Security for 5G and Beyond

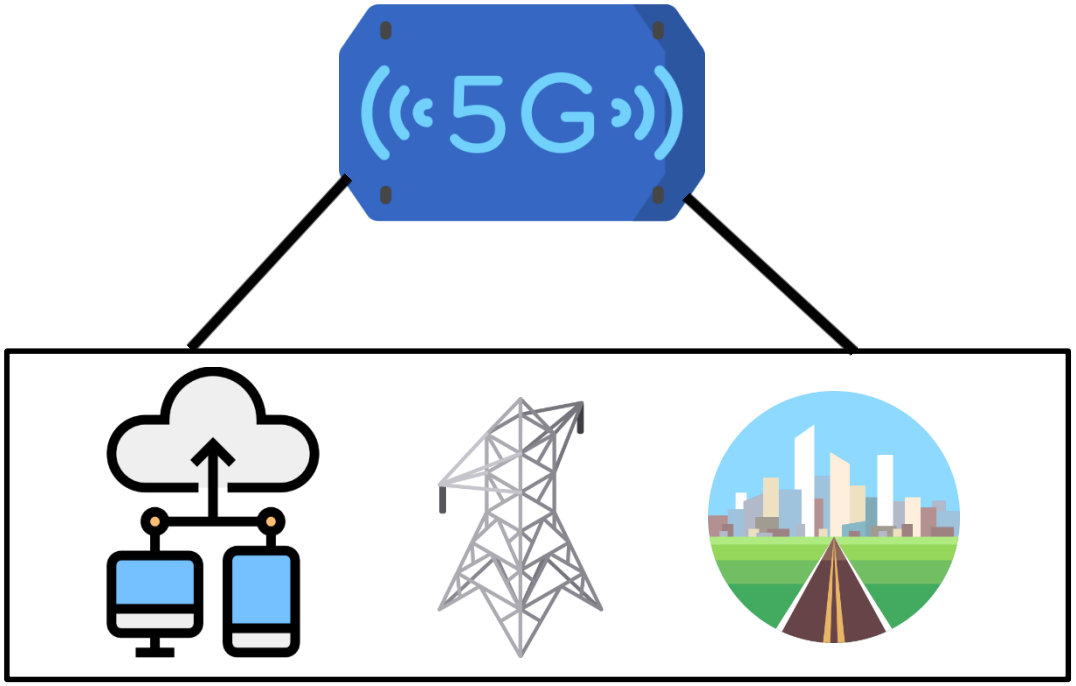
Ijaz Ahmady, Shahriar Shahabuddinz, Tanesh Kumar, Jude Okwuibe, Andrei Gurtovx, Mika Ylianttila

Presented by
Jeonghun Cha

INDEX

SEOULTECH

1. Introduction



- The 5G wireless networks will provide very high data rates and higher coverage with significantly improved Quality of Service (QoS), and extremely low latency

- 5G will connect nearly all aspects of the human life to communication networks

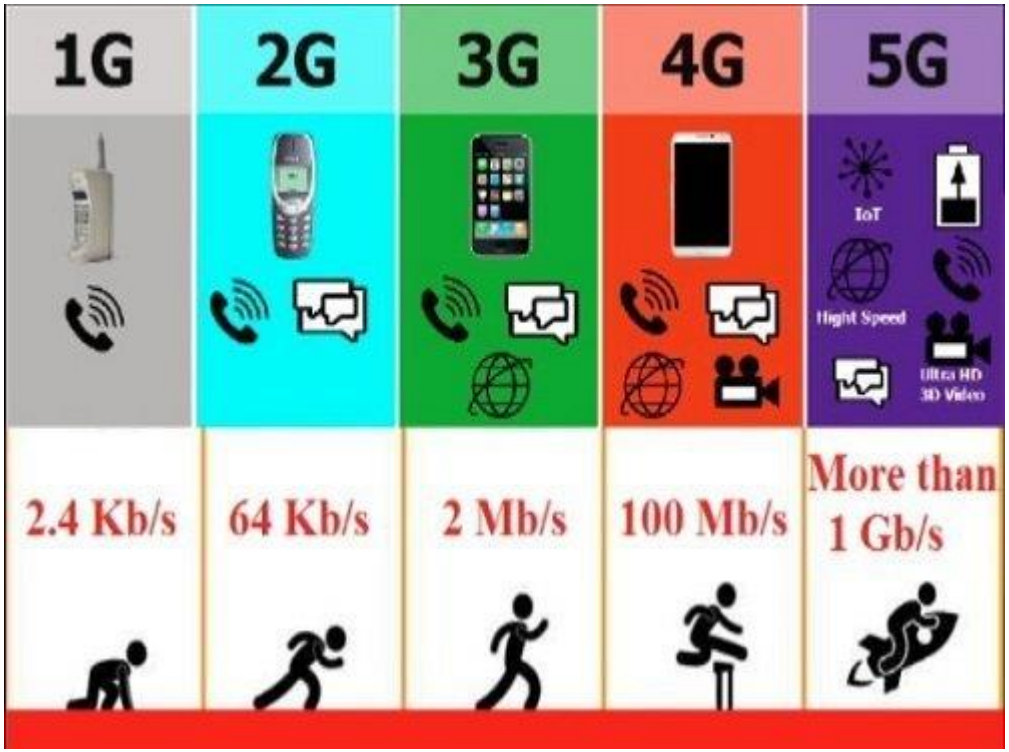
SEOULTECH

1. Introduction

- 5G is not a mere incremental advancement of 4G as one might intuitively think, but an integration of new disruptive technologies to meet the ever growing demands of user traffic, emerging services, existing and future IoT devices

- With all these capabilities, 5G will connect nearly all aspects of the human life to communication networks, and this underscores the need for robust security mechanisms across all network segments of the 5G.

1. Introduction



- The security solutions and architectures used in previous generations (i.e. 3G and 4G), apparently, will not suffice for 5G

- The main reason for new security solutions and architecture is the dynamics of new services and technologies in 5G

SEOULTECH

1. Introduction

- there are new technological concepts or solutions that will be used in 5G to meet the demands of increasingly diverse applications and connected devices

- the concepts of cloud computing, Software Defined Networking (SDN), and Network Function Virtualization (NFV) are considered to be the potential problem solvers in terms of costs and efficiency

- However, each of these technologies have its own security challenges

SEOULTECH

1. Introduction

- the core network entities such as Home Subscriber Server (HSS) and Mobility Management Entity (MME) that hold the user billing, personal, and mobility handling information, respectively, deployed in clouds will render the whole network ineffective if security breaches occur

- Similarly, SDN centralizes the network control logic in SDN controllers.

- These controllers will be the favorite choice for attackers to render the whole network down through Denial of Service (DoS) or resource exhaustion attacks

SEOULTECH

1. Introduction

- This article studies the state of the art of security in 5G networks
- It starts off with a dive into the security challenges and corresponding solutions for the previous generations of networks ranging from 1G to 4G
- It then presents a comprehensive overview of the technologies associated with 5G with regards to their corresponding security challenges and respective solutions

SEOULTECH

2. Related Work

- The vision of 5G lies in providing very high data rates (Gigabits per second), extremely low latency, manifold increase in base station density and capacity, and significant improvement in quality of service, compared to 4G systems

- The concerns related to security, indirectly if not directly effecting it, pertaining to 4G are the lack of mechanisms to support data traffic bursts, limited processing capabilities of base stations, and latency

- These limitations, if not removed, will make the network prone to security challenges

SEOULTECH

2. Related Work

- the survey article [11] provides some interesting insights on the limitations of the current 4G networks that must be solved in 5G

- General requirements and mechanisms for strengthening security in 5G are presented in [15]

- A survey on security of 4G and 5G networks is presented in [16]
  - The article focuses on existing authentication and privacy-preserving schemes for 4G and 5G networks

- Security challenges and the possible mitigation techniques along with standardization efforts in 4G and older generations are presented in [17]

SEOULTECH

2. Related Work

- Security challenges and the possible mitigation techniques in the wireless air interfaces are discussed in [19]
  - The article considers various wireless access technologies such as Bluetooth, Wi-Fi, WiMAX and LTE, and discusses the inherent security limitations and future directions for strengthening the security of each technology

- However, the increasing diversity and number of communicating devices such as IoT and V2X would require drastically new security solutions that will need context awareness and high degree of automation.

