Towards secure 5G networks: A Survey

Zhang, Shunliang, Yongming Wang, and Weihua Zhou. *Computer Networks* 162 (2019).

Presenter: Byoungjin Seok

2019-10-15

국립 서울과학기술대학교
SEOUL NATIONAL UNIVERSITY OF SCIENCE & TECHNOLOGY
Cryptography and
Information Security Lab

Table of Contents

I. Introduction

II. Lessons from 4G networks

III. Requirements for new scenarios and models

IV. Challenges from new technologies and paradigm

V. Solutions to secure the 5G system

VI. Future research opportunities

VII. Conclusion

VIII. Opinion

1. Introduction

- The fifth generation of mobile technology (5G)
  - is an end-to-end ecosystem that enables a fully mobile and connected society. (Hyper-Connectivity)

- the 5G system is supposed to support various new 3 use cases (eMBB, mMTC, URLLC).
  - enhanced Mobile BroadBand (eMBB)
    - ✓ Improvement of data communication speed
  - massive Machine Type Communications (mMTC)
    - ✓ Communications between machines which consists of various type and massive
  - Ultra-Reliable and Low Latency Communication (URLLC, also known as URLCC)
    - ✓ Low latency

1. Introduction

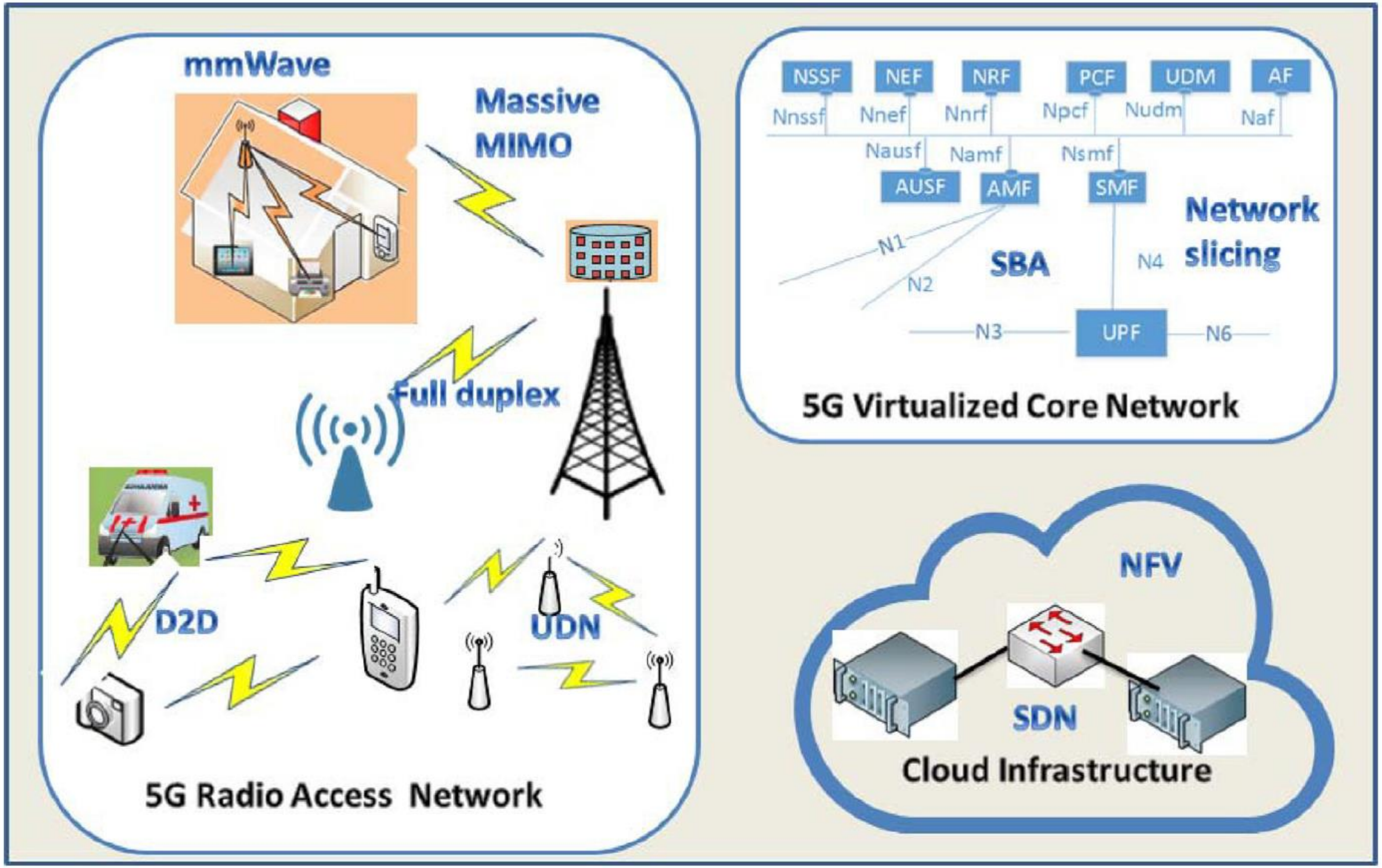


Fig. 1. The structure and key technologies of 5G systems.

Points of view in this paper:

1. 4G network vulnerabilities
2. New scenarios and models
3. New technologies

2. Lessons from 4G networks

- 5G system is evolved from 4G.

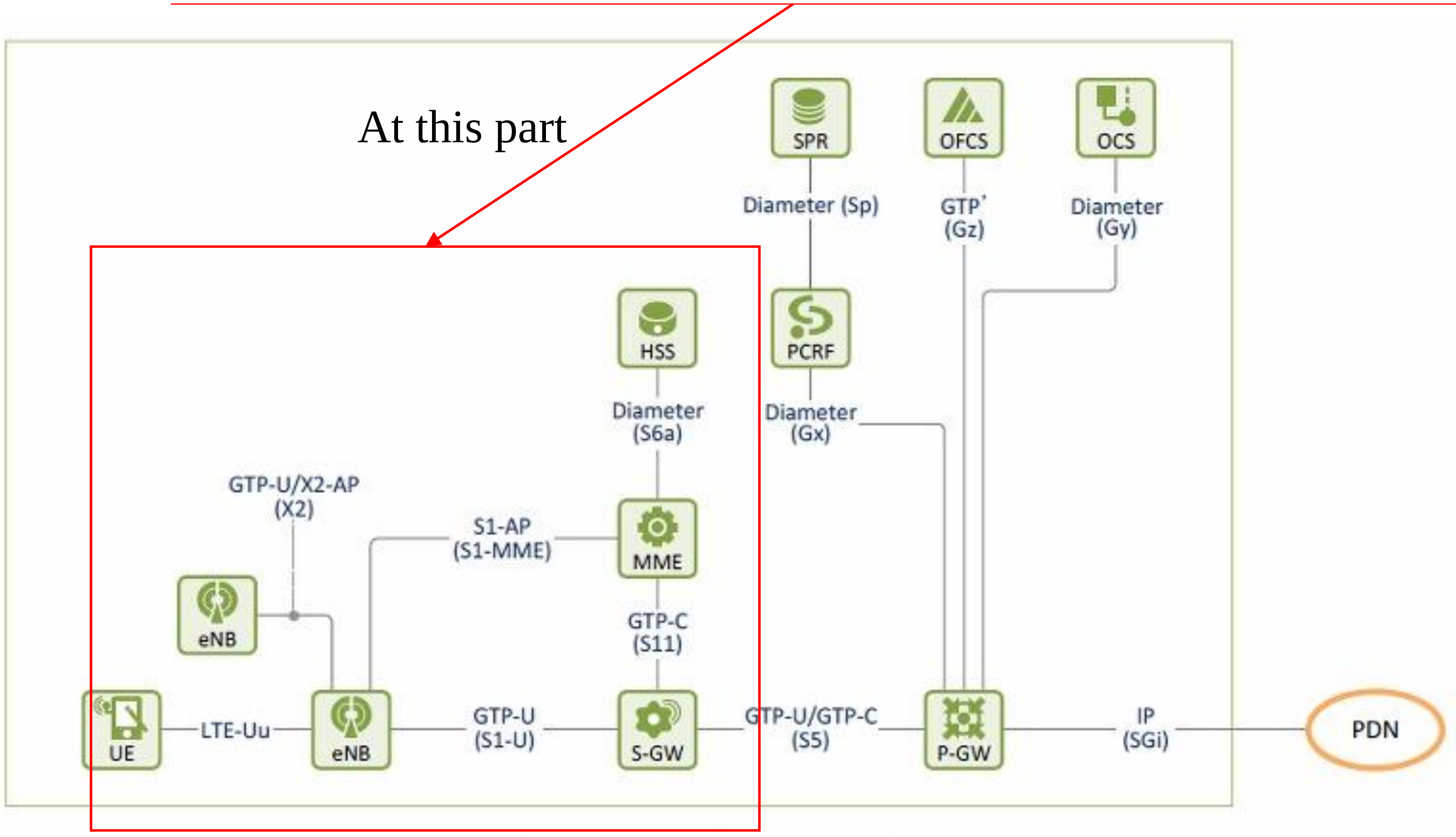
- 4G system has limitations of security as follows:
  - Limitations of architecture
  - User privacy leakage
  - Weak home network control
  - The risk of radio interface

- In this section, we discuss the limitations of 4G have to overcome during the 5G system design.

