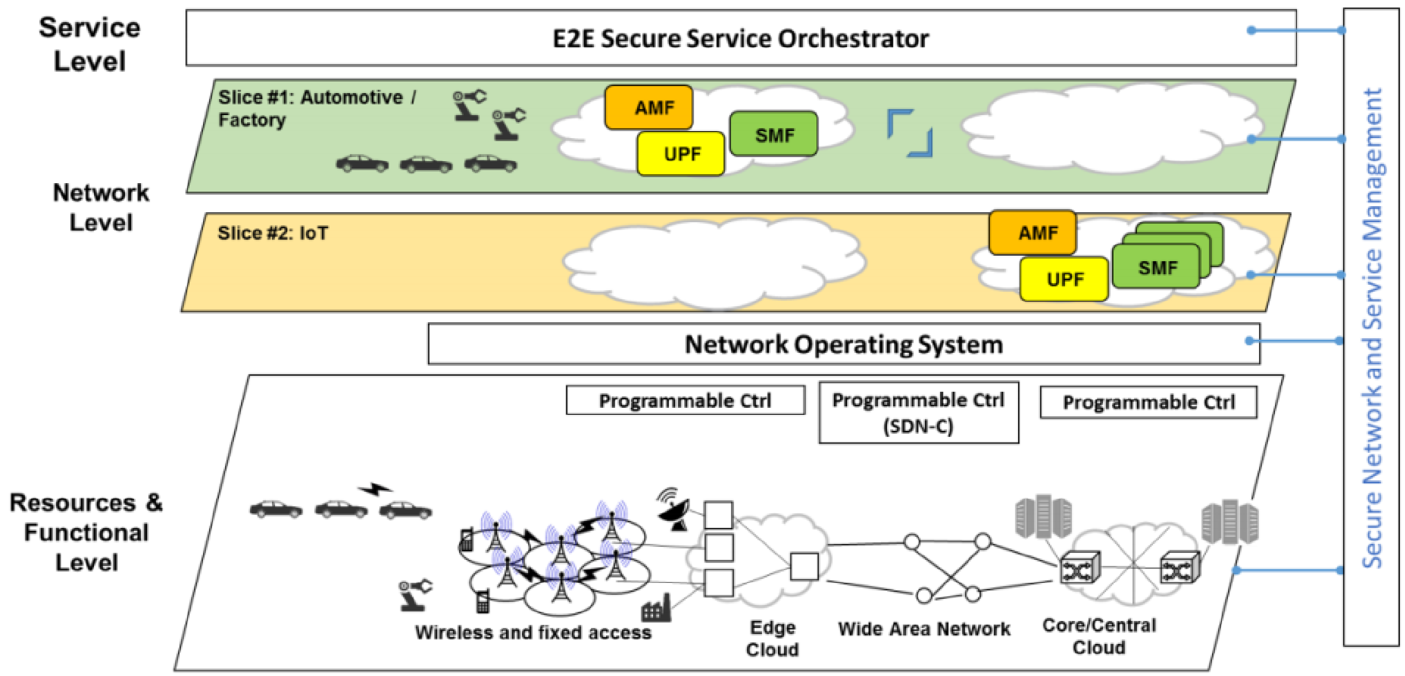


Key Characteristics of 5G

- 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



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

Critical Communications

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

Massive Machine Type Communications

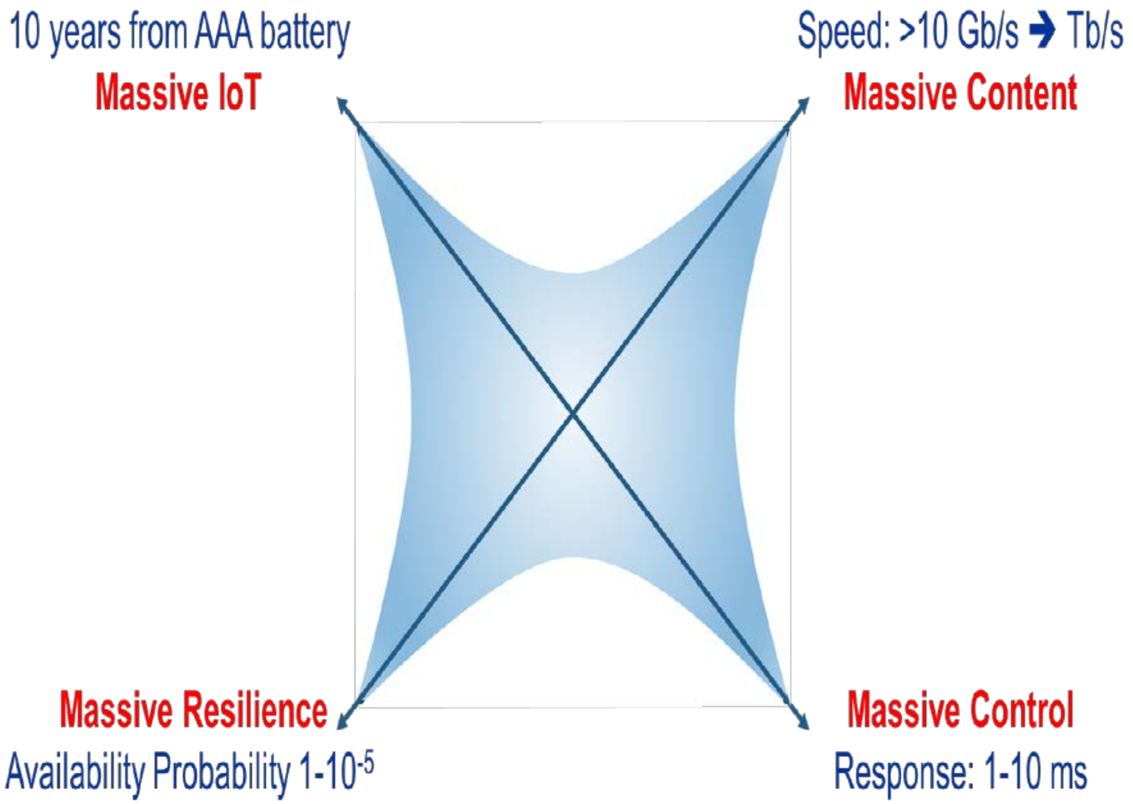
- Subway / Stadium Service, eHealth, Wearables, Inventory Control

Network Operation

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

Enhancement of Vehicle-to-Everything

- Autonomous Driving, safety and non-safety features

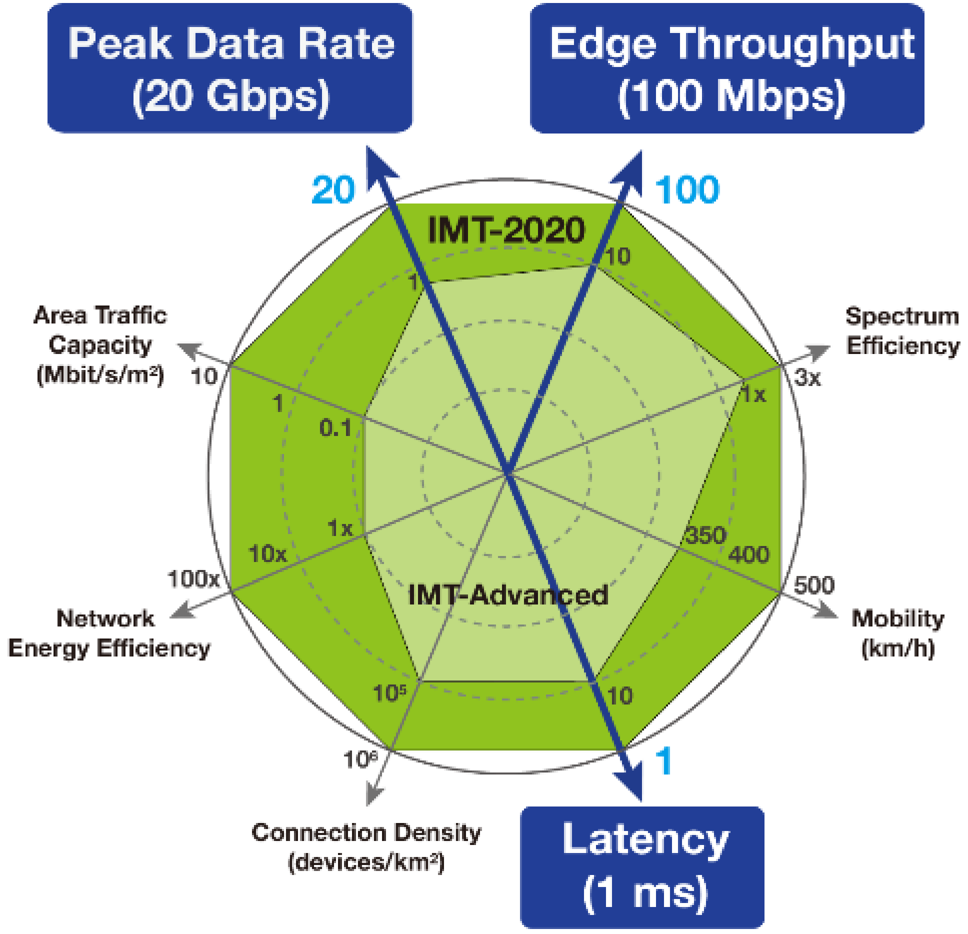


Courtesy: Gerhard Fettweis

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.)

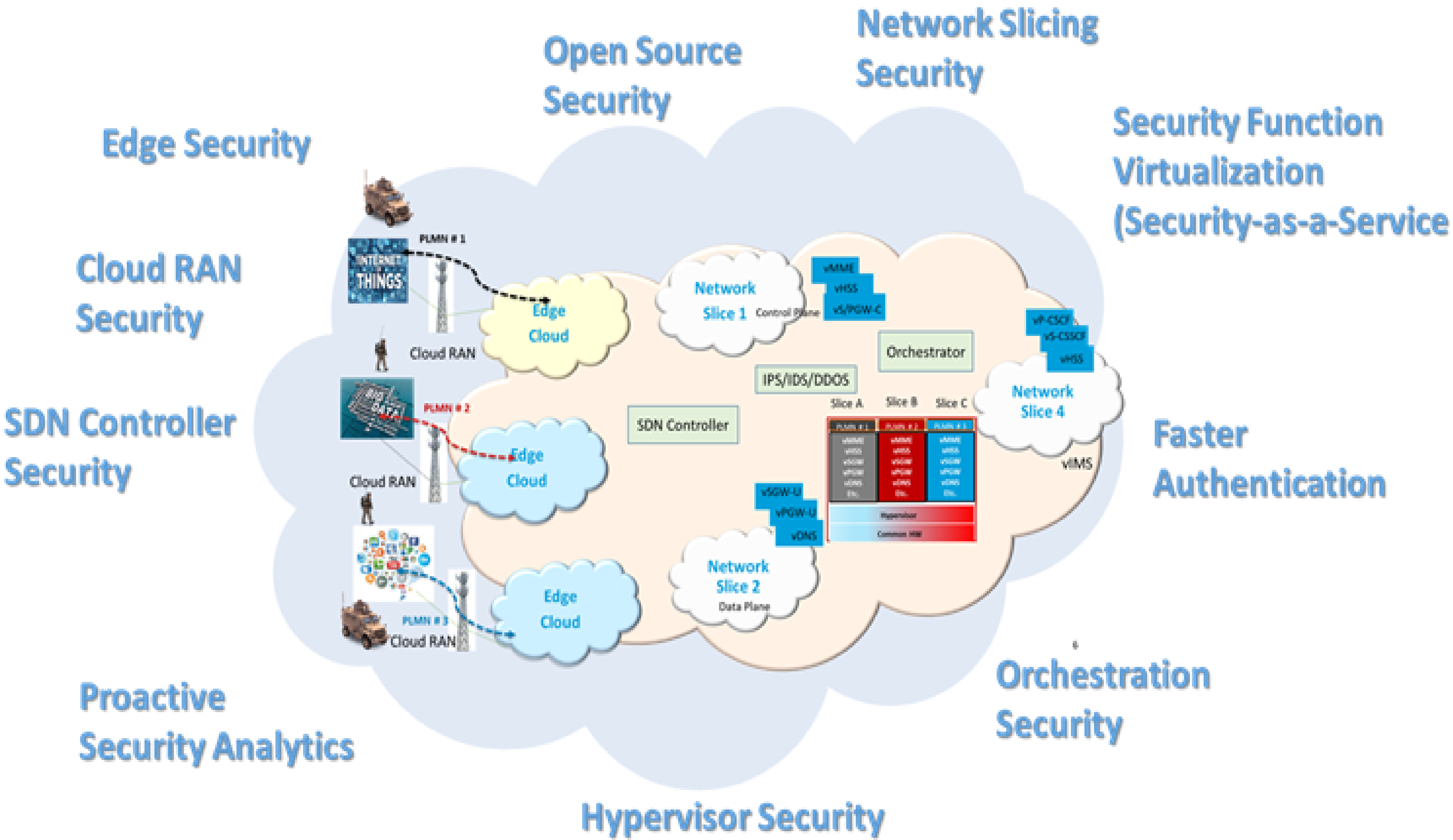
- High reliability / low latency
  - Industrial control
  - Remote manipulation
  - Mission-critical applications e.g. ehealth, hazardous environments, rescue missions, etc.
  - Self-driving vehicles