- Therefore, this article also discusses the future of security in environments replete with massive IoT, such as smart cities

SEOULTECH

Acronyms	Full Form
AI	Artificial Intelligence
AKA	Authentication and Key Agreement
AMF	Autonomous Management Framework
APIs	Application Programming Interfaces
ARIB	Association of Radio Industries and Businesses
BTS	Base Transceiver Stations
CCPS	Cloud-based Cyber-Physical Systems
CPS	Cyber-Physical System
DTLS	Datagram Transport Layer Security
DoS	Denial of Service
DDoS	Distributed DoS
DPI	Deep Packet Inspection
EAP-AKA	Extensible Authentication Protocol-AKA
EPC	Evolved Packet Core
EPS	Evolved Packet System
ETSI	European Telecommunications Standards Institute
E-UTRAN	Evolved Universal Terrestrial Radio Access Network
GSM	Global System for Mobile Communication
GSMA	GSM Association
GTP	GPRS Tunnelling Protocol
HetNets	Heterogeneous Networks
HIDS	Host Intrusion Detection System
HSS	Home Subscriber Server
HTTP	HyperText Transfer Protocol
HX-DoS	HTTP and XML Denial of Service
IaaS	Infrastructure as a Service
IDS	Intrusion Detection Systems
ID/P-S	Intrusion Detection or Prevention Systems
IETF	Internet Engineering Task Force
IP	Internet Protocol
IMSI	International Mobile Subscriber Identity
IoT	Internet of Things
IPSec	Internet Protocol Security
ITU	International Telecommunications Union
(LTE)-(A)	(Long Term Evolution)-(Advanced)
MEC	Multi-access Edge Computing
MIMO	Multiple-Input and Multiple-Output
MME	Mobility Management Entity
mmWave	Millimeter Wave
M2M	Machine-to-Machine Communications

MTC	Machine Type Communication
MVNOs	Mobile Virtual Network Operators
NAS	Non-Access Stratum
NFV	Network Function Virtualization
NGMN	Next Generation Mobile Networks
NIDS	Network Intrusion Detection System
NIST	National Institute of Standards and Technology
OFDM	Orthogonal Frequency Division Multiplexing
ONF	Open Networking Foundation
PaaS	Platform as a Service
PDN	Public Data Network
QoS	Quality of Service
RAN	Radio Access Network
RAT	Radio Access Technology
SaaS	Software as a Service
SIM	Subscriber Identity Module
SIPDAS	Slowly-increase Polymorphic DDoS Attack Strategy
SDN	Software Defined Networking
SN	Serving Network
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TMSI	Temporary Mobile Subscriber Identity
TVDc	Trusted Virtual Data Center
UAVs	Unmanned Aerial Vehicles
UAV-BS	UAV with Base Station
UDP	User Datagram Protocol
UE	User Equipment
UMTS	Universal Mobile Telecommunications System
USIM	Universal Subscriber Identity Module
VNFs	Virtual Network Functions
V2V	Vehicle-to-Vehicle
V2X	Vehicle-to-Everything
XG	Future Generations
XML	Extensible Markup Language
3GPP	3G Partnership Project
5GPPP	5G Public-Private Partnership

TABLE I

ACRONYMS AND CORRESPONDING FULL MEANING

3. SECURITY IN WIRELESS NETWORKS: FROM 1G TO 4G

- The 1G cellular systems used analog signal processing and were designed primarily for voice services

- This advance phone service did not use encryption and thus there was no security of information or telephone conversations

- Hence, practically the whole system and users were open to security challenges such as eavesdropping, illegal access, cloning, and user privacy [4], [32]

3. SECURITY IN WIRELESS NETWORKS: FROM 1G TO 4G

- Global System for Mobile (GSM) communication became the most successful and widely used standard in cellular communications as part of 2G cellular networks

- The signalling and user data protection was carried out through encryption in which the Subscriber Identity Module (SIM) played an important role in the encryption keys.

- However, 2G had several security limitations or weaknesses. The operators only authenticated the UEs in a unilateral mechanism, whereas the UEs had no option to authenticate the operator

3. SECURITY IN WIRELESS NETWORKS: FROM 1G TO 4G

- The 3G cellular networks were developed primarily to provide higher data rates than 2G networks.

- Universal Mobile Telecommunications System (UMTS) is a 3G cellular technology that is developed and maintained by 3GPP

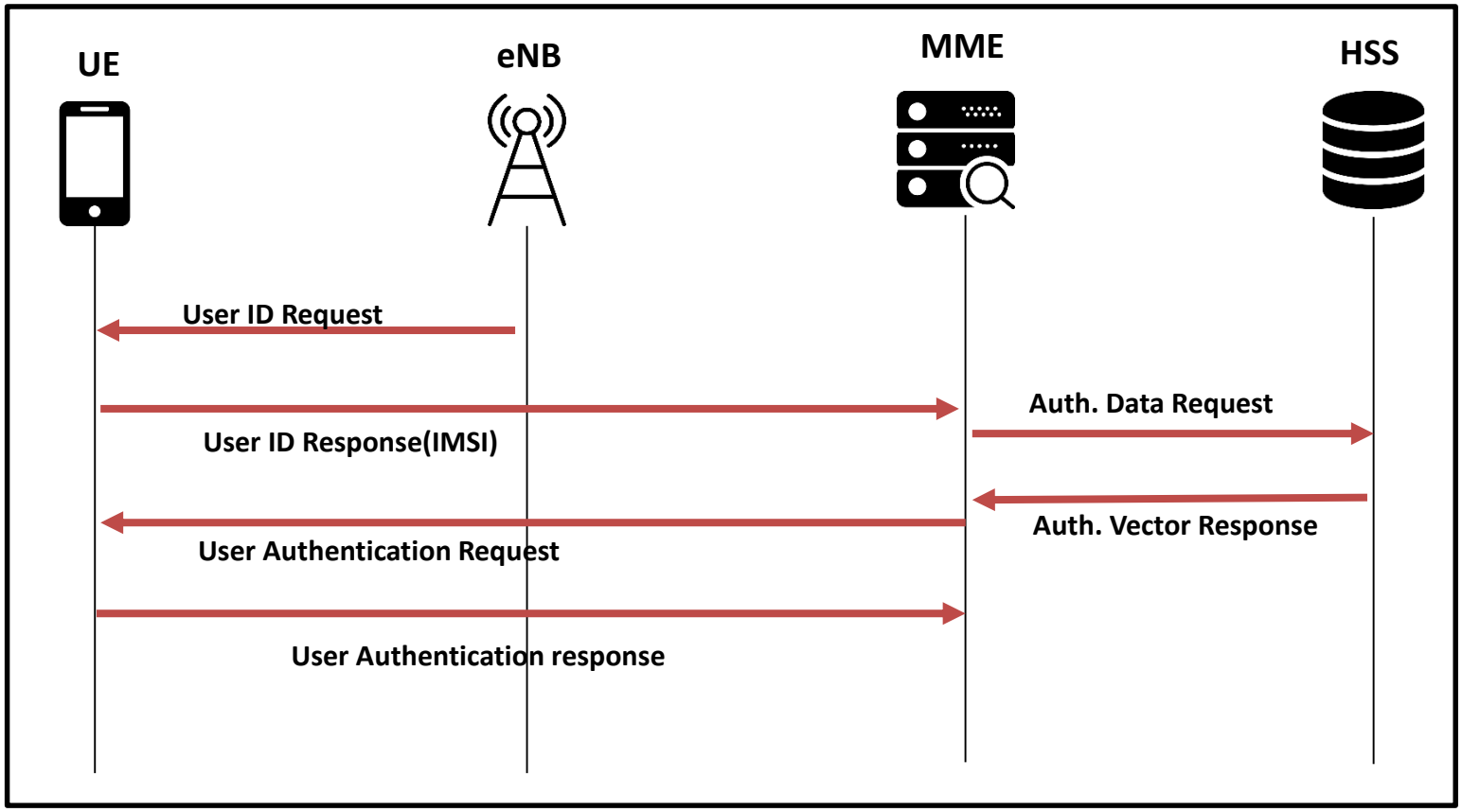
- Contrary to the unilateral authentication of GSM, UMTS supports bilateral authentication which removes the threat of a false base station

3. SECURITY IN WIRELESS NETWORKS: FROM 1G TO 4G

- The release 10 from 3GPP, which is commonly known as LTE-Advanced (LTE-A), fulfills the requirements of the 4G standard that was specified by International Telecommunications Union - Radio Communication Sector (ITU-R) [47]

- The Evolved Packet System-AKA (EPS-AKA) had one major enhancement over UMTS-AKA which is called cryptographic network separation.