2. Lessons from 4G networks

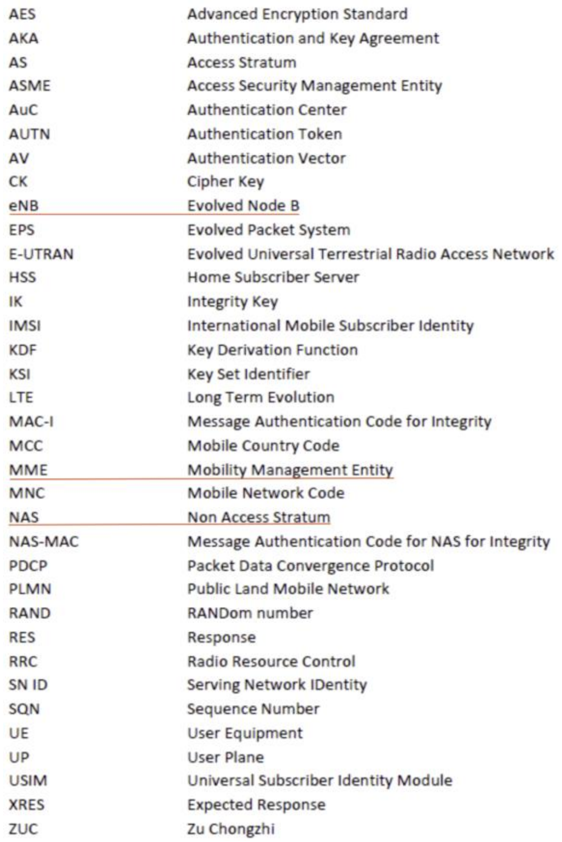
❖ Limitation of architecture

- ➢ is about authentication mechanism
  - ✓symmetric key-based Authentication and Key Agreement (AKA)



At this part

LTE 네트워크 참조 모델



AES	Advanced Encryption Standard
AKA	Authentication and Key Agreement
AS	Access Stratum
ASME	Access Security Management Entity
AuC	Authentication Center
AUTN	Authentication Token
AV	Authentication Vector
CK	Cipher Key
eNB	Evolved Node B
EPS	Evolved Packet System
E-UTRAN	Evolved Universal Terrestrial Radio Access Network
HSS	Home Subscriber Server
IK	Integrity Key
IMSI	International Mobile Subscriber Identity
KDF	Key Derivation Function
KSI	Key Set Identifier
LTE	Long Term Evolution
MAC-I	Message Authentication Code for Integrity
MCC	Mobile Country Code
MME	Mobility Management Entity
MNC	Mobile Network Code
NAS	Non Access Stratum
NAS-MAC	Message Authentication Code for NAS for Integrity
PDCP	Packet Data Convergence Protocol
PLMN	Public Land Mobile Network
RAND	RANDom number
RES	Response
RRC	Radio Resource Control
SN ID	Serving Network IDentity
SQN	Sequence Number
UE	User Equipment
UP	User Plane
USIM	Universal Subscriber Identity Module
XRES	Expected Response
ZUC	Zu Chongzhi

Ref: www.netmanias.com

2. Lessons from 4G networks

❖ Limitation of architecture

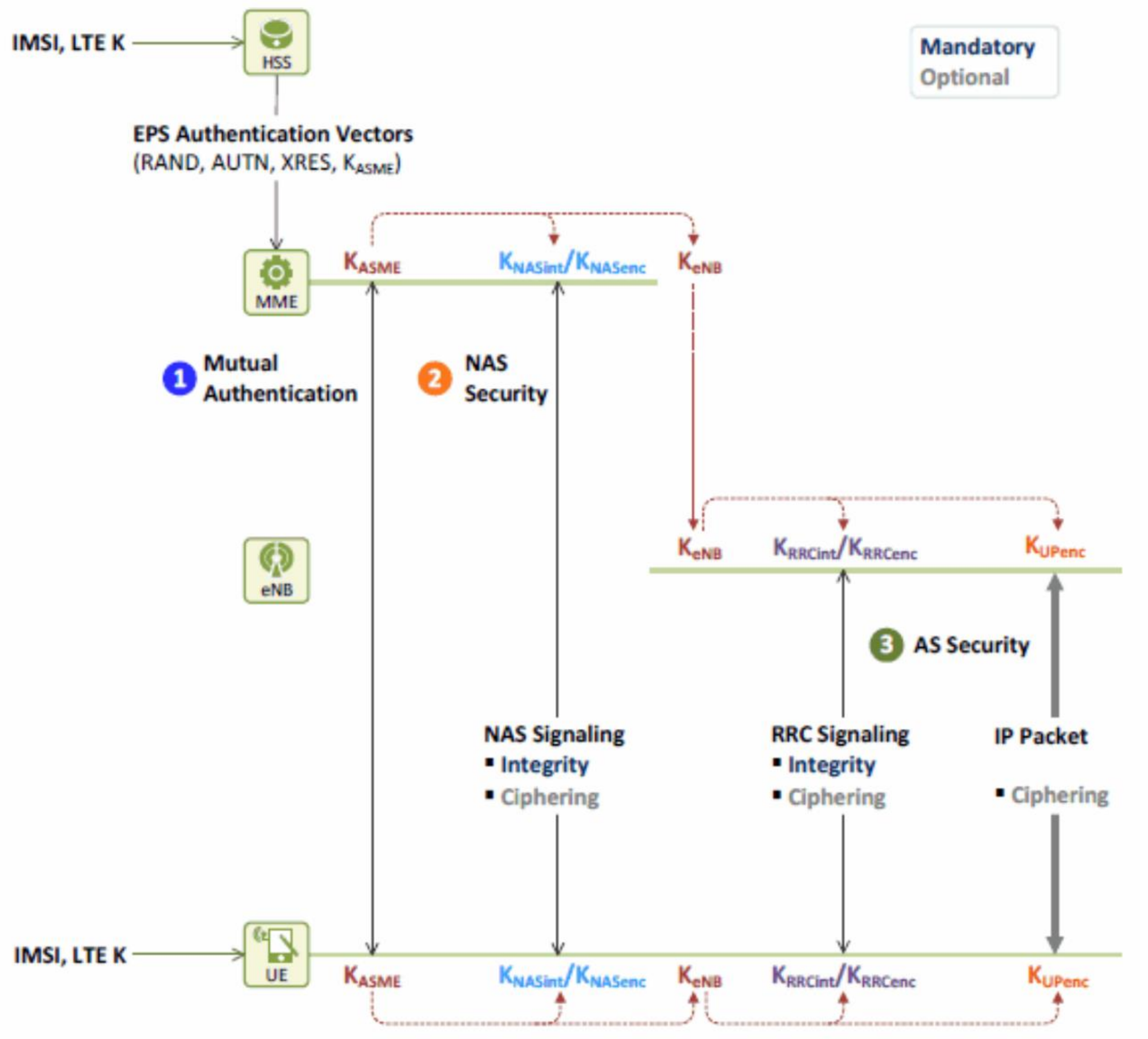


그림 1. LTE Security 범위 및 개념

- LTE Authentication: mutual authentication between UE and network.