Source: ITU-R

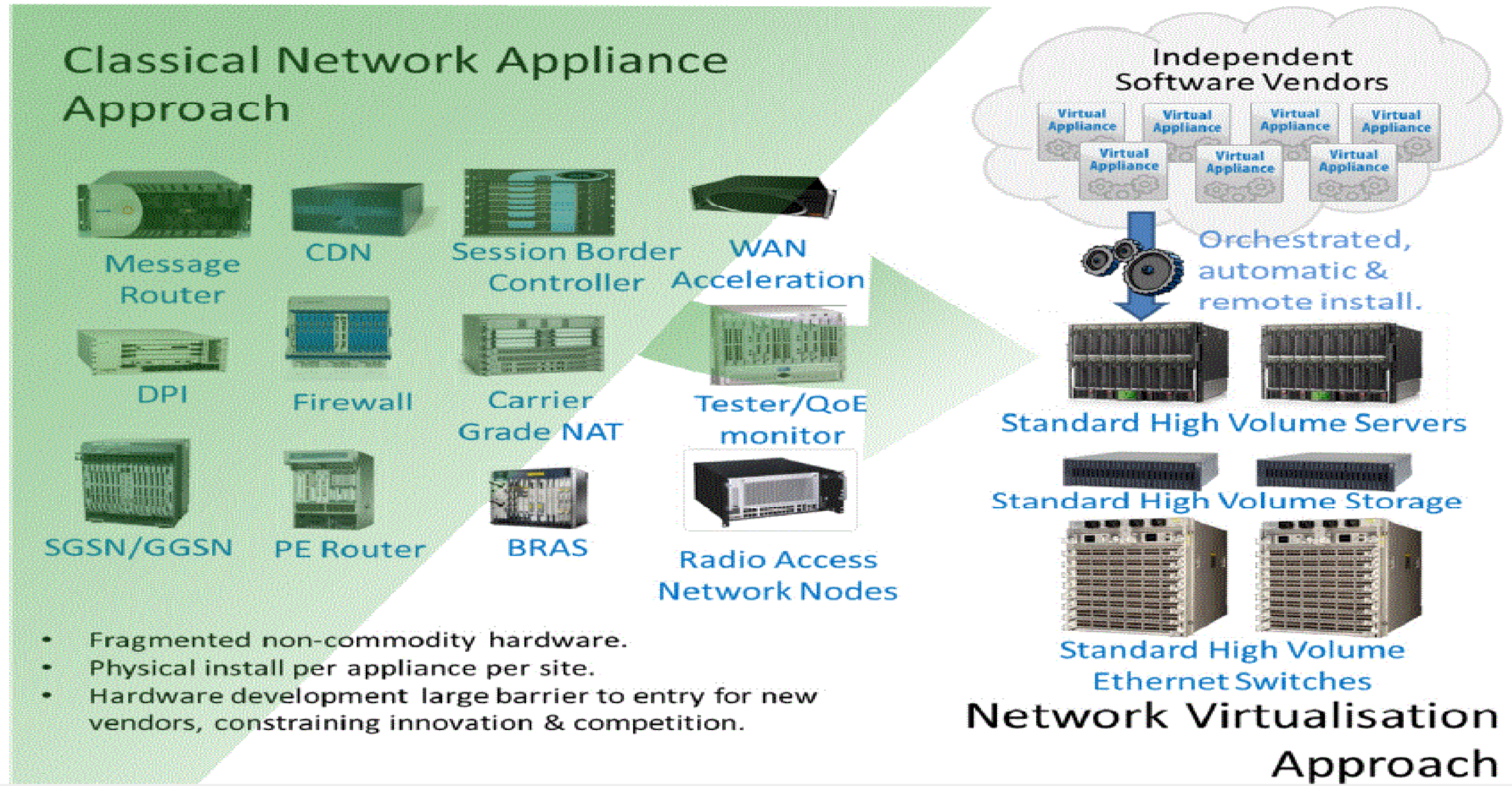
What “5G and Advanced Communication Systems” is About

Key Pillars of SDN/NFV and 5G Security

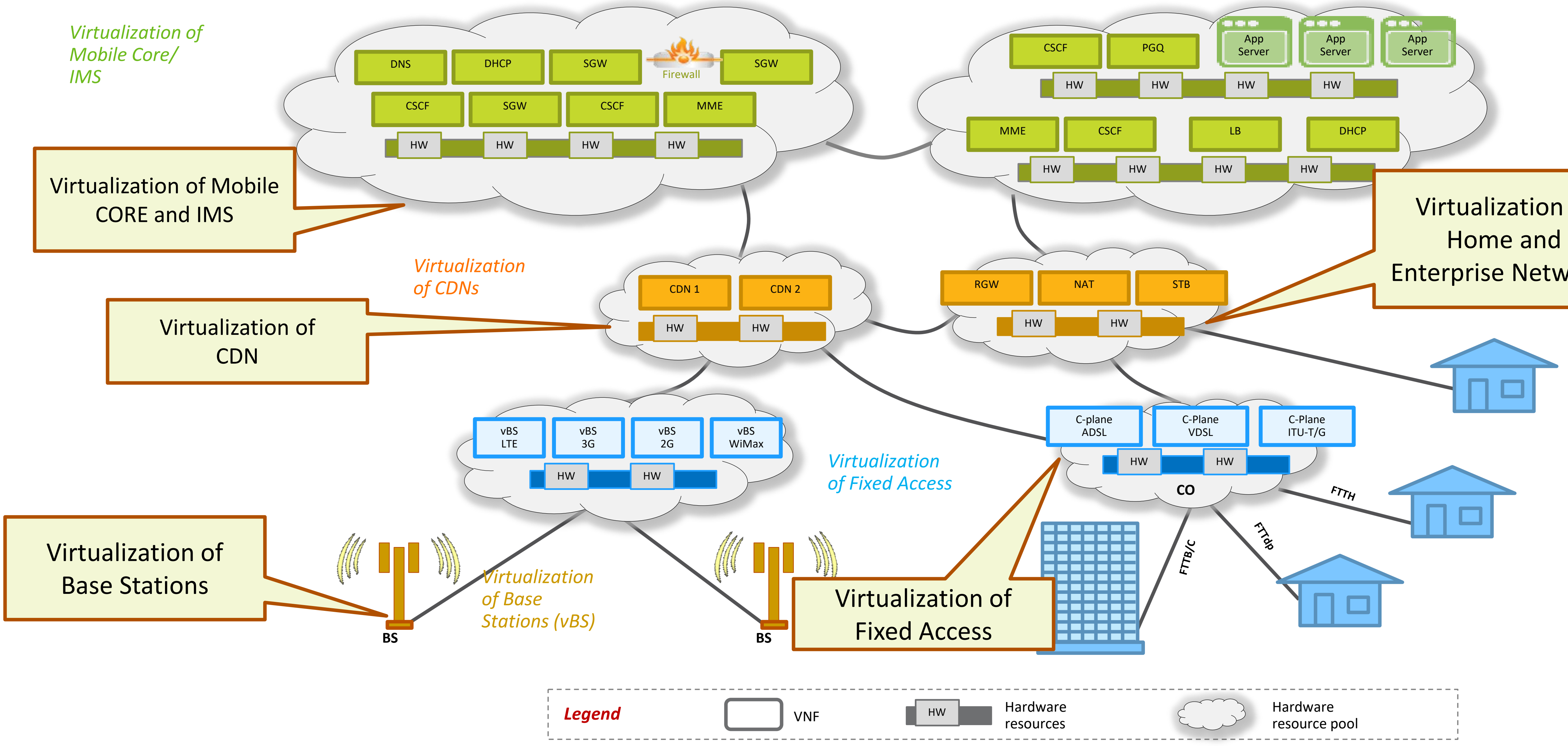


March 26, 2019

SDN/NFV is the Foundation of 5G Core Network



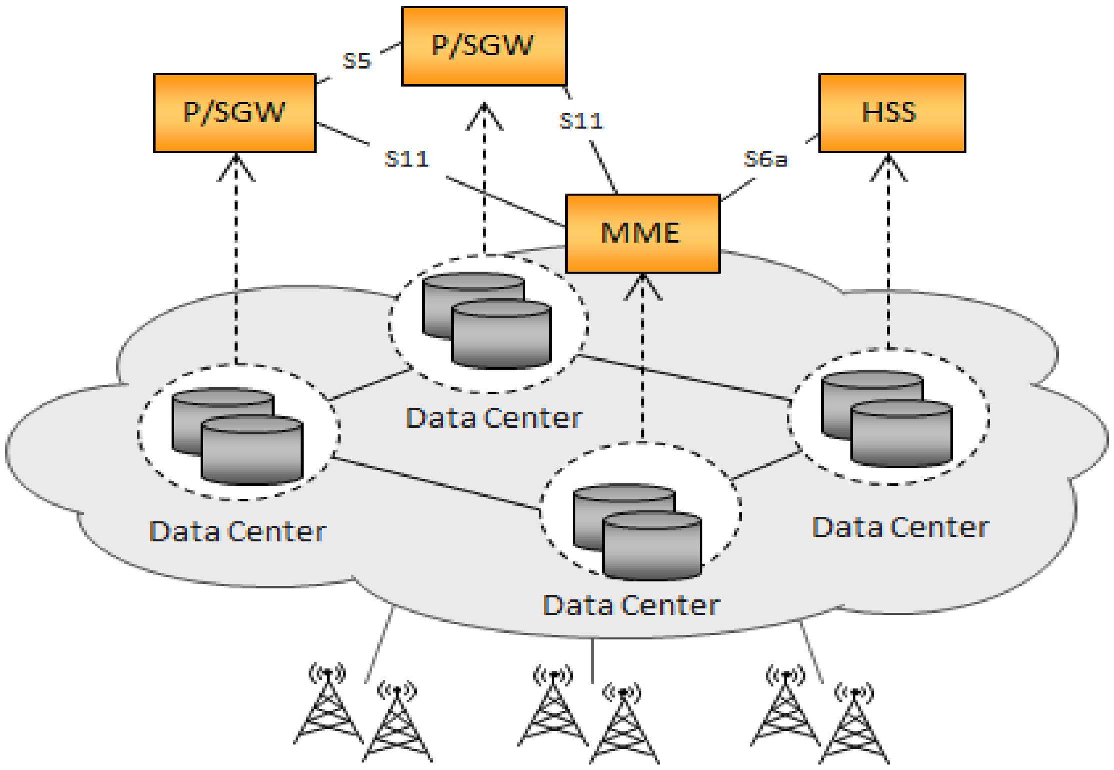
Overview of NFV (Network Function Virtualization) Sample Use cases