The Evolved Packet System-AKA (EPS-AKA)



UE : User Equipment
eNB : eNodeB (based station)
MME : Mobility Management Entity
HSS : Home Subscriber Server

TABLE II
SUMMARY OF SECURITY EVOLUTION FROM 1G TO 4G

Network	Security Mechanisms	Security Challenges
1G	No explicit security and privacy measures.	Eavesdropping, call interception, and no privacy mechanisms.
2G	Authentication, anonymity and encryption-based protection.	Fake base station, radio link security, one way authentication, and spamming.
3G	Adopted the 2G security, secure access to network, introduced Authentication and Key Agreement (AKA) and two way authentication.	IP traffic security vulnerabilities, encryption keys security, roaming security.
4G	Introduced new encryption (EPS-AKA) and trust mechanisms, encryption keys security, non-3G Partnership Project (3GPP) access security, and integrity protection.	Increased IP traffic induced security, e.g. DoS attacks, data integrity, Base Transceiver Stations (BTS) security, and eavesdroping on long term keys. Not suitable for security of new services and devices, e.g. massive IoT, foreseen in 5G.

4. SECURITY IN 5G: AN OVERVIEW

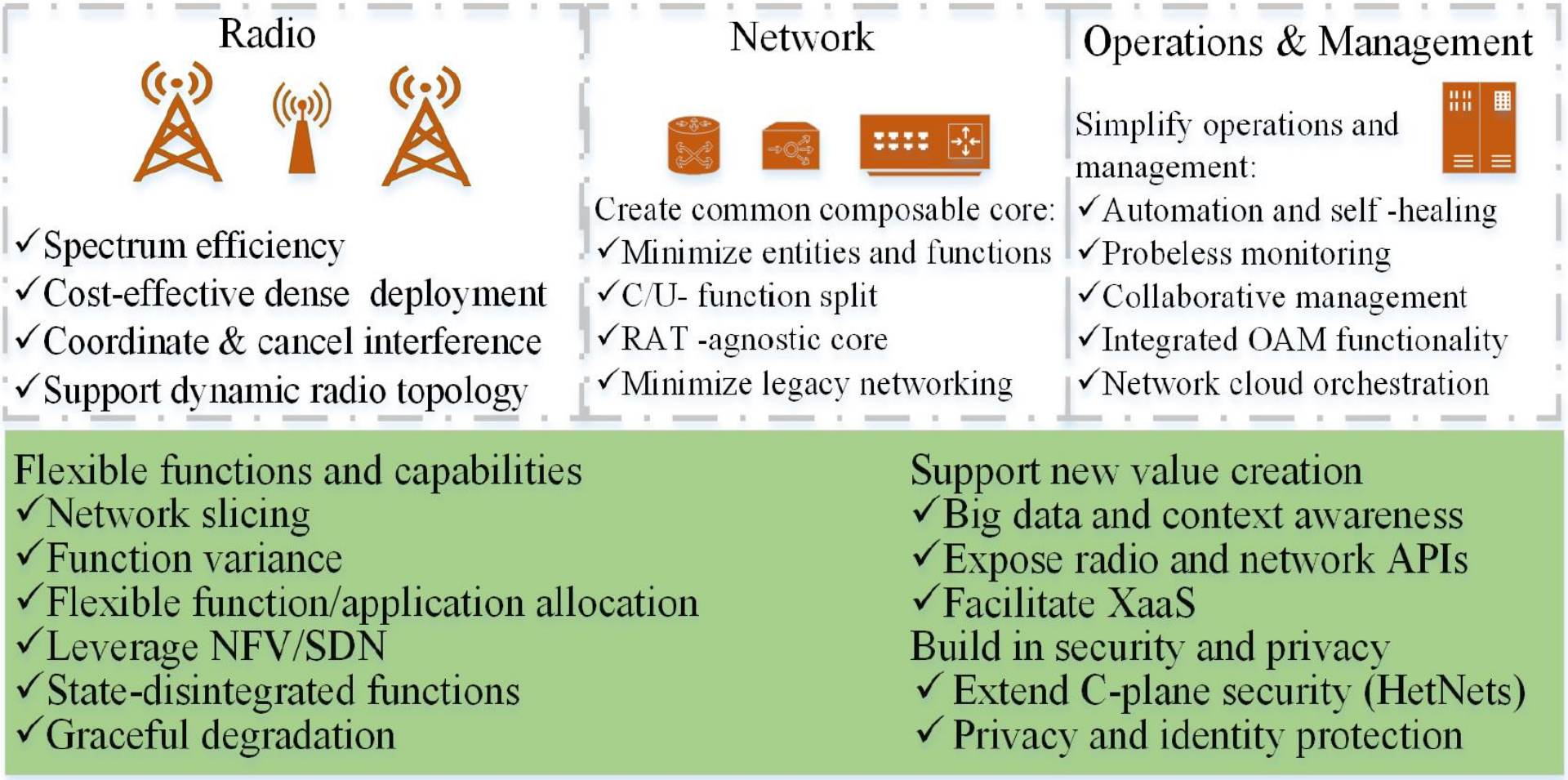


Fig. 2. 5G Design Principles.