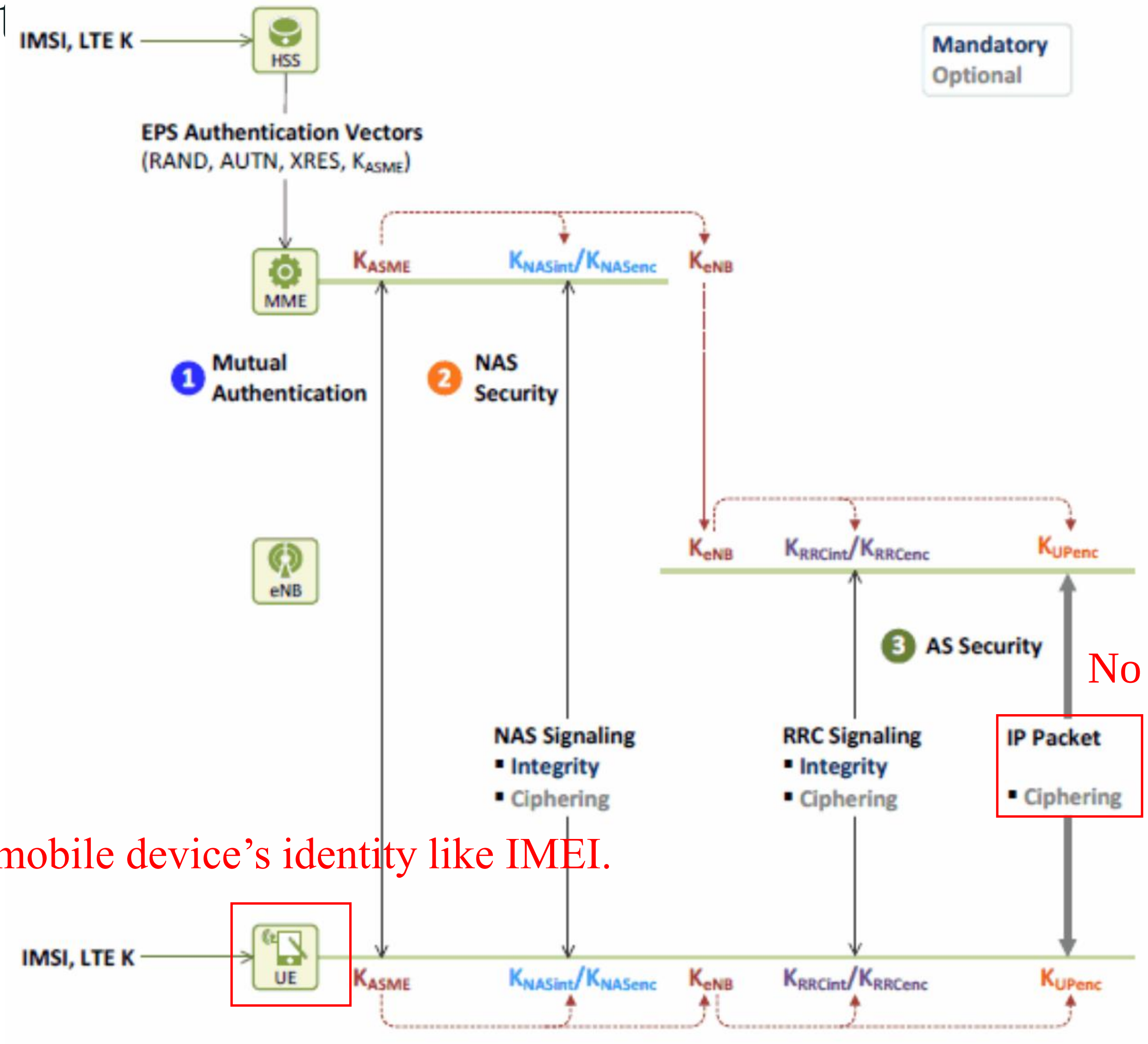
- NAS Security: Integrity and ciphering(encryption/decryption) for NAS signaling between UE and MME.

- AS Security: Integrity and ciphering (encryption/decryption) for RRC signaling, IP packet.

Ref: www.netmanias.com

2. Lessons from 4G networks

❖ Limitation of archi



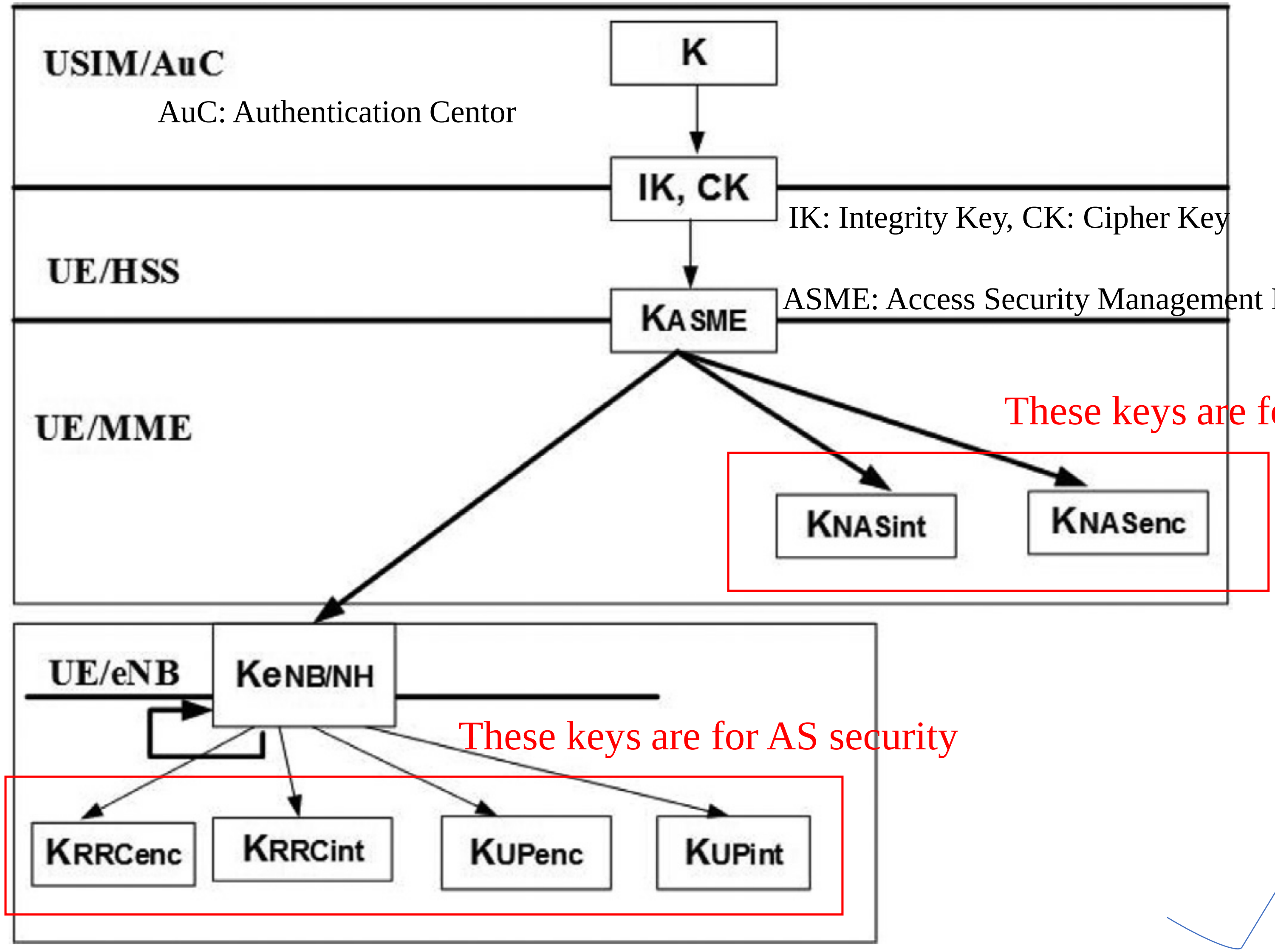
No integrity check

No authentication about mobile device's identity like IMEI.

그림 1. LTE Security 범위 및 개념

Ref: www.netmanias.com

2. Lessons from 4G networks



AuC: Authentication Centor

IK: Integrity Key, CK: Cipher Key

ASME: Access Security Management Entity

These keys are for NAS security

These keys are for AS security

Not completely independent

Fig. 2. 4G Key hierarchy.

2. Lessons from 4G networks

❖ User privacy leakage

- ➢ User privacy data: sensitive data, identifiers, mobility patterns, location information, usage patterns.
- ➢ 4G can protect against passive but active attack.