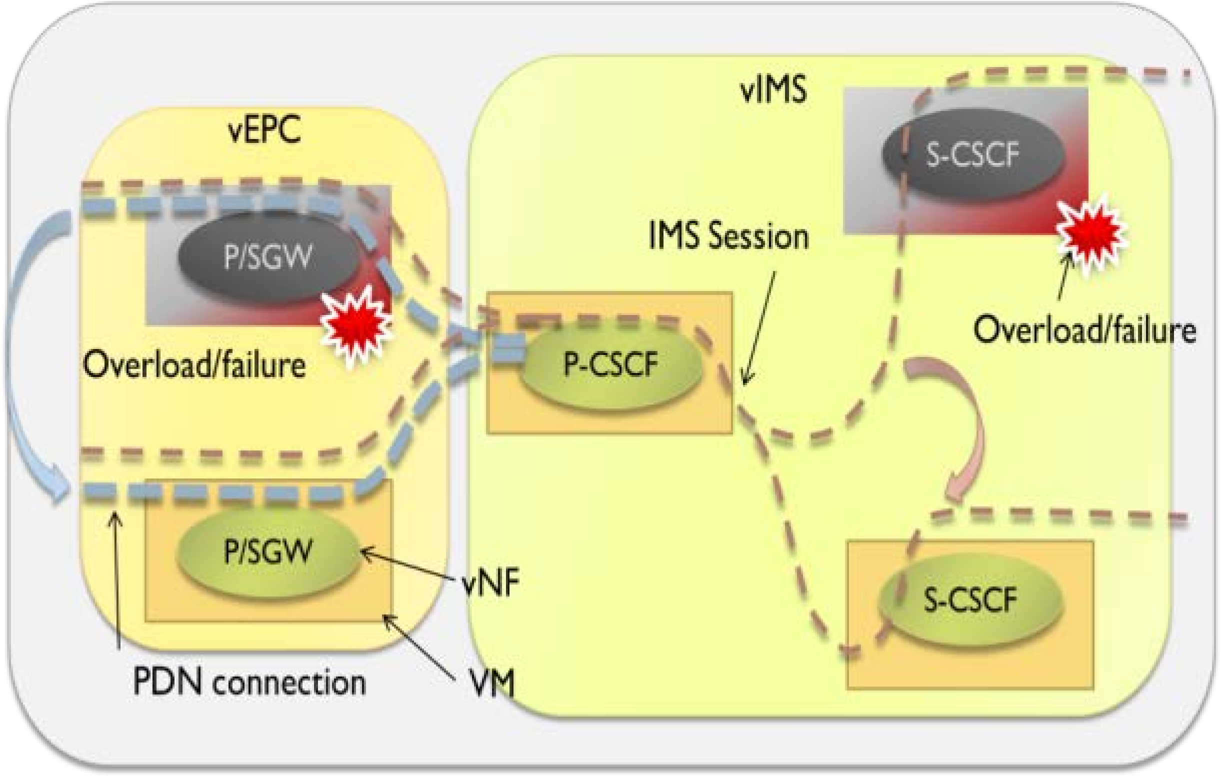


IEEE

NFV Use Case: Virtualization of Mobile Core Network (EPC) and IMS

Network Operation





VNF Relocation

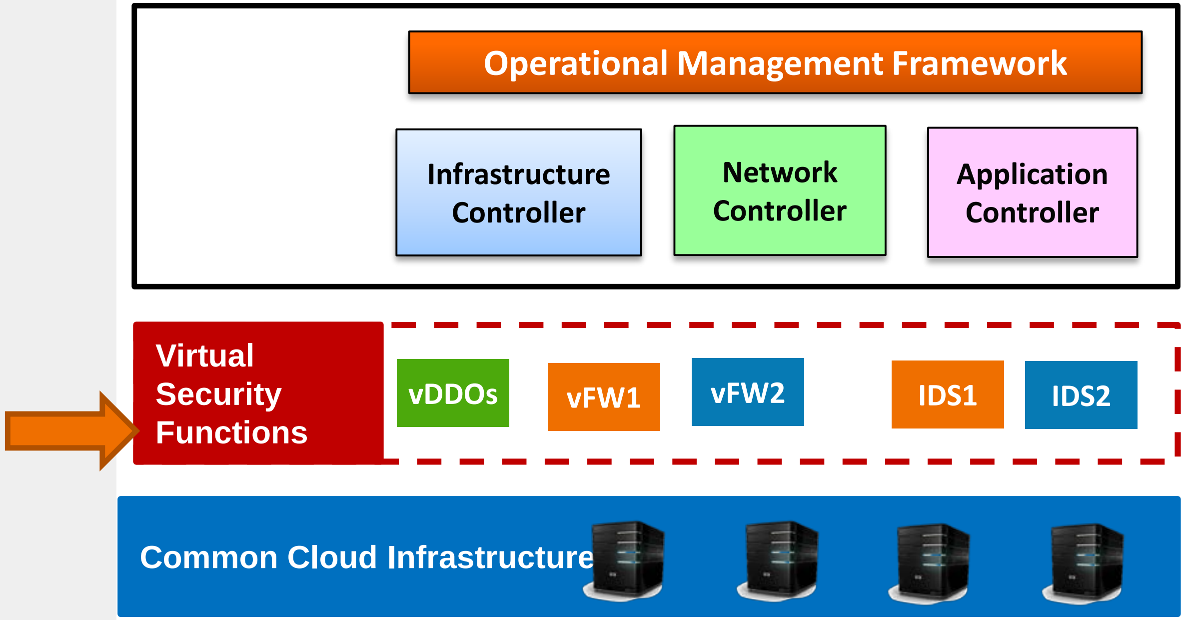
An Example - Security Transformation – Virtual Firewall/Virtual DDOS/Virtual IPS

Non-Virtualized Security

Intel Security
GUAVUS
Tektronix
HP
f5
ARBOR NETWORKS
NETSCOUT
ALLOT
Check Point
A10 NETWORKS
NIKSUN
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

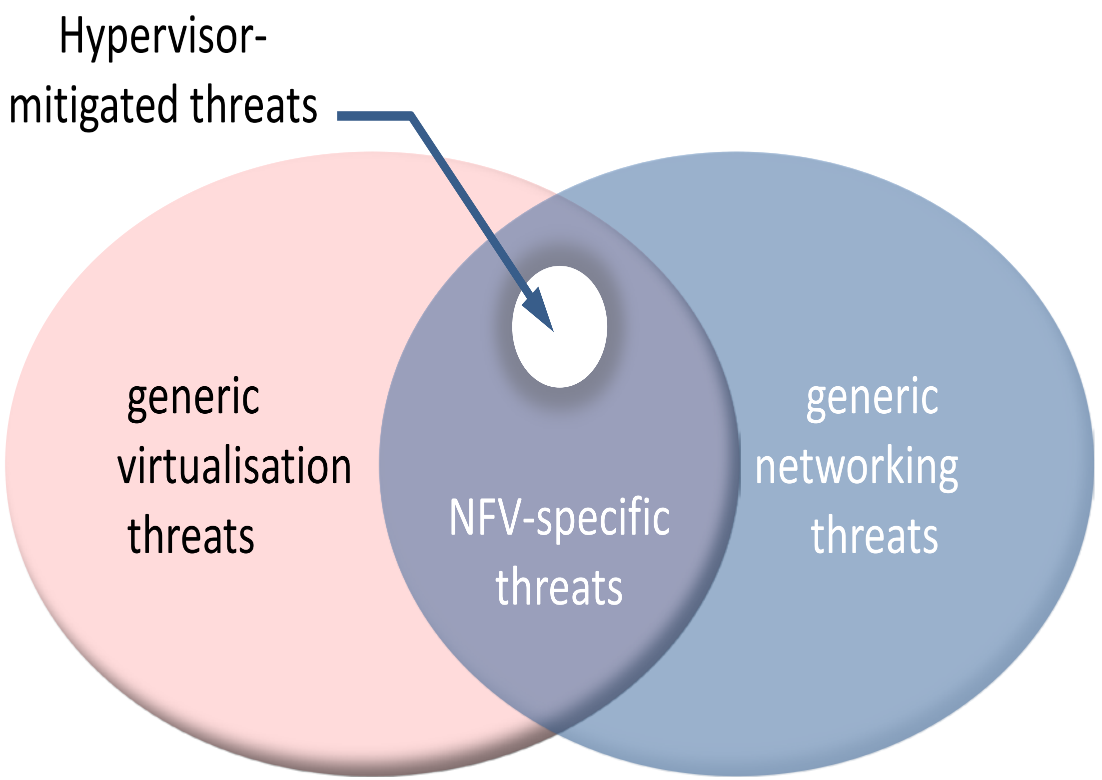


- Security functions will be cloud-based
- Security dynamically orchestrated in the cloud as needed
- Streamlined supplier integration
- Centralized common management platform
- Creates a standard operations/support model

IEEE

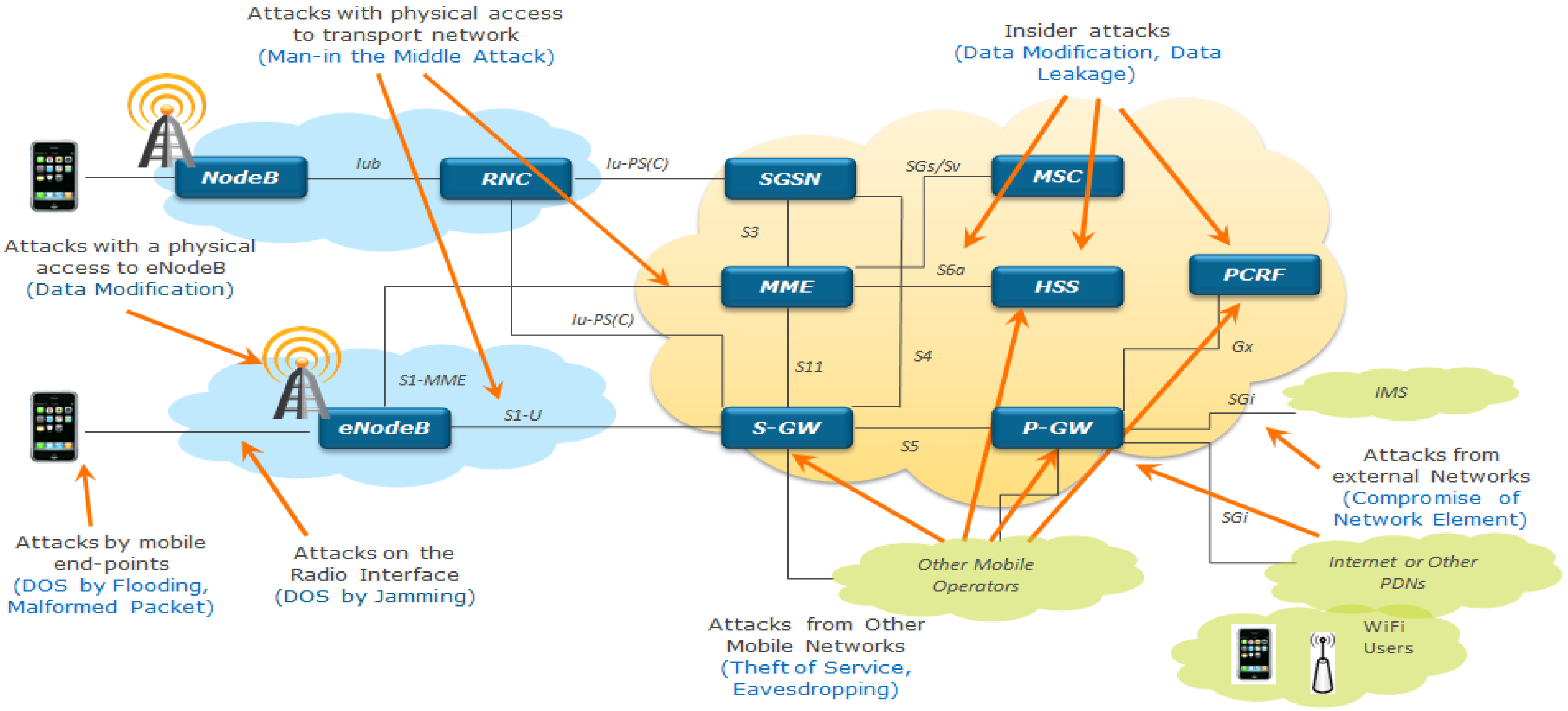
Security Challenges in a Virtual Environment – ETSI Problem Statement Draft