SEOULTECH

4. SECURITY IN 5G: AN OVERVIEW

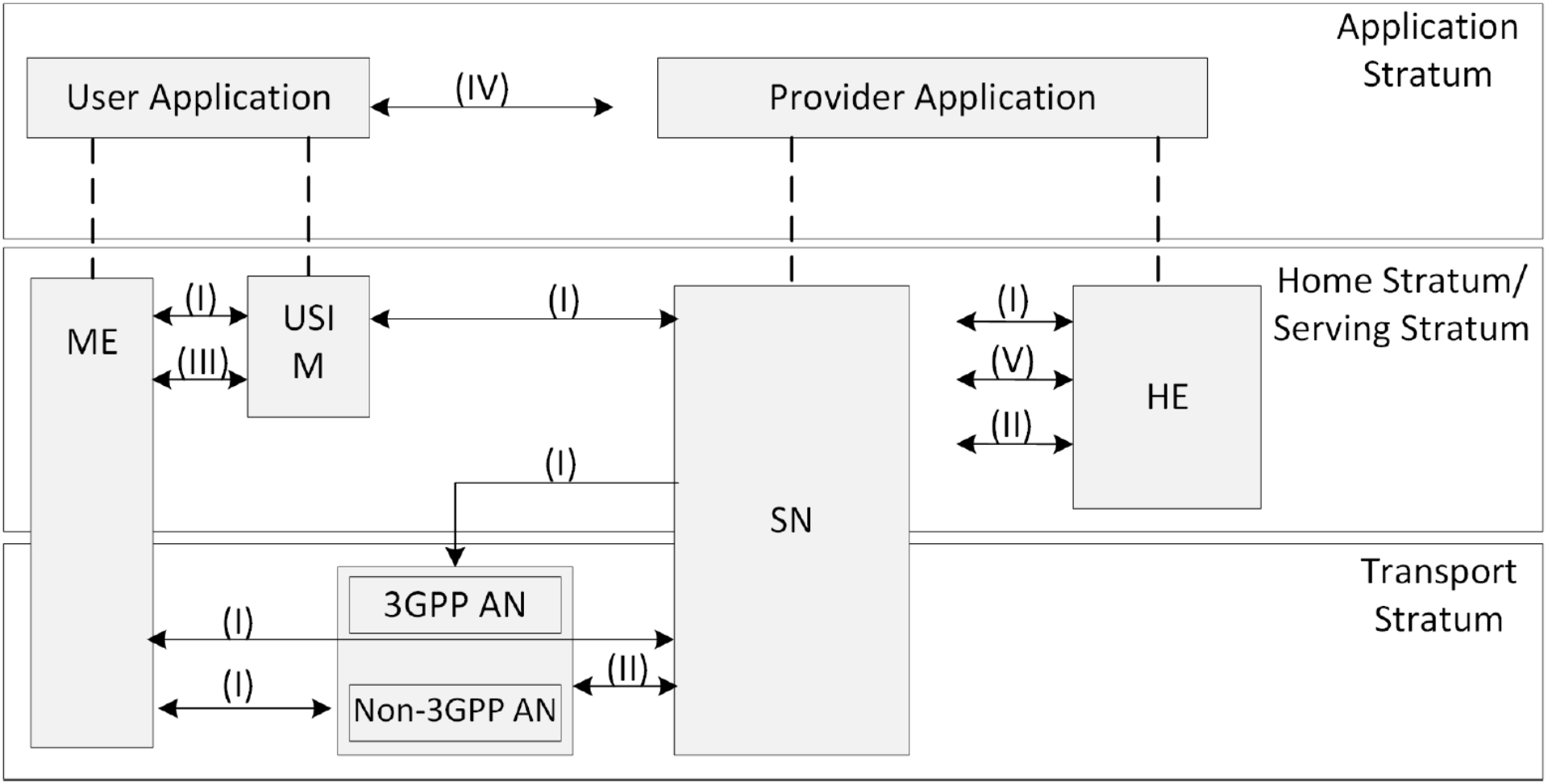


Fig. 3. Overview of the security architecture

SEOULTECH

4. SECURITY IN 5G: AN OVERVIEW

General Overview of Security in 5G

- The Next Generation Mobile Networks (NGMN) has provided recommendations for 5G based on current network architectures and the shortfall in security measures that are either not developed or developed but not yet put to use

- **Flash network traffic**: It is projected that the number of end user devices will grow exponentially in 5G that will cause significant changes in the network traffic patterns either accidentally or with malicious intent

- **Security of radio interface keys**: In previous network architectures, including 4G, the radio interface encryption keys are generated in the home network and sent to the visited network over insecure links causing a clear point of exposure of keys

4. SECURITY IN 5G: AN OVERVIEW

- **User plane integrity:** The 3G and 4G systems provide protection to some signaling messages but do not provide cryptographic integrity protection for the user data plane.

- **Mandated network security**: There can be certain servicedriven constraints (e.g. latency) in security architectures leading to optional use of security measures.

- **Consistency in subscriber level security policies**: User security measures must be intact when a user moves from one operator network to another.

- **DoS attacks on the Infrastructure:** This threat will be more severe due to the possibility of attacks from machines that are geographically dispersed and are in huge numbers (compromised IoT)

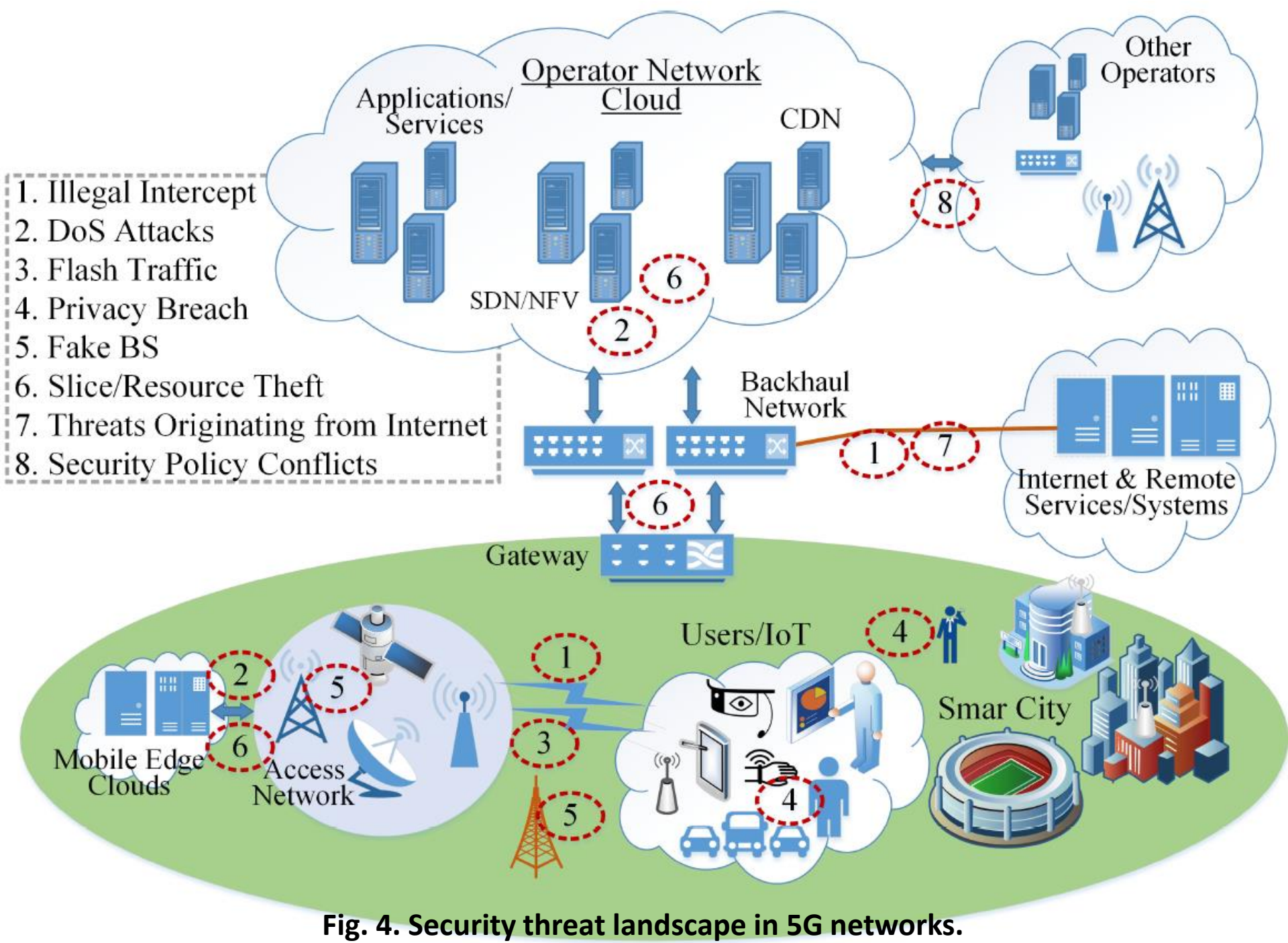
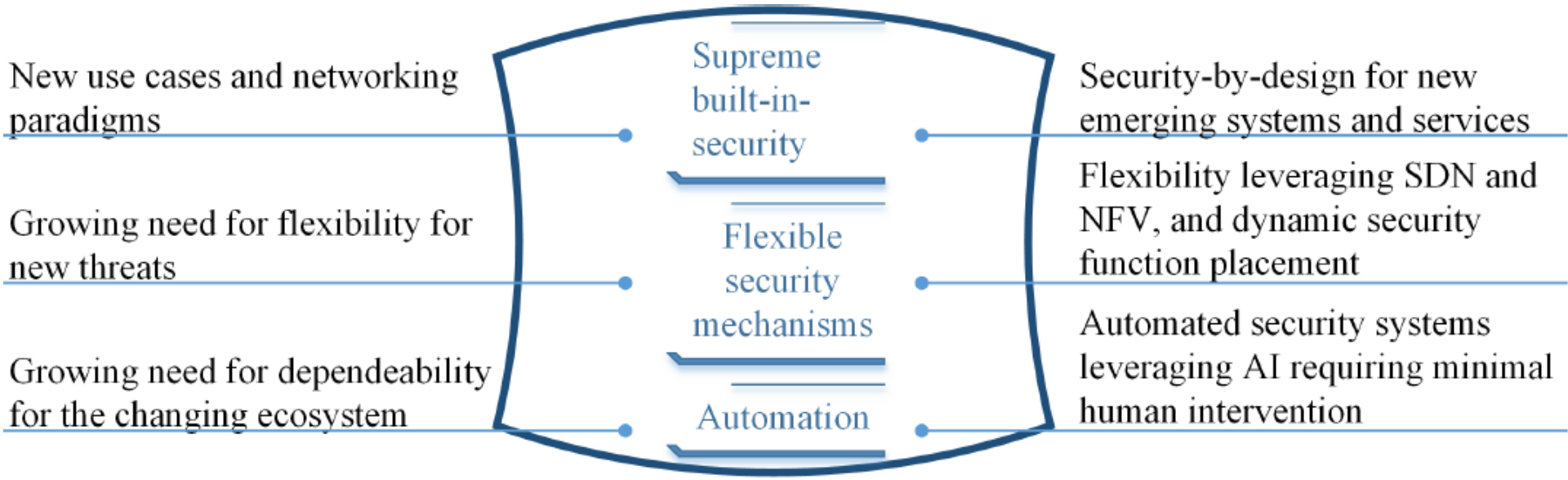