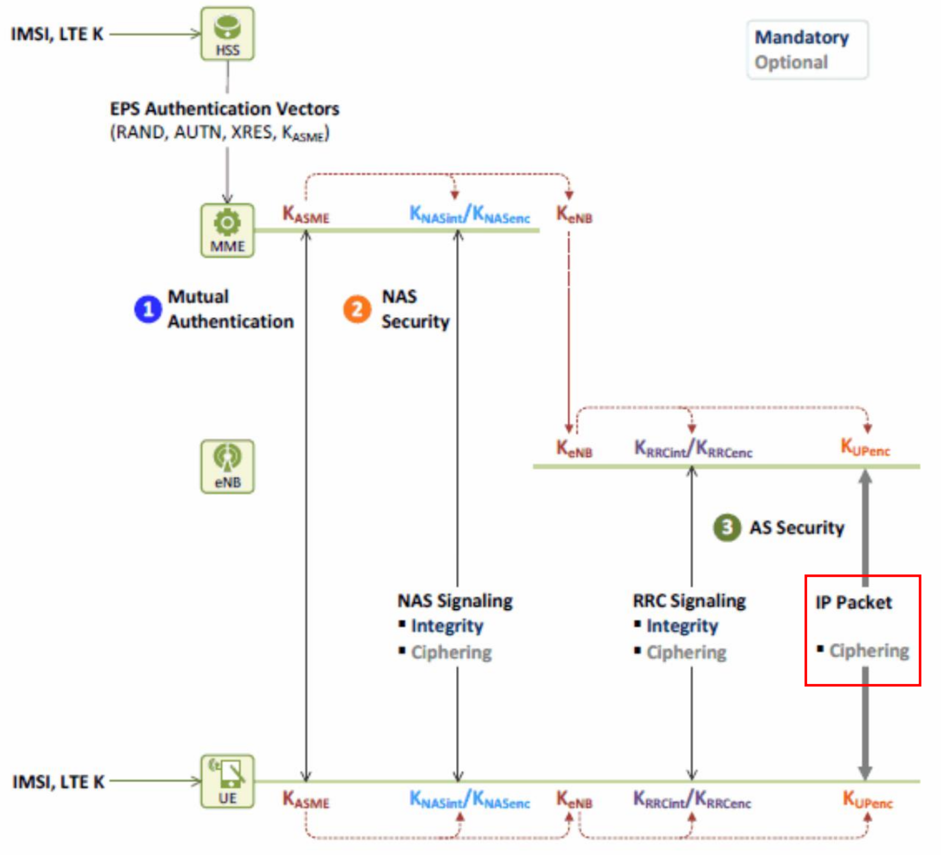


그림 1. LTE Security 범위 및 개념

Ciphering can protect against passive attack.
But, in 4G system, there is a function for avoiding abnormal state.
This function is that BS can require IMSI of UE with no encryption.

Active attacker may make fake BS, then require IMSI of UE.
It result in user privacy leakage.

2. Lessons from 4G networks

- Weak home network control
  - In roaming scenario of the 4G system, the MME in the visited network performs the mutual authentication with UE based on authentication vector from home network
  - However, it does not inform the authentication result to the home network.
  - It leads to a security loophole if trust relationship between the home network operator and visited network operator is abused for false charging.

2. Lessons from 4G networks

❖ The risk of radio interface

- ➢ Due to a loop hole in RRC idle mode
  - ✓RRC idle mode?
    - a UE in idle mode needs to listen to the broadcast channel to receive system information or paging.

- ➢But the UE does not verify if the message is broadcasted by a legal BS or a fake BS before reacting.
  - ✓It means that we can make the UE access the rogue cell if we can make fake BS.

    (It may results in DoS attack because the rogue cell can block all services of UE.)

- ➢Also, the security of 4G mainly depends on upper layer protocols, not physical layer.
  - ✓It has security issue about the jamming attack.

3. Requirements for new scenarios and models

❖ Diverse requirements from IoT (two scenarios)

- massive Machine Type Communications (mMTC): low-cost, low-power, long-range MTC and broadband MTC.
  - ✓ Such as smart wearable scenario, sensor networks for agriculture.
  - ✓ Because of resource-constrained IoT devices, the lightweight cryptographic algorithms and key management protocols are critical.
  - ✓ Security threats: data manipulation, rogue devices, device cloning, and DoS attack

Resource-constraint

- Ultra-Reliable and Low Latency Communication (URLLC): Applications with strong demand for real-time interaction.
  - ✓ Such as autonomous driving scenario.
  - ✓ Quick access and strong authentication protocol, high-speed cryptographic algorithms are expected to meet the low latency and high-reliability requirement.
  - ✓ Security threats: man-in-the-middle attacks, eavesdropping, DoS attack, and rogue devices

Ultra-reliable & ultra-real-time interaction

3. Requirements for new scenarios and models

- Typical threats of 5G IoT can be categorized into devices/user or network infrastructure.

- Typical threats to devices/user
  - Device Trigger: An attacker can impersonate the network or MTC server to send a trigger to an MTC device in the detached state. It leads to the MTC device is awakened and power is wasted.
  - Attack to devices: Many MTC devices are deployed remotely in the field. An adversary can exploit the physical access to the device and gain full control, which is known as node capture attacks.
  - Privacy leaking: Flaws in data integrity and confidentiality can cause privacy information leakage.

3. Requirements for new scenarios and models

❖ Typical threats to networks

- ➢Congestion control: Different access priority indicators are assigned to various MTC services and people-oriented services for efficient congestion control. Attackers may tamper with the priority assigned to MTC devices, which may make the congestion control invalid, and negatively impact people-oriented services.

- ➢Small data: Most optimization approaches such as piggyback have not fully considered security risks. It can be used by attacker for transporting malicious big data.

- ➢Signaling attack: To control the access of massive MTC devices to mobile networks, authentication and authorization mechanisms is usually enforced by mobile networks. The authentication of massive MTC device will bring significant signaling overhead. The attacker request authentication process repeatedly using compromised MTC devices.

3. Requirements for new scenarios and models

- New business model
  - 5G should be able to provide a future-proof technology platform allowing the evolution of existing business models.
    - ✓ Such as XaaS (Anything as a Service)
    - ✓ For partnership between network operators and vertical service providers

- New trust model
  - The trust relationship between users and applications is not covered by the mobile communication system. However, in 5G, the trust model with an additional actor, e.g. the vertical service provider. The new trust model is supported due to close cooperation between network operators and vertical service providers.
    - ✓ Efficient identity management, mutual authentication (including non-repudiation) are required.

3. Requirements for new scenarios and models

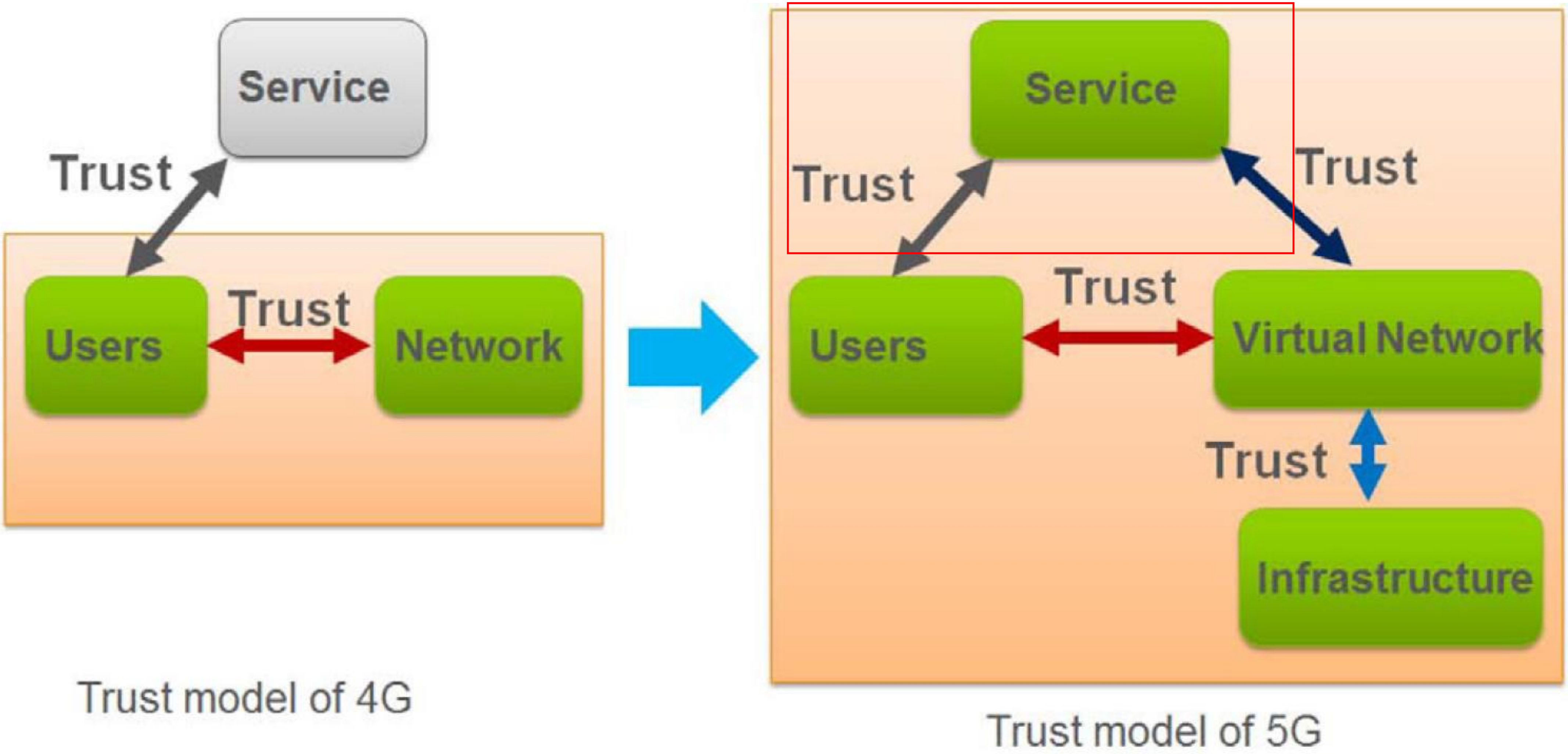


Fig. 3. The changing ecosystem and trust model.