- 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)



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

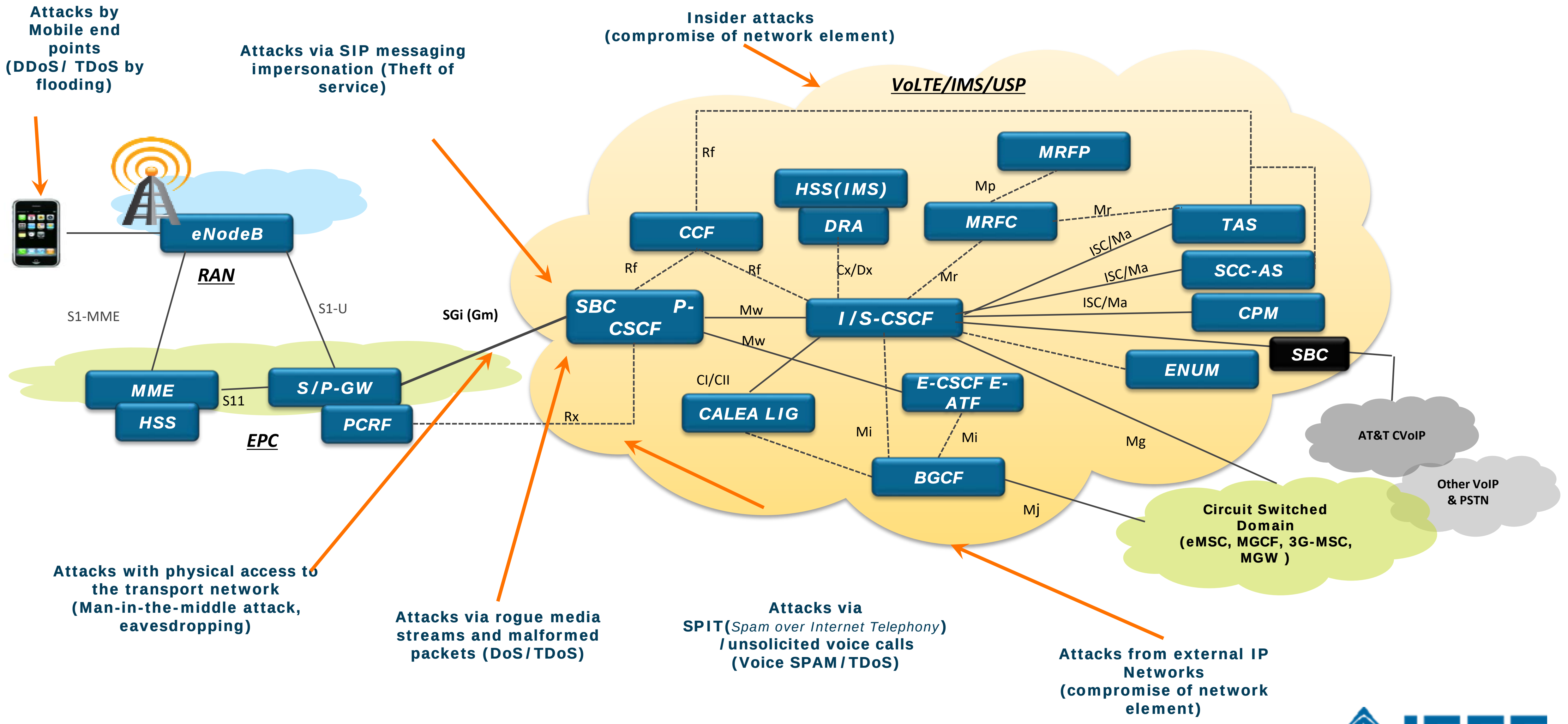
LTE/EPC Security Threats Categories



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

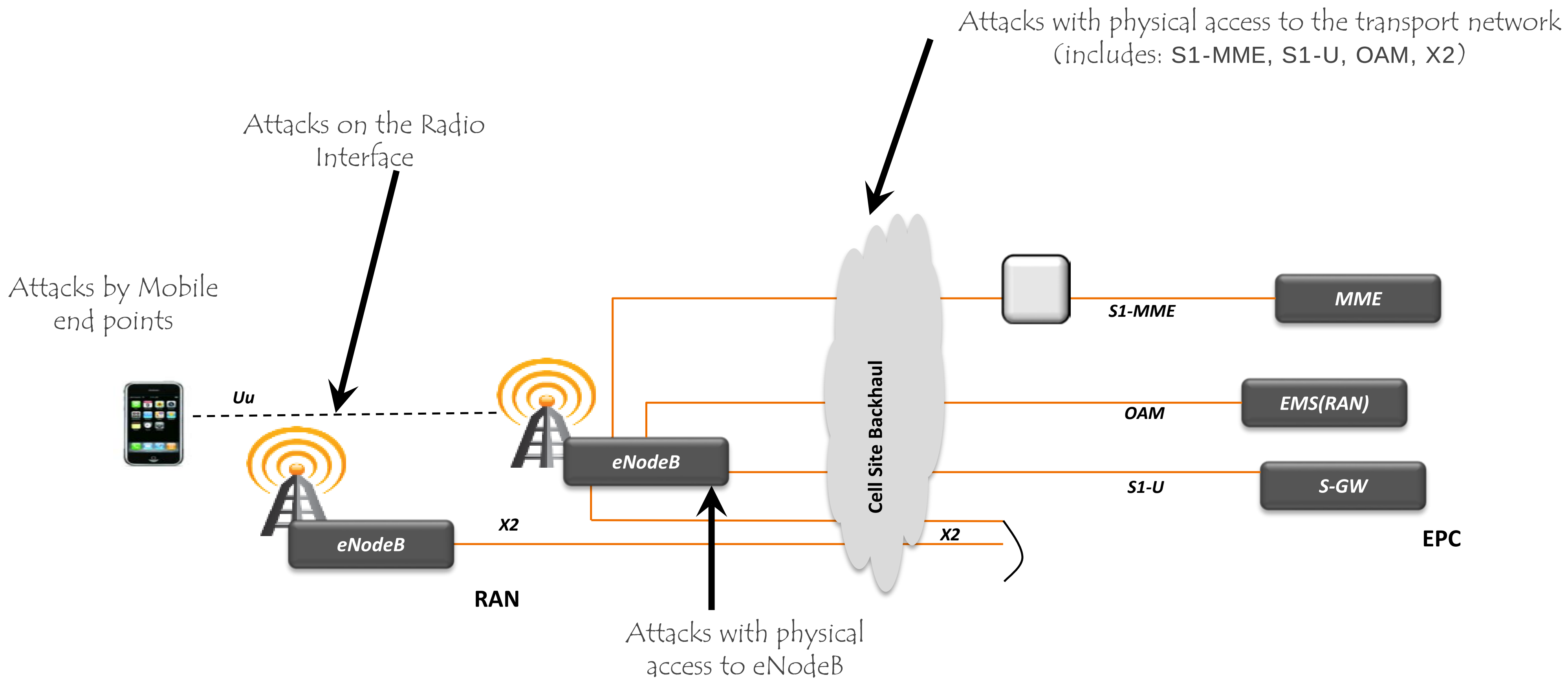


IMS Threat Categories

	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

IEEE