Fig. 4. Security threat landscape in 5G networks.

4. SECURITY IN 5G: AN OVERVIEW

- The vision of secure 5G systems that is outlined by NGMN [7] is based on three principles. These are: i) flexible security mechanisms, ii) supreme built-in security, and iii) security automation, as highlighted in Fig. 5



SEOULTECH

TABLE III
SECURITY DIMENSIONS DEFINED BY ITU-T

Security Dimension	**Brief Explanation**
Access Control	Protects against unauthorized use of network resources. It also ensures that only authorized persons or devices access the network elements, services, stored information and information flows.
Authentication	Confirms identities of communicating entities, ensures validity of their claimed identities, and provides assurance against masquerade or replay attacks.
Non-Repudiation	Provides means for associating actions with entities or user using the network and that an action has either been committed or not by the entity.
Data Confidentiality	Protects data from unauthorized disclosure, ensures that the data content cannot be understood by unauthorized entities.
Communication security	Ensures that information flows only between the authorized end points and is not diverted or intercepted while in transit.
Data integrity	Ensures the correctness or accuracy of data, and its protection from unauthorized creation, modification, deletion, and replication. It als provides indications of unauthorized activities related the data.
Availability	Ensures that there is no denial of authorized access to network resources, stored information or its flow, services and applications.
Privacy	Provides protection of information that might be derived from the observation of network activities.

4. SECURITY IN 5G: AN OVERVIEW

- With the anticipation of 5G, various actors; even outside the telecom sector such as automotive are indulging in evaluating the security impacts of 5G
- However, the standardization is still in the drafting phase

TABLE IV
SECURITY ACTIVITIES OF VARIOUS STANDARDIZATION BODIES

Standardization bodies	Workgroups	Major security areas in focus	Milestones
3GPP	Service and System Aspects Security Group (SA3)	Security architecture, RAN security, authentication mechanism, the subscriber privacy, network slicing	TR 33.899 Study on the security aspects of the next generation system, TS 33.501: Security architecture and procedures for 5G System
5GPPP	5GPPP Security WG	Security architecture, the subscriber privacy, the authentication mechanism	5G PPP Security Landscape (White Paper) June 2017.
IETF	I2NSF, DICE WG, ACE WG, DetNet WG	Security solutions for massive IoT devices in 5G, User privacy, Network security functions (NSFs)	RFC 8192, RFC 7744, Deterministic Networking (DetNet) Security Considerations
NGMN	NGMN 5G security group (NGMN P1 WS1 5G security group)	Subscriber privacy, Network slicing, MEC security	5G security recommendations: Package 1 and 2, and 5G security: Package 3
ETSI	ETSI TC CYBER, ETSI NFV SEC WG, ESTI MEC ISG	Security architecture NFV security, MEC security, privacy	ETSI GS NFV-SEC 010, ETSI GS NFV-SEC 013 ETSI GS NFV-SEC 006 and ETSI GS MEC 009
NIST	Security working group	IoT security guidelines and assessment	Draft Interagency Report, NISTIR 8200

5. SECURITY IN 5G NETWORKS: CHALLENGES AND SOLUTIONS

- To properly investigate the security perspectives of the overall network in a systematic way, security in the network architecture is described in three-tiers i.e. i) access networks, ii) backhaul network, and iii) the core network

- i) access networks :
  - The current networks are already prone to many Internet-based threats that can target the access nodes such as eNBs in LTE and low powered access nodes, as detailed in [68].
  - 5G will leverage virtualization, SDN, and cloud technologies to adapt execution logic to specific services with composition and instantiation of access in different network locations [130].
  - With such capabilities, 5G will improve the systems' robustness against various types of security challenges arising in diverse access technologies.

SEOULTECH

5. SECURITY IN 5G NETWORKS: CHALLENGES AND SOLUTIONS

- ii) backhaul network :
  - The security of backhaul is different in a sense that it involves both radio and core part of the network.
  - For traffic towards the Internet or external network, the eNB sends the traffic to the serving gateway through GPRS Tunneling Protocol (GTP).
  - The serving gateway sends the traffic to Public Data Network (PDN) gateway which communicates with external networks or the Internet.
  - The LTE the backhaul enhanced network security through introducing Internet Protocol Security (IPSec) based GTP tunnels for the X2 interface between eNBs, and S1 interface between eNBs and MMEs

5. SECURITY IN 5G NETWORKS: CHALLENGES AND SOLUTIONS

- iii) the core network :
  - The core network of LTE or 4G, called EPC, comprised different entities such as MME, serving gateway, PDN gateway, and HSS [163]
  - The core network is IP based and ensures end to end service delivery, security and QoS, and maintains subscriber information
  - The 5G core network is more dynamic compared to the previous generations leveraging NFV, SDN and cloud technologies as described in Section VI.
  - it is the main target of security threats and prone to security vulnerabilities as well.