4. Challenges from new technologies and paradigm

- In this section, we discuss security challenges from new technologies.

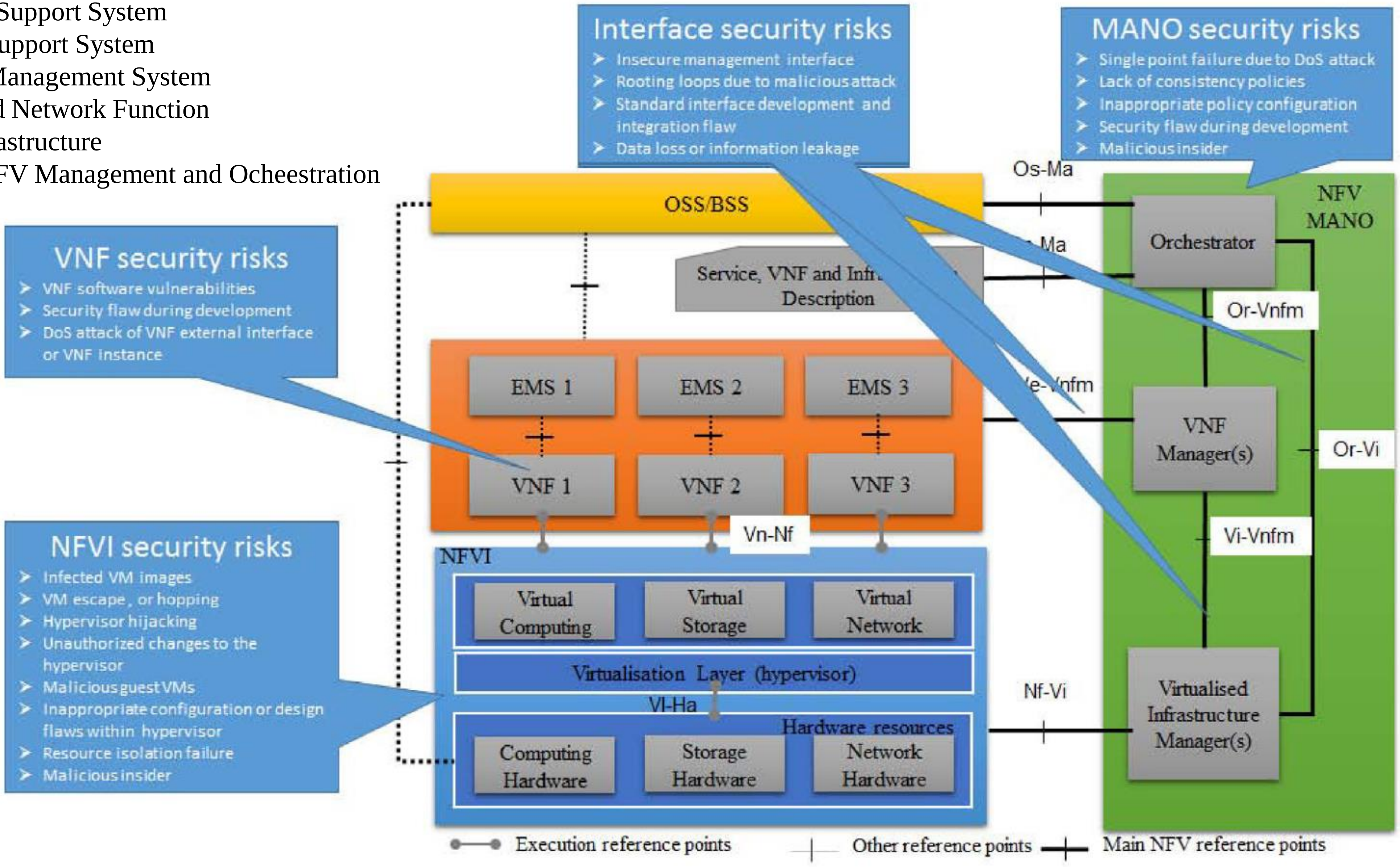
- The security challenges can be categorized as follows:
  - Network virtualization and slicing (NFV/Network slicing)
  - Software defined network (SDN)
  - Service based architecture (SBA)
  - Mobile edge computing (MEC)
  - D2D communications
  - 5G New radio technologies (M-MIMO, mmWave, UDN, FD)

4. Challenges from new technologies and paradigm

- Network virtualization
  - NFV (Network Function Virtualization)
    - NFV paradigm is introduced in 5G to consolidate multiple network functions onto software appliances, which run on a range of industry-standard hardware.
    - The decoupling of software from hardware
      - Advantages: reducing capital and operating expenditures, increasing the scalability, resilience of network service
    - But NFV have security challenges may come from NFV infrastructure (NFVI), NFV Management and orchestration (NFVO), and the interfaces between VNF, NFVI and NFVO.

4. Challenges from new technologies and paradigm

OSS: Operation Support System
BSS: Business Support System
EMS: Element Management System
VNF: Virtualized Network Function
NFVI: NFV Infrastructure
NFV MANO: NFV Management and Ocheestration



Interface security risks
- Insecure management interface
- Rooting loops due to malicious attack
- Standard interface development and integration flaw
- Data loss or information leakage

MANO security risks
- Single point failure due to DoS attack
- Lack of consistency policies
- Inappropriate policy configuration
- Security flaw during development
- Malicious insider

VNF security risks
- VNF software vulnerabilities
- Security flaw during development
- DoS attack of VNF external interface or VNF instance

NFVI security risks
- Infected VM images
- VM escape, or hopping
- Hypervisor hijacking
- Unauthorized changes to the hypervisor
- Malicious guest VMs
- Inappropriate configuration or design flaws within hypervisor
- Resource isolation failure
- Malicious insider

Fig. 4. NFV framework and typical security risks.

4. Challenges from new technologies and paradigm

❖ Network slicing

- ➢Based on cloud computing, network slicing is introduced to provide customized services in 5G. Meanwhile, it brings additional security challenges.

1. Isolation between different network slices.
   - Without good isolation, attackers may abuse the capacity elasticity of one slice to consume the resources of another target slice, which makes the target slice out of service.
2. Network Slice Selection Functions (NSSF)
   - is common to multiple slices.
   - it possible for attackers to eavesdrop on the data of the target slice by accessing to the common functions from another slice illegally.
3. It is possible that a UE can simultaneously access more than one network slice. The UE may be misused as a bridge to initiate security attacks from one slice to another.
4. The information exchanged between UE and network for slice selection may be tampered or forged. Moreover, attackers may eavesdrop user’s privacy information used during the network slice selection procedure.

4. Challenges from new technologies and paradigm

❖ Software-Defined Network (SDN)

- SDN is regarded as an emerging network architecture to facilitate innovation in communication networks and simplify network management.
- The essential thinking is to provide programmability through decoupling the control functions from the data forwarding plane.
- Three layers
  - ✓Application plane contains various SDN applications such as security services
  - ✓Control plane maintains a global view of network, provides data plane abstractions to SDN applications and generates data forwarding policy based requirement from applications
  - ✓Data plane is used to forward traffic flows according to policies from the control plane to provide required network services.
- The logically centralized SDN controller can become the single point of failure and disrupt the whole network in the case of security compromises.

4. Challenges from new technologies and paradigm

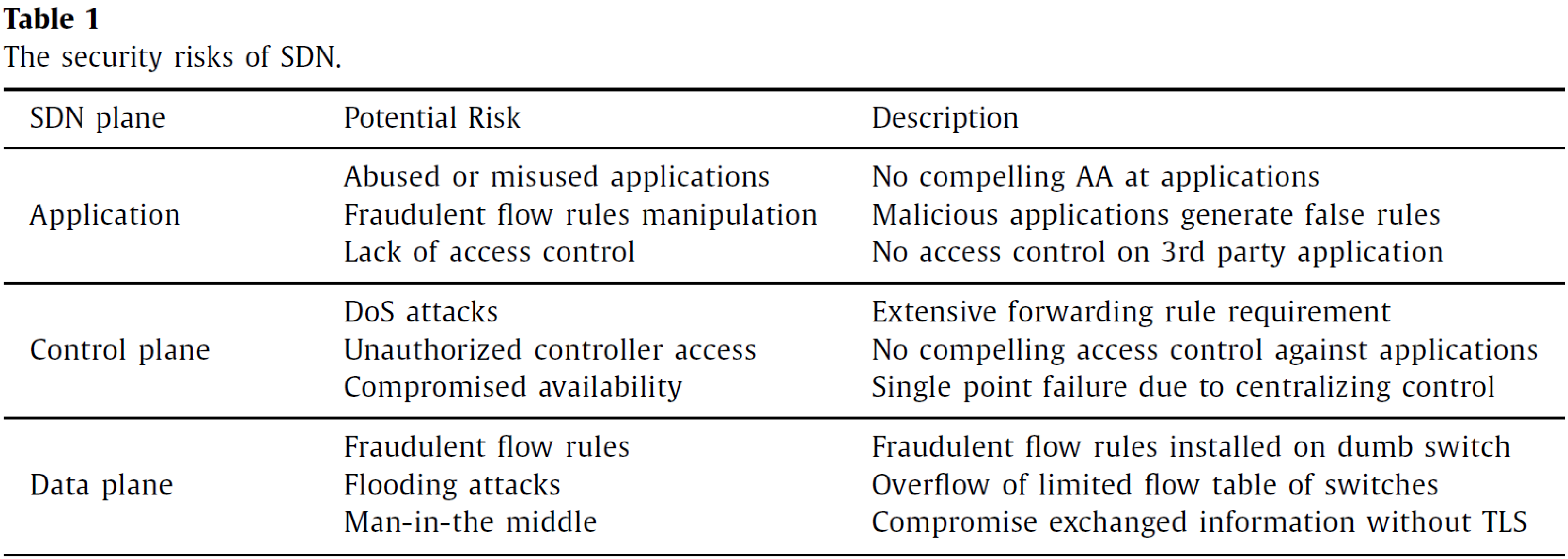


Table 1
The security risks of SDN.