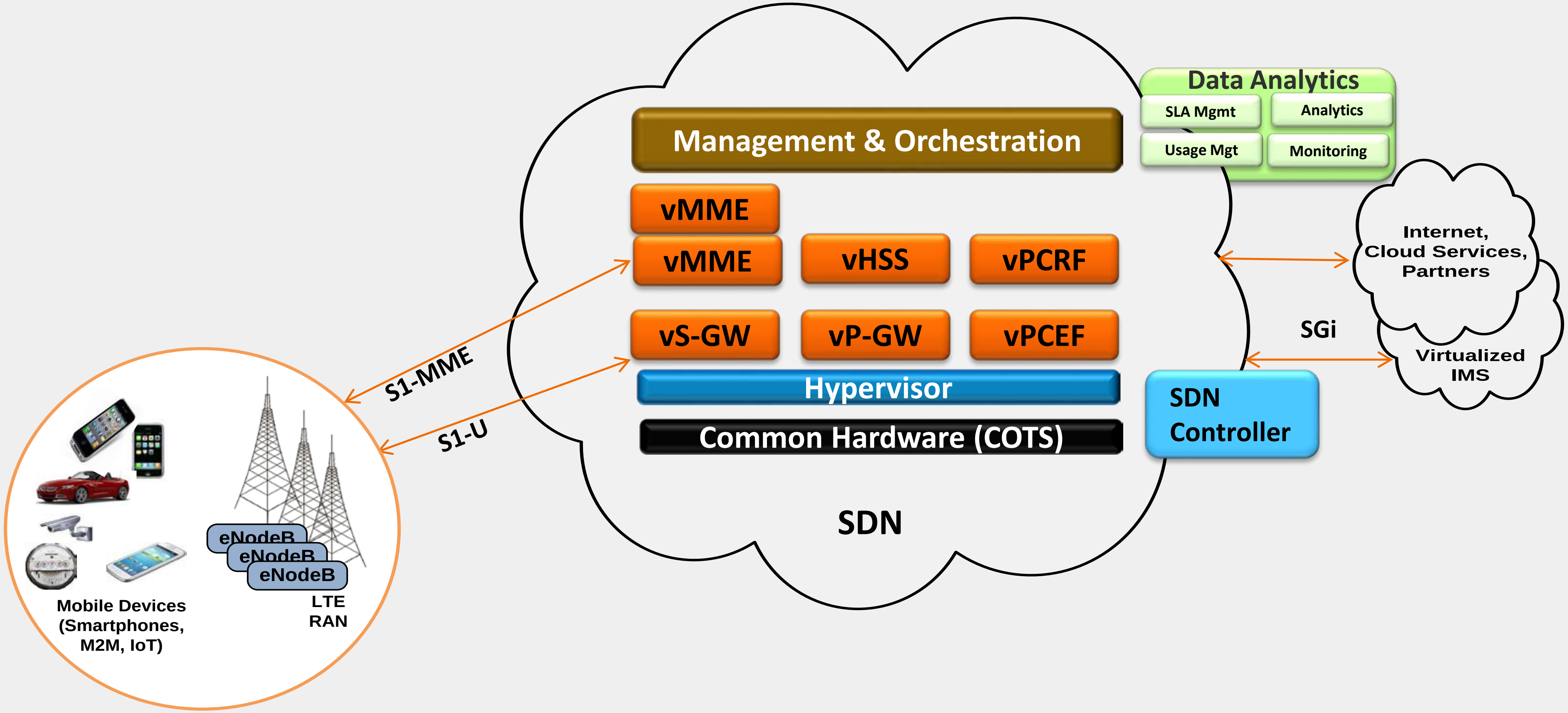
Attacks on LTE-RAN



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

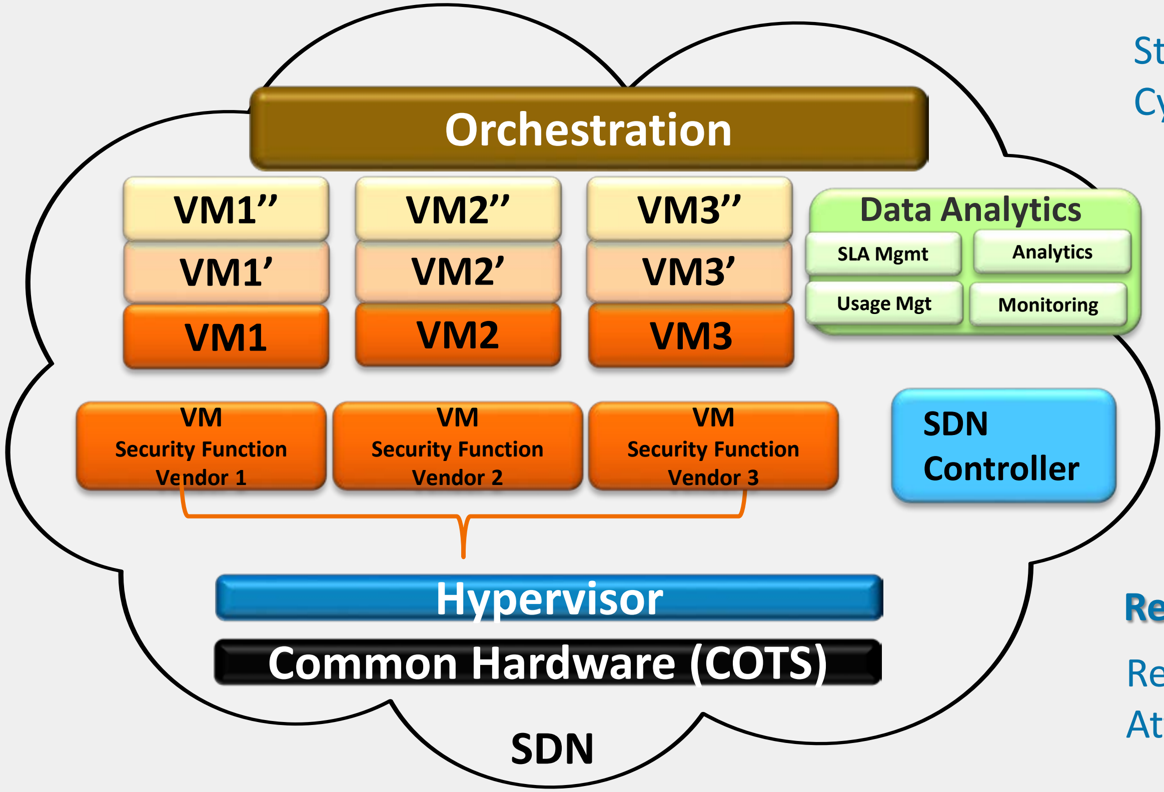
Design Enhancements:

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

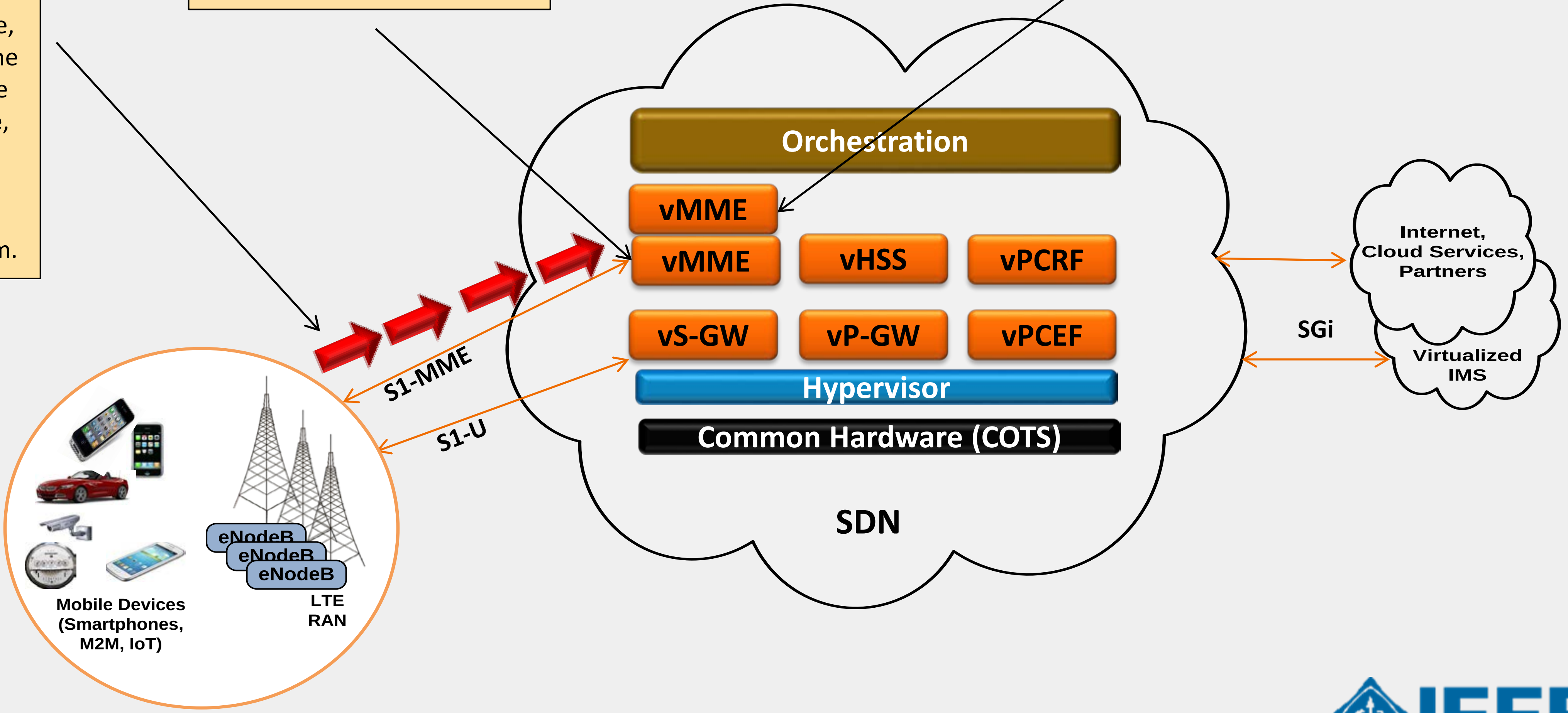
Security Opportunities from Virtualization

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.