SEOULTECH

5. SECURITY IN 5G NETWORKS: CHALLENGES AND SOLUTIONS

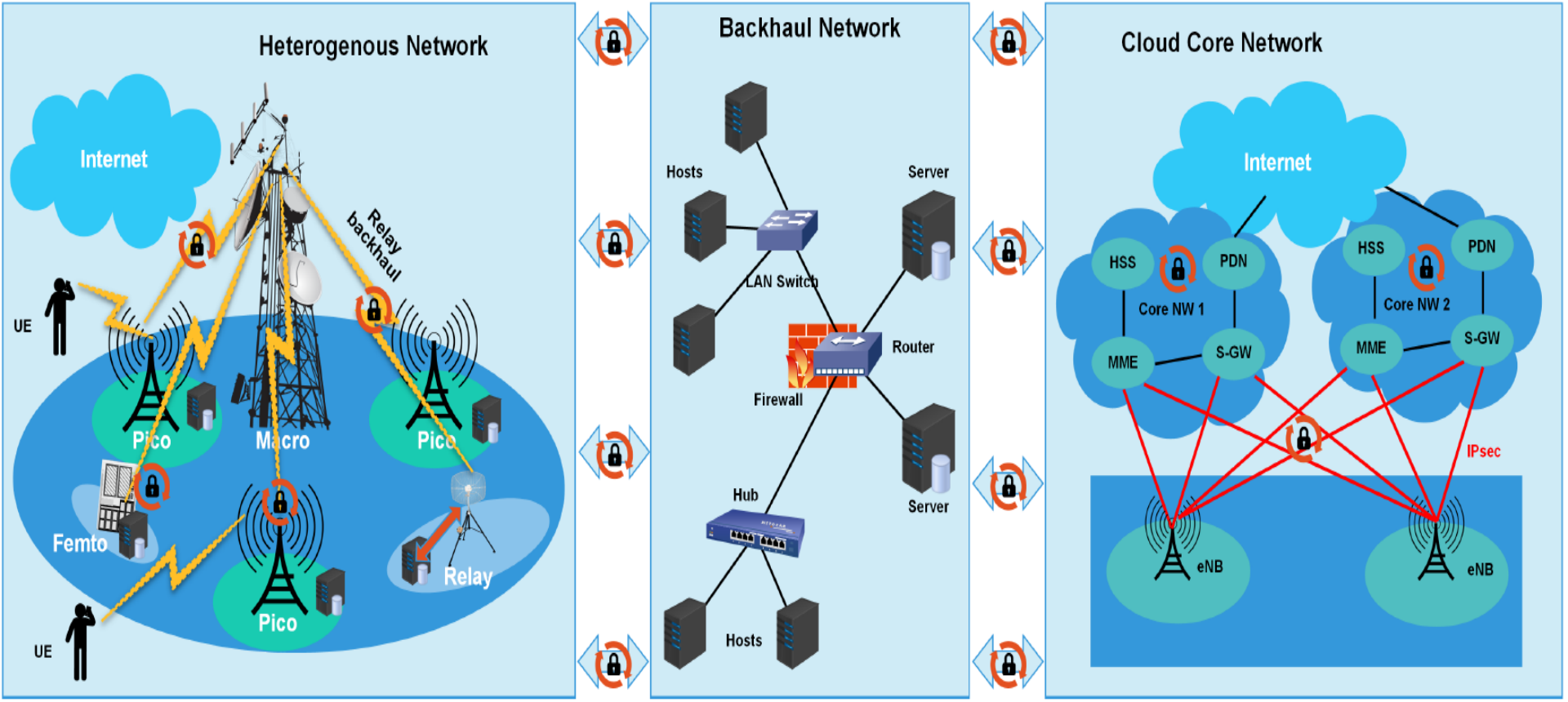


Fig. 6. High-level architecture presentation of 5G networks.

SEOULTECH

6. SECURITY IN KEY 5G TECHNOLOGIES

- the main enabling and disruptive technologies compared to the previous generations are massive MIMO antennas, SDN, NFV and the concepts of cloud computing such as Multi-access Edge Computing (MEC)

- 1) Security Challenges in massive MIMO:

  - Massive MIMO is considered as one the most promising and disruptive technologies for 5G [179]

  - The key idea of massive MIMO is to equip the base station with a large number of antenna elements that can serve a large number of user terminals with the same frequency band [3]

  - The large number of antenna elements can be used in various modes to increase the data rates or to enhance the reliability, coverage or energy efficiency

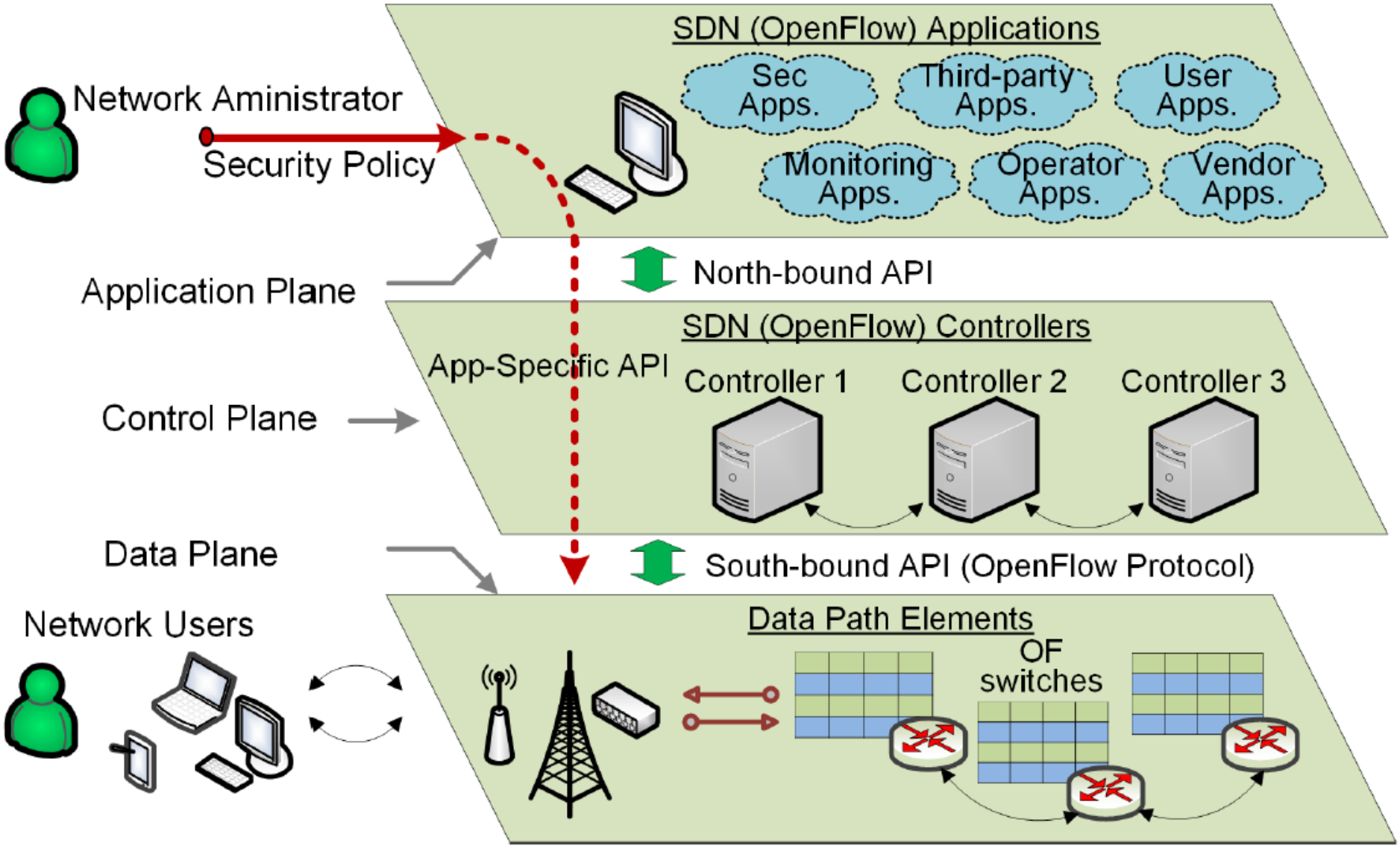
6. SECURITY IN KEY 5G TECHNOLOGIES

- 1) The security vulnerabilities in massive MIMO:
  - In the passive eavesdropping, the attacker tries to intercept the transmitted signals. The passive eavesdropper does not transmit any signal itself
  - In the active eavesdropping, the attacker also transmits signals to disrupt the legitimate user's transmission
  - If the only goal of the active attack is to disrupt the legitimate transmission, it can be called a jamming attack [183]
  - Another intelligent form of the active attack is based on pilot contamination
    - It is called pilot spoofing where the attacker pretends to be a legitimate user

SEOULTECH

6. SECURITY IN KEY 5G TECHNOLOGIES

- 2) Security in SDN :
  - SDN separates the network control plane from the forwarding plane and centralizes the network control into softwarebased network control platforms
  - The softwarized network control functions are logically centralized that interact with forwarding devices through programmable APIs
  - This achieves simplicity in network control, management and operation, and accelerates novelty in network feature development and deployment
  - centralizing the network control make the control platform a favorable choice for DoS attacks
  - exposing critical APIs to unintended software will expose the network to security threats. The number of security challenges have grown since the inception of OpenFlow


SDN (OpenFlow) Applications
Sec Apps.
Third-party Apps.
User Apps.
Monitoring Apps.
Operator Apps.
Vendor Apps.
Network Aministrator
Security Policy
Application Plane
North-bound API
SDN (OpenFlow) Controllers
App-Specific API
Controller 1
Controller 2
Controller 3
Control Plane
Data Plane
South-bound API (OpenFlow Protocol)
Network Users
Data Path Elements
OF switches

6. SECURITY IN KEY 5G TECHNOLOGIES

- 2) Security in NFV :
  - The main idea behind virtualization is to decouple a system's service model from its physical realization to use logical instances of the physical hardware for different purposes
  - Since the number of services or virtual functions will grow a growing concern is related to the manual configurations of the virtual systems or VNFs [226] that can lead to potential security breaches due to the increased complexity with the growth of the systems.