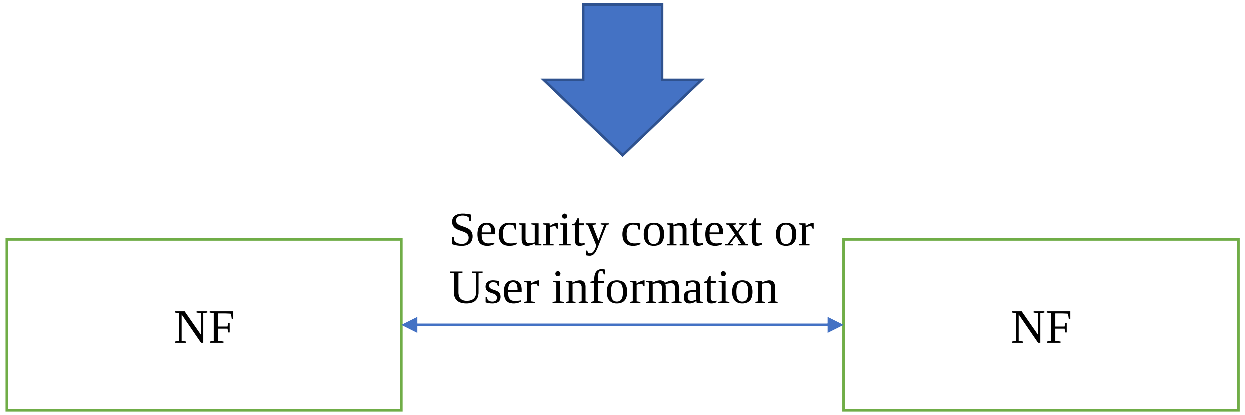
SDN plane	Potential Risk	Description
Application	Abused or misused applications Fraudulent flow rules manipulation Lack of access control	No compelling AA at applications Malicious applications generate false rules No access control on 3rd party application
Control plane	DoS attacks Unauthorized controller access Compromised availability	Extensive forwarding rule requirement No compelling access control against applications Single point failure due to centralizing control
Data plane	Fraudulent flow rules Flooding attacks Man-in-the middle	Fraudulent flow rules installed on dumb switch Overflow of limited flow table of switches Compromise exchanged information without TLS

4. Challenges from new technologies and paradigm

❖ Service based architecture (SBA)

- ➢SBA is the natural step that enables 5G network functionality to become more granular and decoupled, which allows for the flexible and customized service provision.

- ➢If there is no secure protection including confidentiality, integrity, authentication, authorization, then attacker can attack user privacy or security context between NFs.



NF

Security context or User information

NF

4. Challenges from new technologies and paradigm

❖ Mobile Edge Computing (MEC)

- ➢Given that many mission-critical IoT services such as virtual reality (VR), augmented reality (AR) applications are expected to be supported by 5G, the MEC paradigm is introduced to 5G network architecture.

- ➢But there are some security challenges
  - ✓Physical security protection
    - e.g. a base station in 5G RAN.
  - ✓Trust management in open platform
    - The trust management functions located at different trust domains should be able to exchange compatible trust information with each other as less latency as possible.
  - ✓Data security and privacy protection
    - the security and privacy of outsourcing data is still a fundamental issue of edge computing.

4. Challenges from new technologies and paradigm

❖ D2D communications

- Direct links, not cellular links, between devices are exploited for providing proximity and diversity gains.

- Security challenges
  - ✓Impersonation
  - ✓Eavesdropping and Fabrication
  - ✓Privacy sniffing
  - ✓Jamming
  - ✓Free-Riding
  - ✓Location-spoofing

4. Challenges from new technologies and paradigm

- 5G new radio technologies
  - M-MIMO, mmWave, UDN, Full-duplex
  - Very core technologies for 5G networks.
  - But, these technologies can make stronger the attacker too.
  - Example:
    - ✓ an eavesdropper armed with FD capability can also actively attack the communication process while eavesdropping.

5. Solutions to secure the 5G system

- Table 2 summarizes 5G specific security challenges and corresponding countermeasures.
  - We already mentioned security challenges. From now, we discuss the corresponding countermeasures.

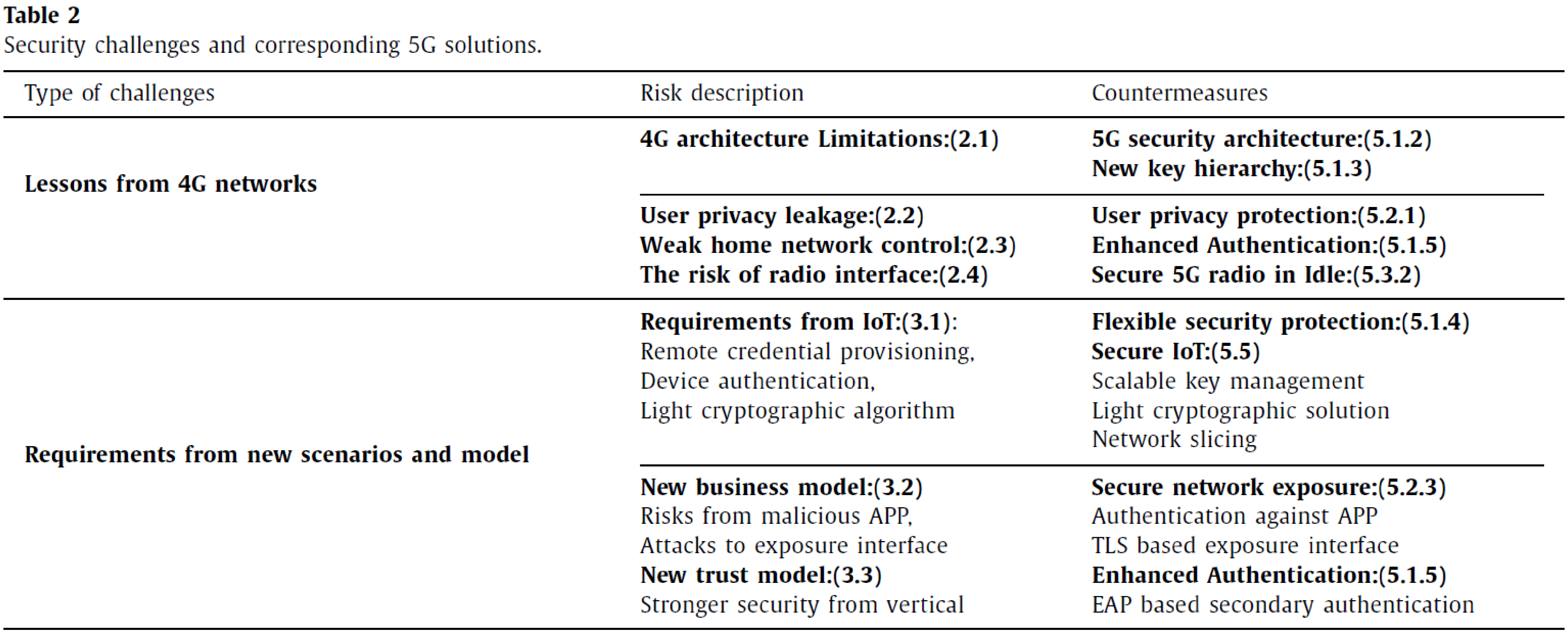
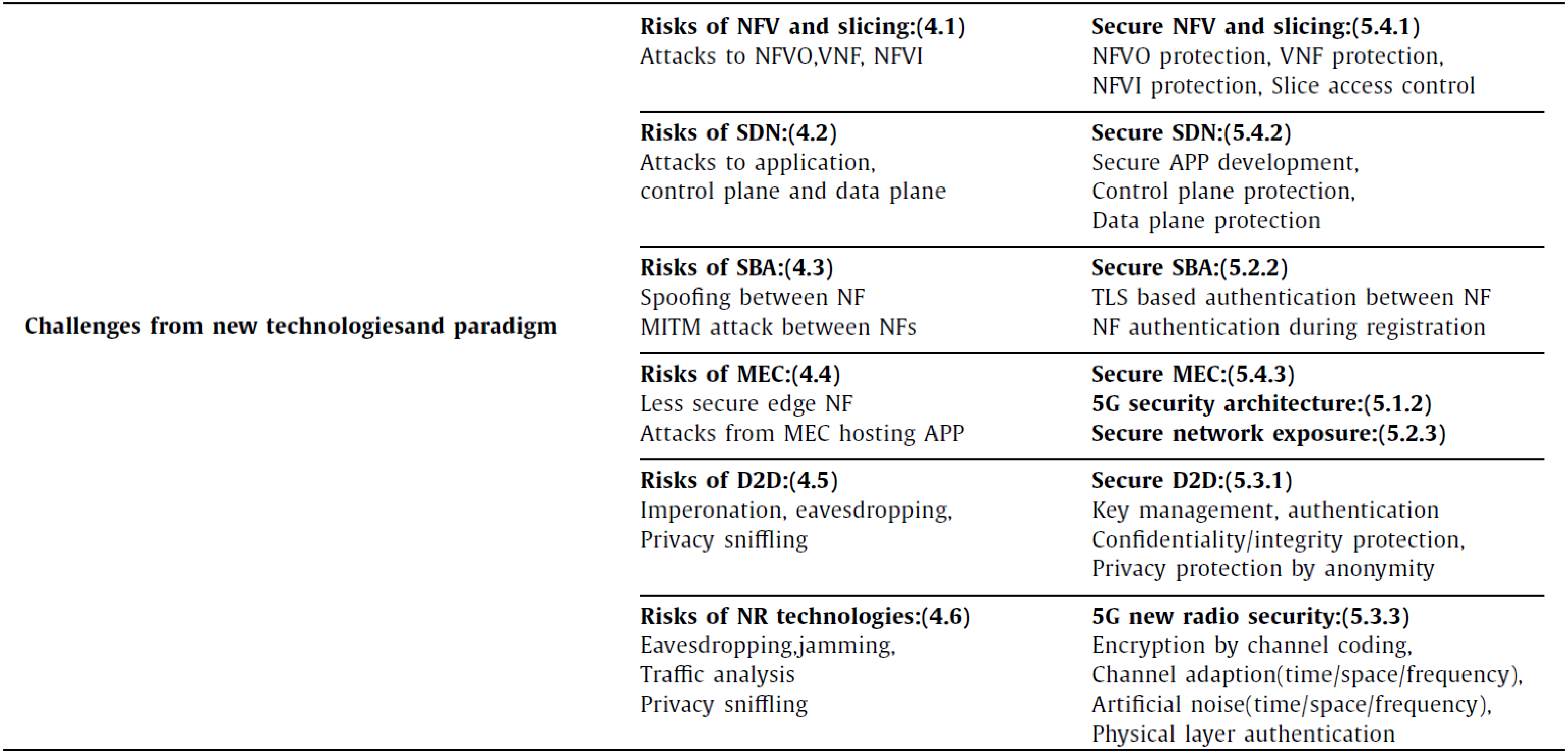