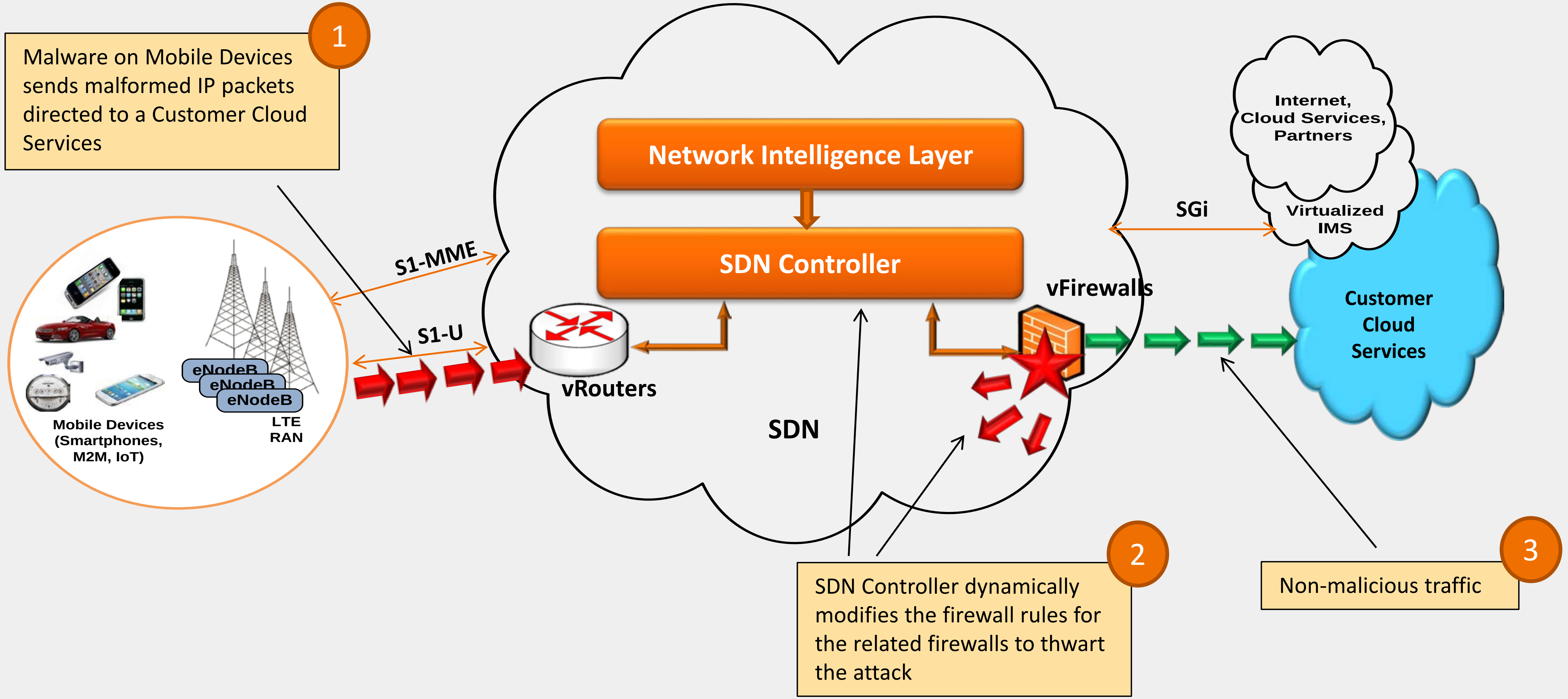
2 vMME is under DDoS attack

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



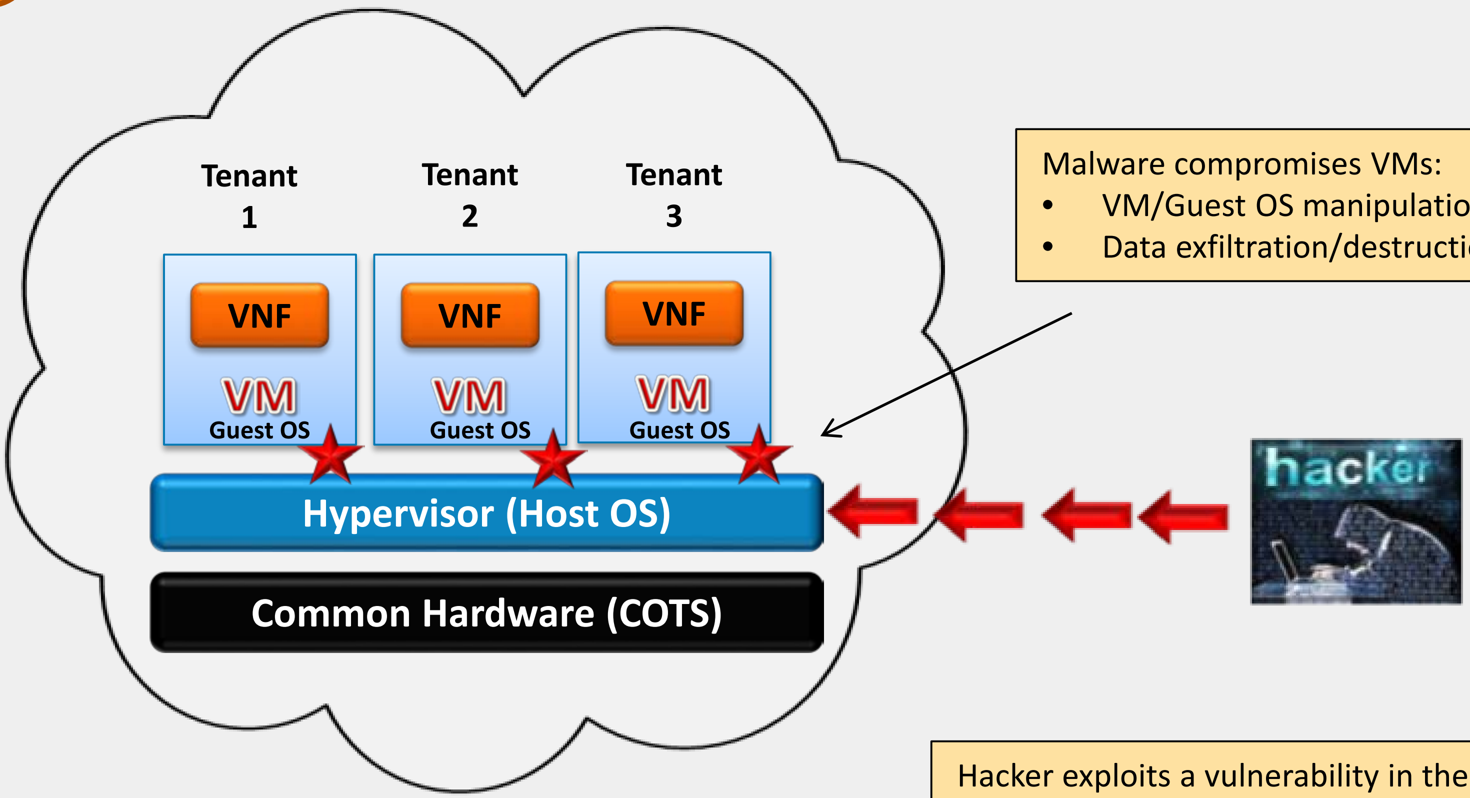
Security Challenges from Virtualization

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

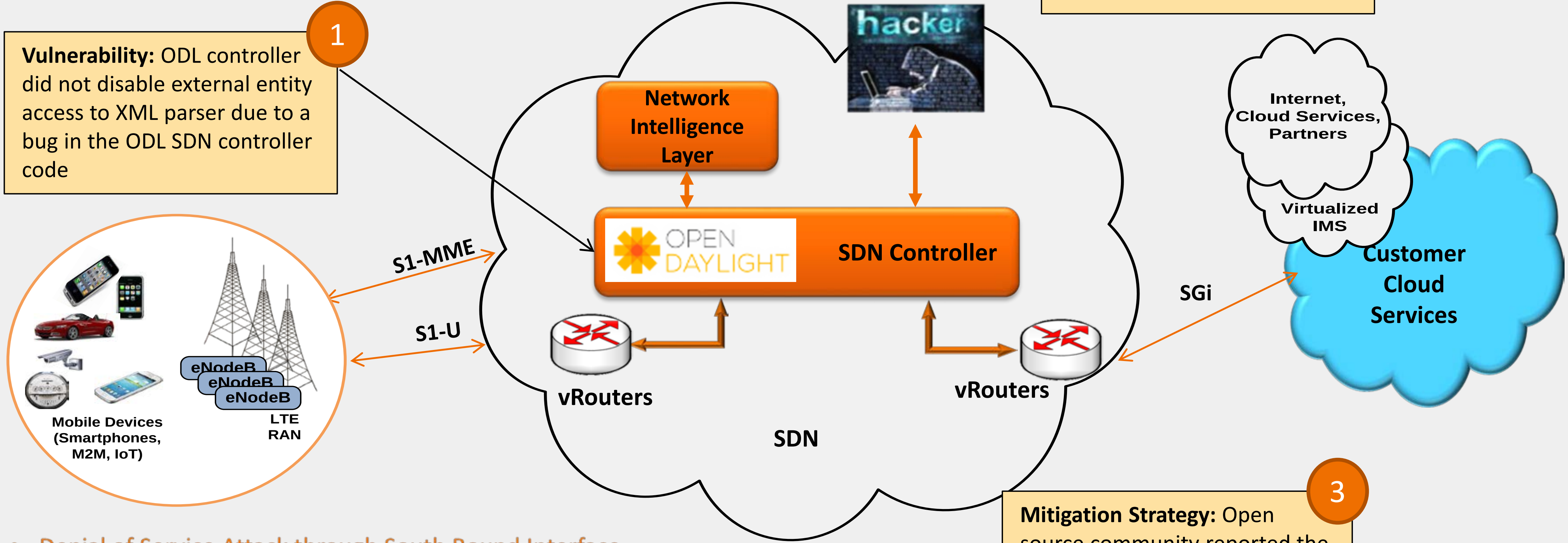
1

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



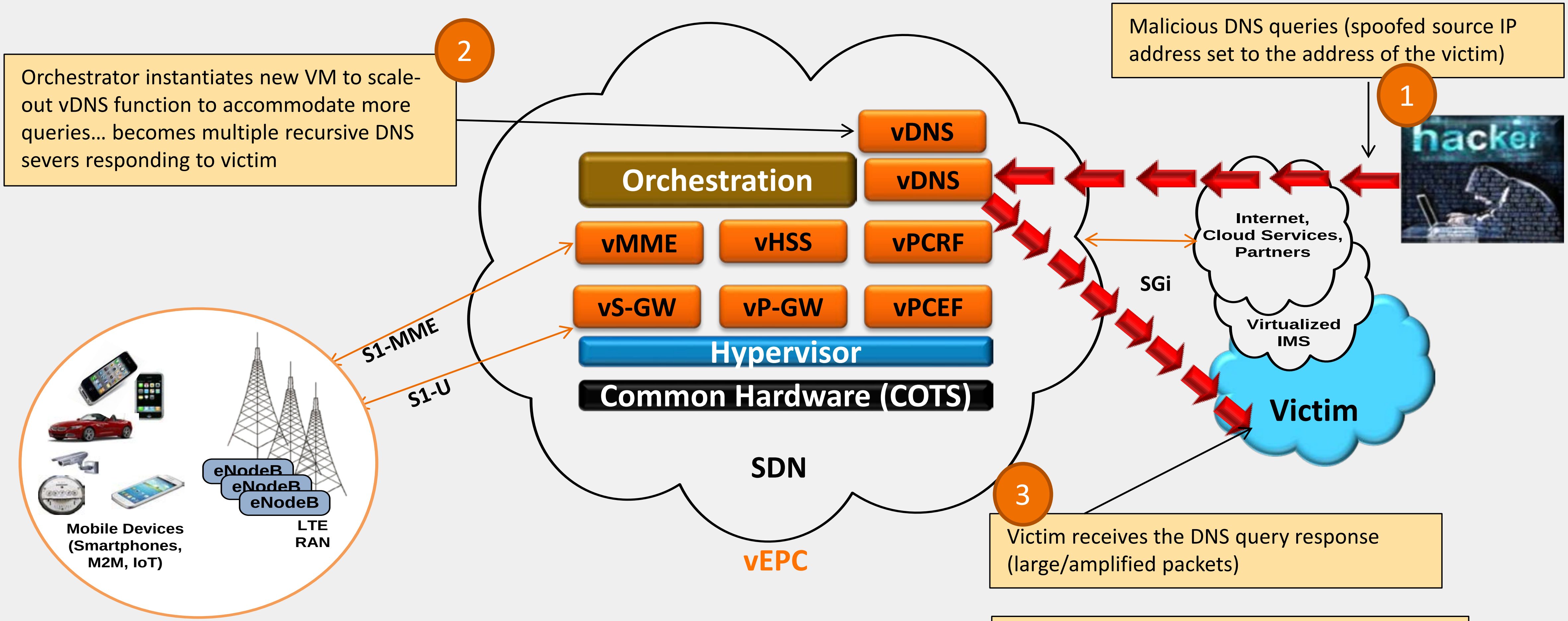
3 **Mitigation Strategy:** Open source community reported the problem, Patch was applied that disabled external entity access and fixed the problem.

- 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

SDN Controller Security Use Cases

- 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

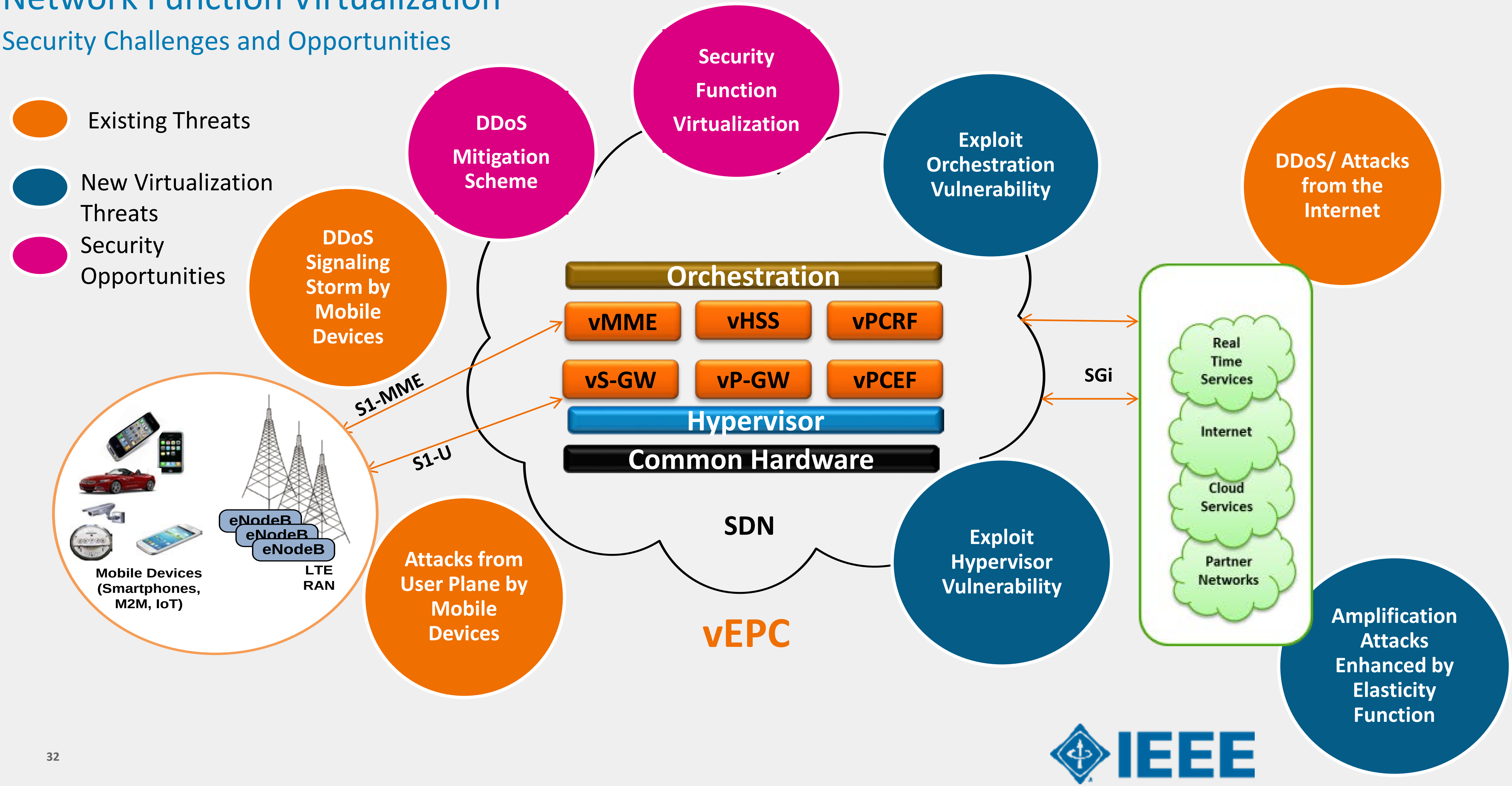
DNS Amplification Attacks Enhanced by Elasticity Function