- Virtualization can highly increase the user, service and network security. A basic mechanism is to use slicing to separate traffic of different services (Fig. 8) or network segments based on security priorities

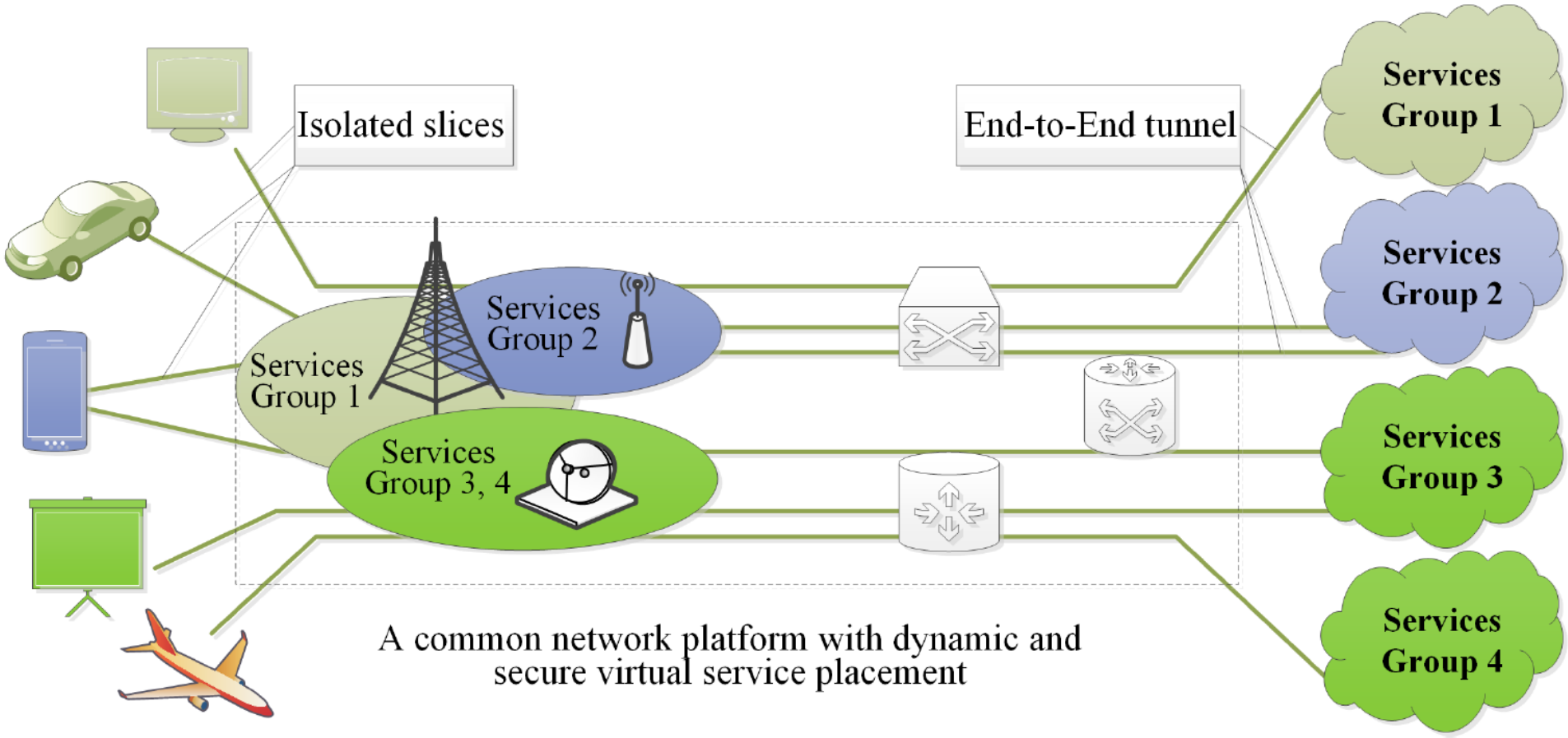


Fig. 8. Secure end-to-end tunnels for different services

6. SECURITY IN KEY 5G TECHNOLOGIES

- 2) Security in NFV :
  - Even though virtual systems can be difficult to monitor compared to physical systems, virtual systems have their own benefits in terms of security
  - For instance, a virtual system can be easily migrated or replicated to minimize the effect of security attacks
  - The dynamic nature of VNFs and virtualized resources can be used as a strength in terms of security
  - For instance, the flexibility of NFV allows isolating compromised network elements, or even whole network segments through defining security zones and using traffic steering [228]

SEOULTECH

6. SECURITY IN KEY 5G TECHNOLOGIES

❑ 3) Security in Cloud :

❑ Cloud-based Cyber-Physical Systems (CCPS) achieve virtualization of network components using cyber-physical clouds

- Typical security attack in this landscape include HyperText Transfer Protocol (HTTP) and Extensible Markup Language (XML) DoS (HX-DoS) attack

- possible mitigation technique for networked DoS attack in virtualized systems is the implementation of firewall proxies, this will require an ACK to be received on the client side before an attacker's request can be forwarded

❑ Cloud intrusion: Mitigating against cloud intrusion is mainly achieved by building IDSs to work in conjunction with other control mechanisms in the cloud computing environment

SEOULTECH

7. PRIVACY CHALLENGES AND SOLUTIONS

- 1) Privacy: 1G - 3G :
  - 1G did not have suitable encryption mechanisms to ensure privacy Hence, private communications can be listened to and intercepted by the adversaries even from a far away distance
  - 2G systems did not have mutual authentication approaches between mobile phone subscribers and corresponding networks
  - 3G is observed that they are exposed to various attacks which were mainly targeting the identity and confidentiality of the subscribers such as IMSI paging attacks and AKA error message attacks[282], [280]

7. PRIVACY CHALLENGES AND SOLUTIONS

- 1) Privacy: 4G :
  - 4G networks are currently the most widely used mobile networks and have significant amount of enhancement in terms of data rates compared to the previous generations
  - Two of the most critical vulnerabilities being man-in-middle attacks, and eavesdropping attacks
  - This happens when adversaries set up fake base stations and act as real network base stations [16]
  - Several research works have proffered various possible solutions to mitigate man-in-the-middle attacks, popular among these is the use of cryptographic authentication protocols

7. PRIVACY CHALLENGES AND SOLUTIONS

- 1) Privacy: 5G :
  - The advent of new architectures, technologies and services in 5G networks will eventually generate higher privacy risks for users and other stakeholders as compared to previous generations
  - In addition, the integration of technologies such SDN, NFV, cloud/edge computing with the 5G eco-system will expose the networks to even more serious privacy challenges
  - various heterogeneous operators and service providers involved in the process may access personal data of the consumer with or without their consent
  - Therefore, end-to-end data confidentiality mechanisms are required to ensure data protection [284]