Table 2
Security challenges and corresponding 5G solutions.

Type of challenges	Risk description	Countermeasures
Lessons from 4G networks	**4G architecture Limitations:**(2.1)	**5G security architecture:**(5.1.2) **New key hierarchy:**(5.1.3)
	User privacy leakage:(2.2) **Weak home network control:**(2.3) **The risk of radio interface:**(2.4)	**User privacy protection:**(5.2.1) **Enhanced Authentication:**(5.1.5) **Secure 5G radio in Idle:**(5.3.2)
Requirements from new scenarios and model	**Requirements from IoT:**(3.1): Remote credential provisioning, Device authentication, Light cryptographic algorithm	**Flexible security protection:**(5.1.4) **Secure IoT:**(5.5) Scalable key management Light cryptographic solution Network slicing
	New business model:(3.2) Risks from malicious APP, Attacks to exposure interface **New trust model:**(3.3) Stronger security from vertical	**Secure network exposure:**(5.2.3) Authentication against APP TLS based exposure interface **Enhanced Authentication:**(5.1.5) EAP based secondary authentication

5. Solutions to secure the 5G system



Challenges from new technologiesand paradigm	**Risks of NFV and slicing:(4.1)** Attacks to NFVO,VNF, NFVI	**Secure NFV and slicing:(5.4.1)** NFVO protection, VNF protection, NFVI protection, Slice access control
	Risks of SDN:(4.2) Attacks to application, control plane and data plane	**Secure SDN:(5.4.2)** Secure APP development, Control plane protection, Data plane protection
	Risks of SBA:(4.3) Spoofing between NF MITM attack between NFs	**Secure SBA:(5.2.2)** TLS based authentication between NF NF authentication during registration
	Risks of MEC:(4.4) Less secure edge NF Attacks from MEC hosting APP	**Secure MEC:(5.4.3)** **5G security architecture:(5.1.2)** **Secure network exposure:(5.2.3)**
	Risks of D2D:(4.5) Imperonation, eavesdropping, Privacy sniffling	**Secure D2D:(5.3.1)** Key management, authentication Confidentiality/integrity protection, Privacy protection by anonymity
	Risks of NR technologies:(4.6) Eavesdropping,jamming, Traffic analysis Privacy sniffling	**5G new radio security:(5.3.3)** Encryption by channel coding, Channel adaption(time/space/frequency), Artificial noise(time/space/frequency), Physical layer authentication

5. Solutions to secure the 5G system

❖ Overall 5G security framework (outlined by 3GPP at Release 15).