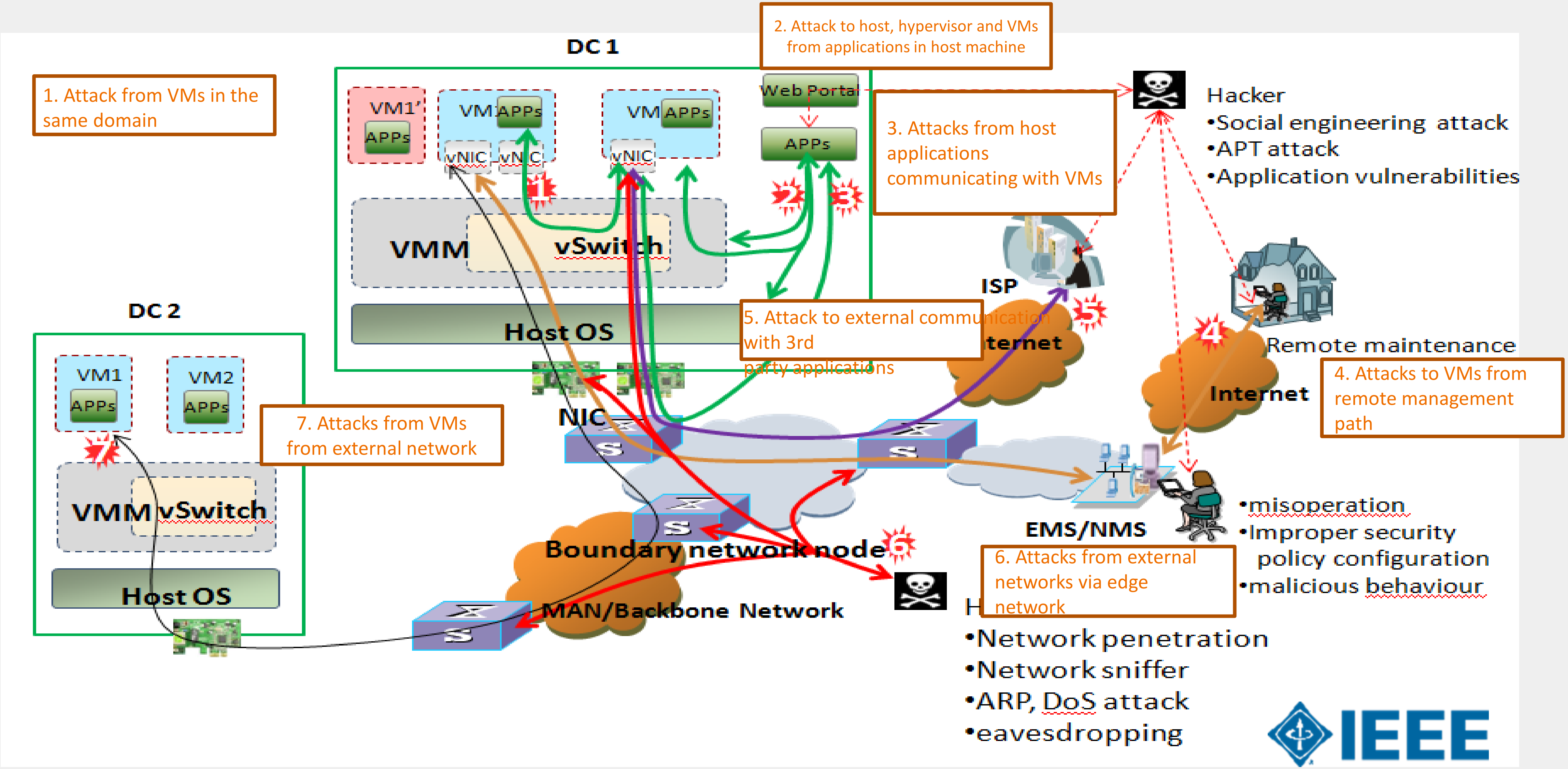
NOTE: we must implement vIDS/vIPS & vFirewalls to mitigate these types of attacks

Network Function Virtualization

Security Challenges and Opportunities



Threat Scenarios in NFV (Reference - ETSI NFV)



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

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

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

Security Use Cases for Network Slicing

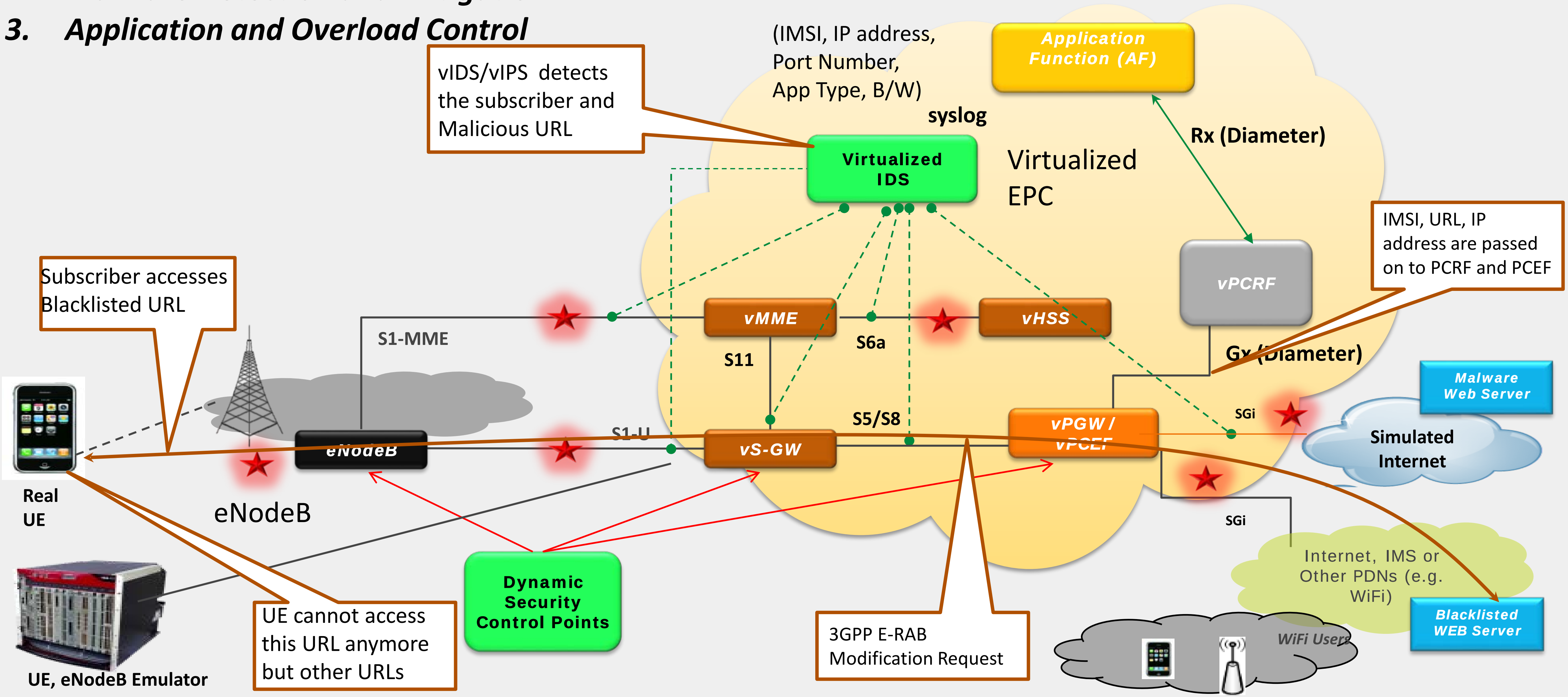
- Controlling Inter-Network Communications
- Instantiation time Impersonation attacks against Network Slice Manager
- Impersonation attacks against a Network Slice instance within an Operator Network
- Impersonation attacks against different Network Slice managers within an Operator Network
- Different 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

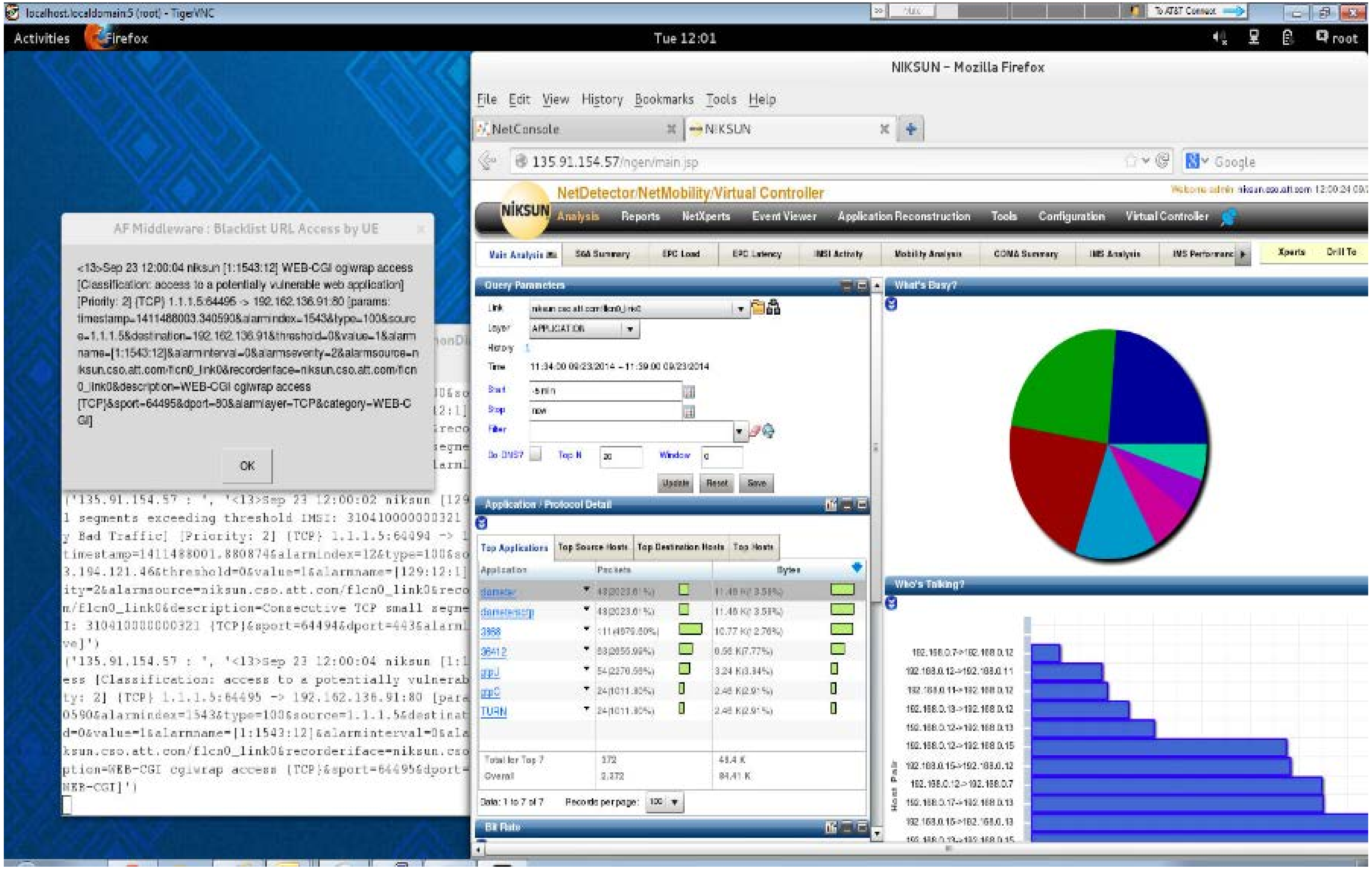
Forum	Focus
IETF	Network Virtualization Overlay, Dynamic Service Chaining, Network Service Header
3GPP	Mobility and Security Architecture and Specification
ETSI ISG NFV	NFV Platform/Deployment Standards – Security, Architecture/Interfaces, Reliability, Evolution, Performance
IEEE	Develop Technologies 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