7. PRIVACY CHALLENGES AND SOLUTIONS

TABLE VIII
POTENTIAL PRIVACY CONCERNS FOR VARIOUS GENERATIONS

Privacy Concern	1G - 3G	4G	5G	XG	Relevant References
Lack of Authentication	M	H	H	H	[16], [138], [279], [296], [297]
Data Privacy Attacks	M	M	H	H	[16], [292], [284], [298]
Lack of Access Control	L	M	H	H	[14], [153], [299], [300]
Identity based Attacks	L	M	H	H	[279], [282], [281], [301], [295], [15]
Location based Attacks	L	M	H	H	[281], [292], [302], [303], [304], [305]
Cross-Border Privacy	H	H	H	H	[306], [298], [307], [308]
Legalization/Regulation and Governance	M	H	H	H	[307], [309], [308], [310]
Cloud based Privacy	L	M	H	H	[311], [312], [313], [314]
IoT based Privacy	L	M	H	H	[285], [286], [99], [311], [315], [316]
Context/AI based Privacy	NA	L	M	H	[317], [318], [319], [320], [321]

SEOULTECH

8. NEW DIMENSIONS IN SECURITY OF FUTURE NETWORKS: THE XG

- The Concept of XG:
  - For presenting future directions in network security, we define XG as a secure and autonomous network of numerous smart objects in smart environments
  - Hence, the real benefits of IoT, aiming the smart cities, can be realized when the communication systems are also smart enough to intelligently and autonomously deliver the necessary information generated and needed by IoT [330]
  - This needs i) intelligent communication systems that are responsive to the needs of IoT in real-time, and ii) provide coverage, in ideal conditions, everywhere. XG, in our view, will be the future network having these capabilities.

SEOULTECH

8. NEW DIMENSIONS IN SECURITY OF FUTURE NETWORKS: THE XG

- The Concept of XG:
  - Taking the network functions from software rather than hardware is one of the key trends in future wireless networks
  - changes in network policies and traffic conditions require complex configuration of firewalls
  - Technologies like SDN that enable programmability, centralize the network control, and equip the network management plane with global visibility of the network state can mitigate the risks involved in configurations and easily monitor the overall network traffic

SEOULTECH

8. NEW DIMENSIONS IN SECURITY OF FUTURE NETWORKS: THE XG

- The Concept of XG (Automation & AI):
  - Proactive security measures would require continuous intelligence gathering with AI, and using that intelligence o mitigate the possibility of security risks or lapses
  - Due to the complexity of next generation networks in terms of heterogeneity in networks, devices, applications and services, network functions must be automated [365], [366]

SEOULTECH

8. NEW DIMENSIONS IN SECURITY OF FUTURE NETWORKS: THE XG

- The Concept of XG (Blockchain):
  - Blockchain allows various stakeholders/entities to securely share and access the the critical data
  - most of the related work suggest that many of the security frameworks are based on centralized approaches
  - Centralized security systems, however, have challenges of scalability and single point of failures
  - Thus, blockchain based approaches in such cases can offer decentralized means of security and privacy mechanisms for IoT applications [385], [386]

SEOULTECH

8. NEW DIMENSIONS IN SECURITY OF FUTURE NETWORKS: THE XG

- The Concept of XG (Privacy):
  - As highlighted above, the XG technology will be key enabler of massive and critical applications in various domains such as smart health-care, industries automation, transportation/ Vehicle-to-Vehicle (V2V) and massive IoT
  - all other involved stakeholders such as infrastructure provider, network operator and service providers need to ensure that users' personal information should not leak during various phases such as user interaction with environment, identification process and data storage among others
  - In addition to technological solutions to protect the privacy, there will also be need of strong regulations and polices for such smart environments [397]

SEOULTECH

8. NEW DIMENSIONS IN SECURITY OF FUTURE NETWORKS: THE XG

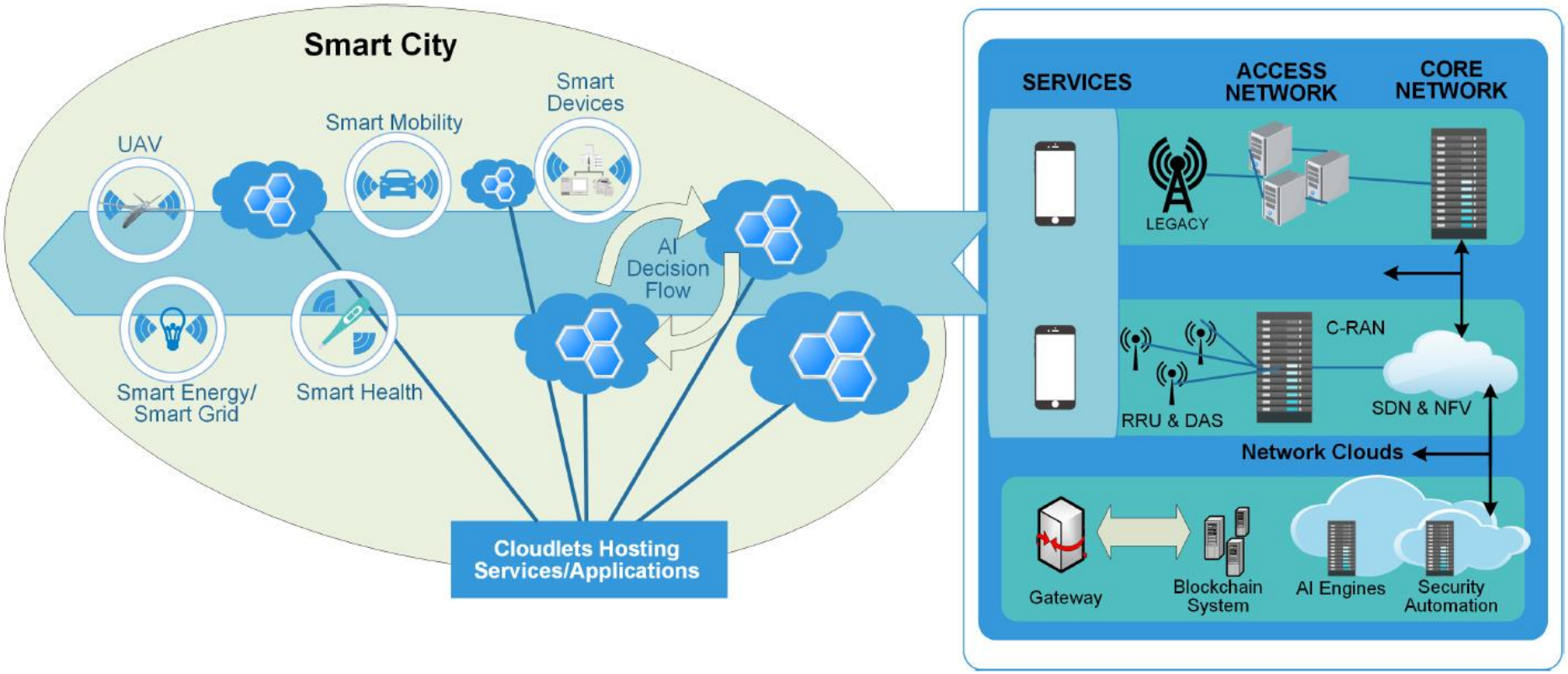


Fig. 9. Overview of security systems in communication networks for future cities (highlight AI, SDN, NFV in figure).

SEOULTECH

9. Conclusion & Opinion

- For integrating new things (IoT) and services into the network, 5G will use new technologies such as advanced cloud computing concepts (e.g. MEC), SDN, NFV, and massive MIMO etc

- These technologies have their own inherent security challenges which can further complicate the network security landscape

- The conglomeration of diverse devices, services, and new networking technologies does increase the security threat landscape, and thus new security solutions must be sought for efficient and secure connectivity

Thank you.

SEOULTECH

reference

Ahmad, Ijaz, et al. "Security for 5G and Beyond." IEEE Communications Surveys & Tutorials (2019).

SEOULTECH