Virtual IDS Prototype for Mobility CORE

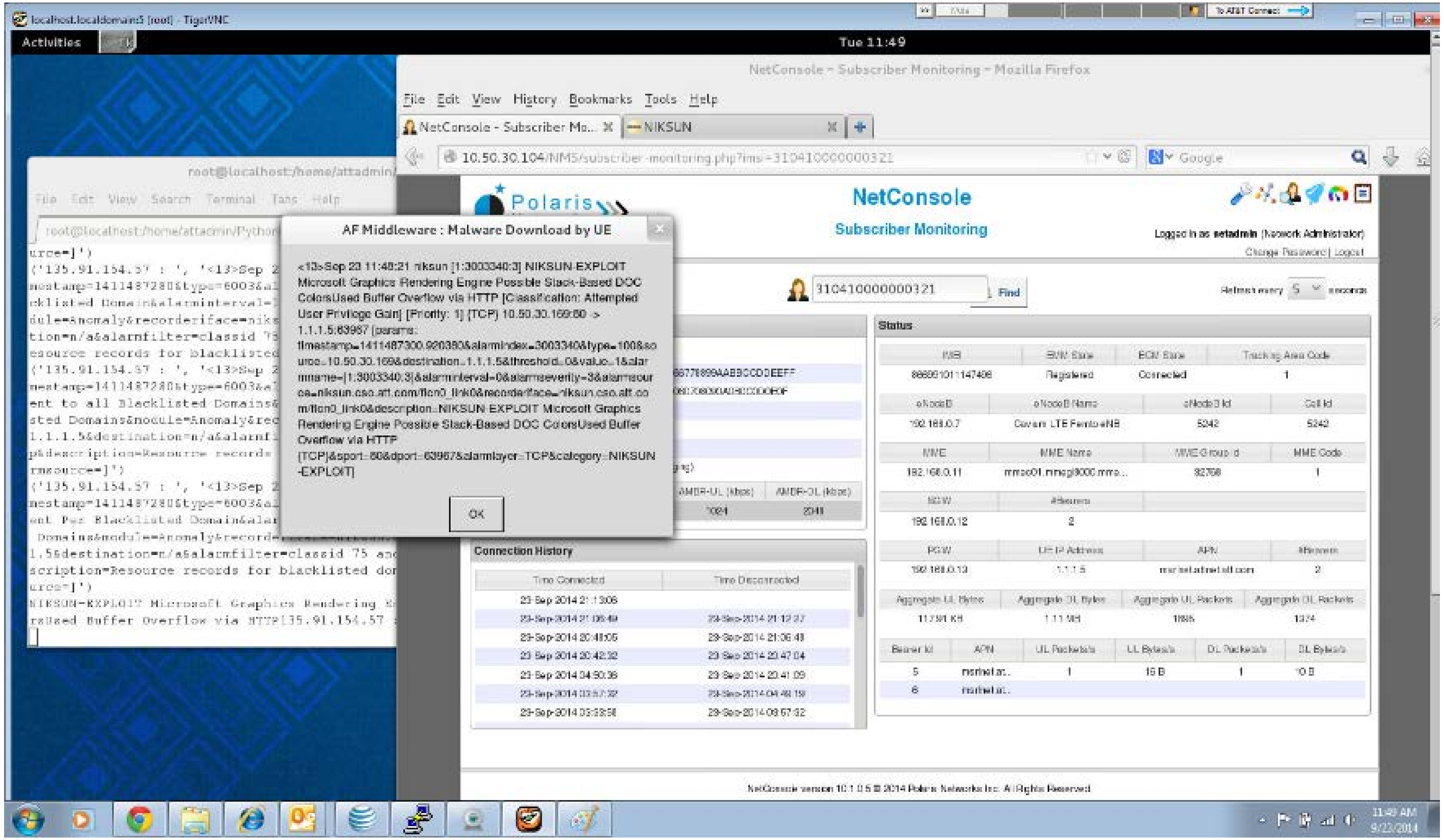
1. ***Malicious URL Detection and Mitigation***
2. ***Malware Detection and Mitigation***
3. ***Application and Overload Control***

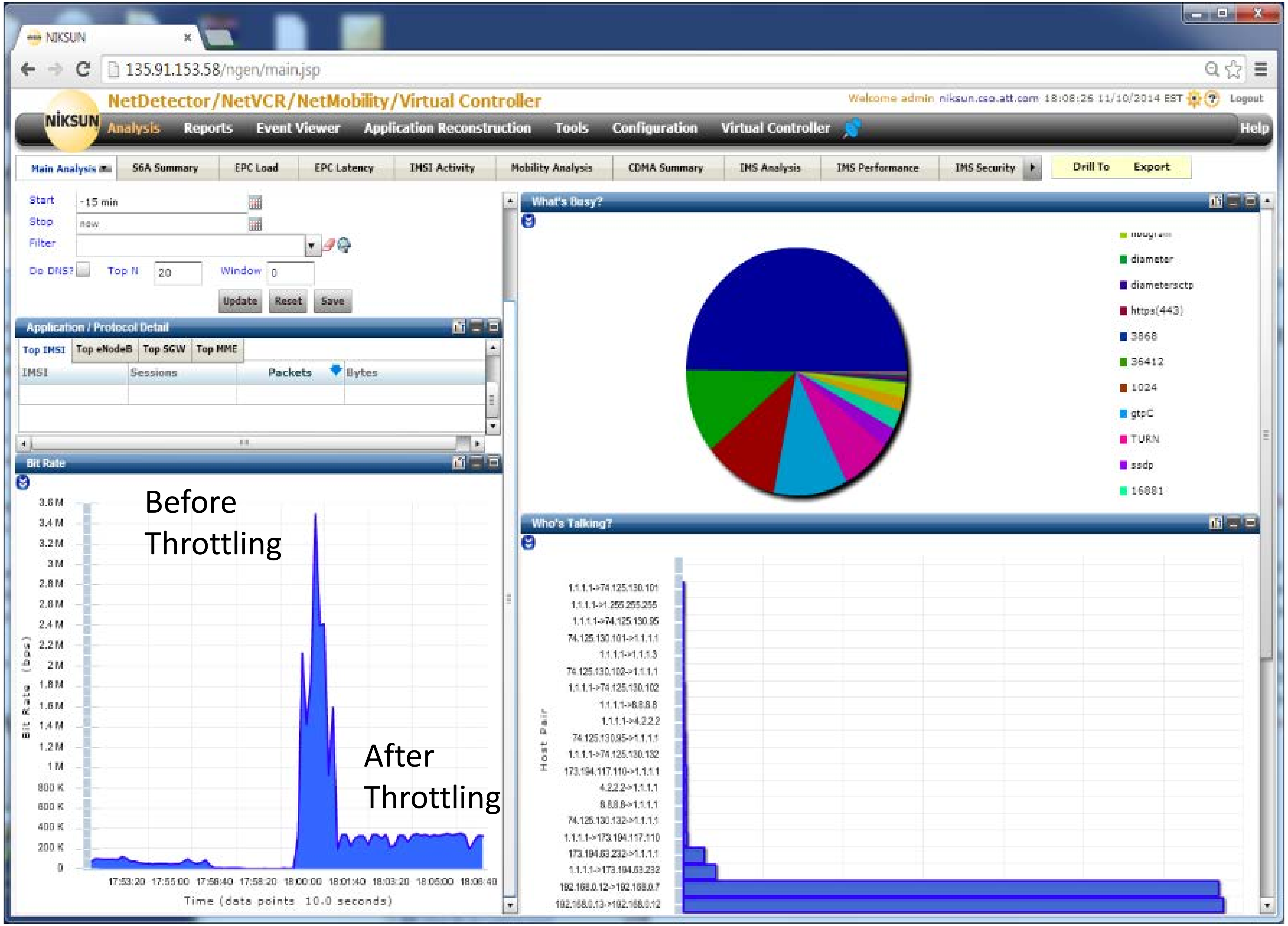


Blacklist Detection for DSC



Malware Download Detection for GDSC




NIKSUN
135.91.153.58/ngen/main.jsp
NetDetector/NetVCR/NetMobility/Virtual Controller
Analysis
Reports
Event Viewer
Application Reconstruction
Tools
Configuration
Virtual Controller
Help
Logout
Main Analysis
S6A Summary
EPC Load
EPC Latency
IMSI Activity
Mobility Analysis
CDMA Summary
IMS Analysis
IMS Performance
IMS Security
Drill To
Export
Start
Stop
Filter
Update
Reset
Save
Application / Protocol Detail
Top IMSI
Top eNodeB
Top SGW
Top MME
IMSI
Sessions
Packets
Bytes
Bit Rate
Before Throttling
After Throttling
Time (data points 10.0 seconds)
What's Busy?
diameter
diametersctp
https(443)
3868
36412
1024
gtpC
TURN
ssdp
16881
Who's Talking?
Host Pair

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 Electronics Packaging Society

Industry

Academia, Students

Initiative Profile

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

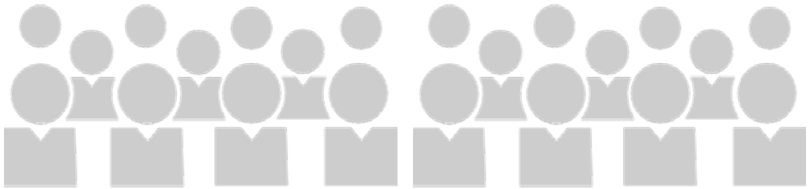
IEEE OUs

IEEE STANDARDS ASSOCIATION

IEEE EDUCATIONAL ACTIVITIES

Futurenetworks.IEEE.org

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

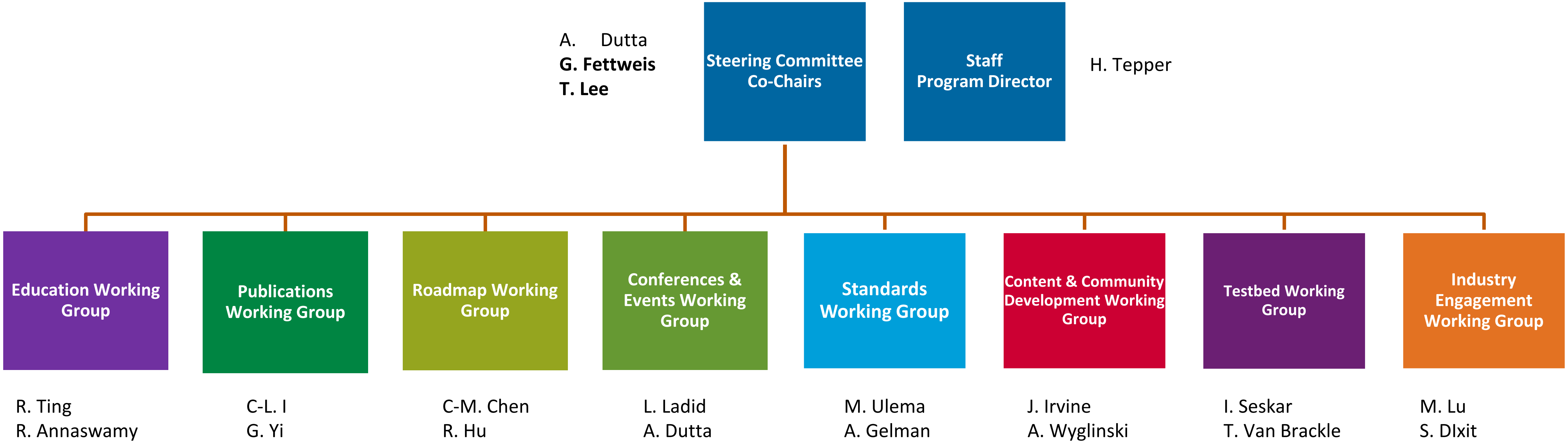
Publications

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



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

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

Thank you