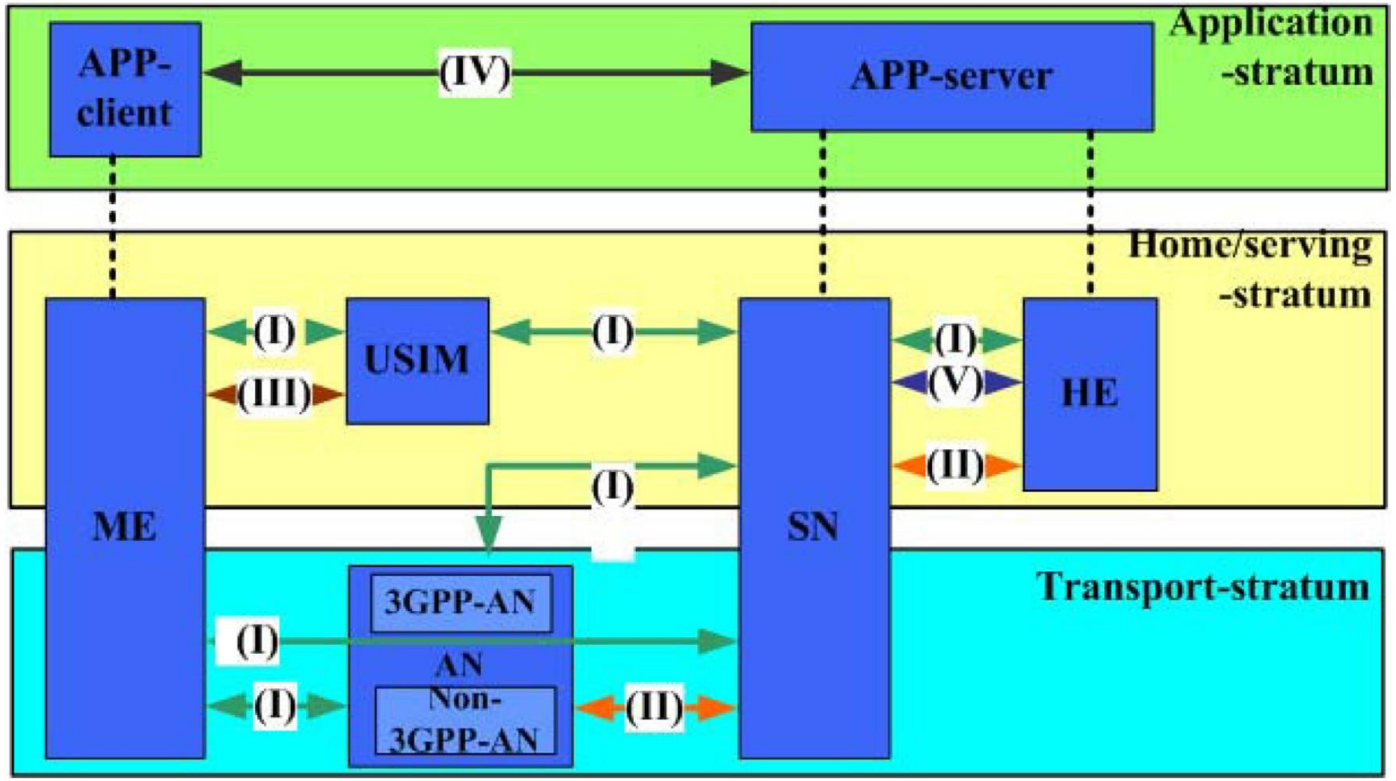
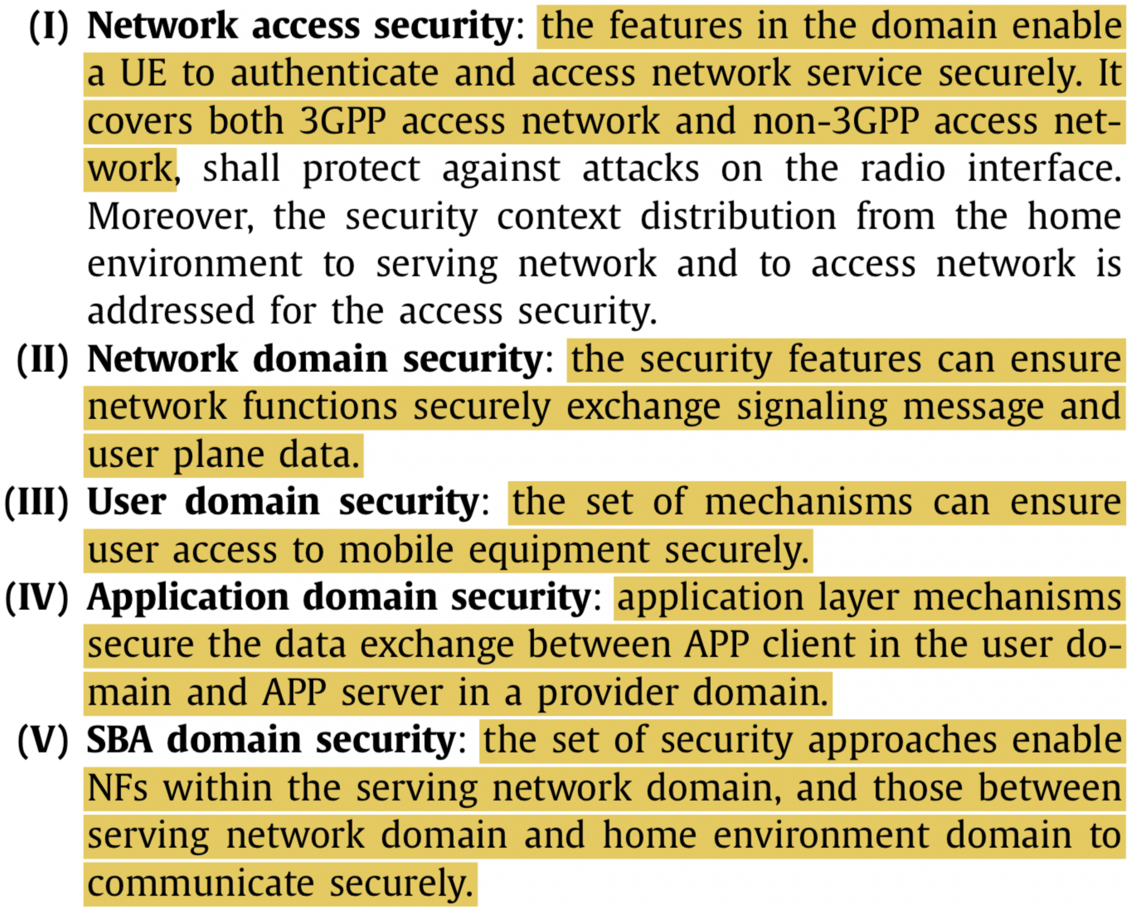


Fig. 5. Security framework of 5G system.

HE: Home Environment
SN: Serving Network
ME: Mobile Equipment



(I) **Network access security**: the features in the domain enable a UE to authenticate and access network service securely. It covers both 3GPP access network and non-3GPP access network, shall protect against attacks on the radio interface. Moreover, the security context distribution from the home environment to serving network and to access network is addressed for the access security.

(II) **Network domain security**: the security features can ensure network functions securely exchange signaling message and user plane data.

(III) **User domain security**: the set of mechanisms can ensure user access to mobile equipment securely.

(IV) **Application domain security**: application layer mechanisms secure the data exchange between APP client in the user domain and APP server in a provider domain.

(V) **SBA domain security**: the set of security approaches enable NFs within the serving network domain, and those between serving network domain and home environment domain to communicate securely.

5. Solutions to secure the 5G system

❖Example of non-roaming scenario (based on current discussion and 3GPP Release 15)

ARPF: Authentication Credential Repository and Processing Function
UDM: Unified Data Management
AUSF: Authentication Server Function
SEAF: Security Anchor Function
SMF: Session Management Function
AMF: Access and mobility Management Function
PCF: Policy Control Function

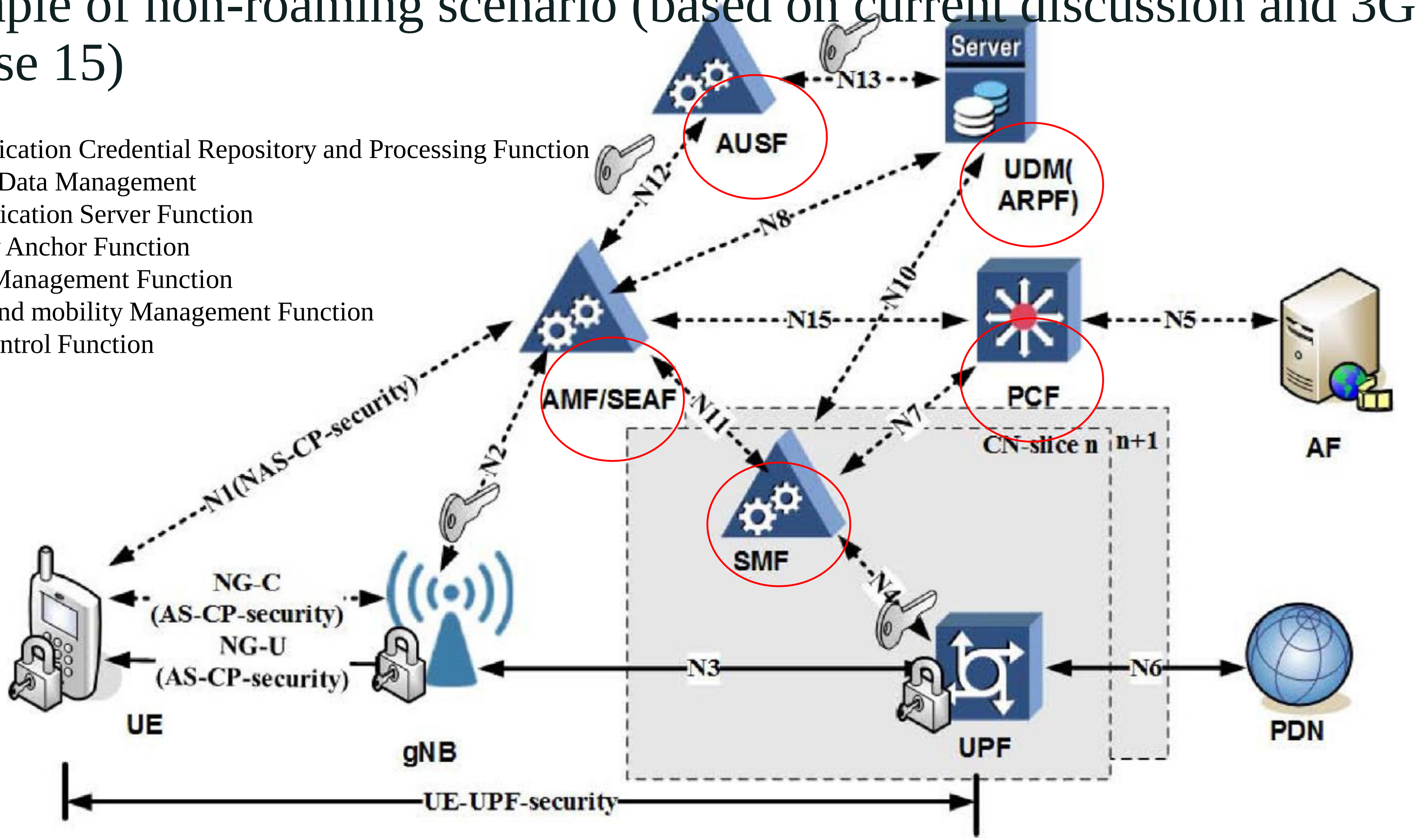


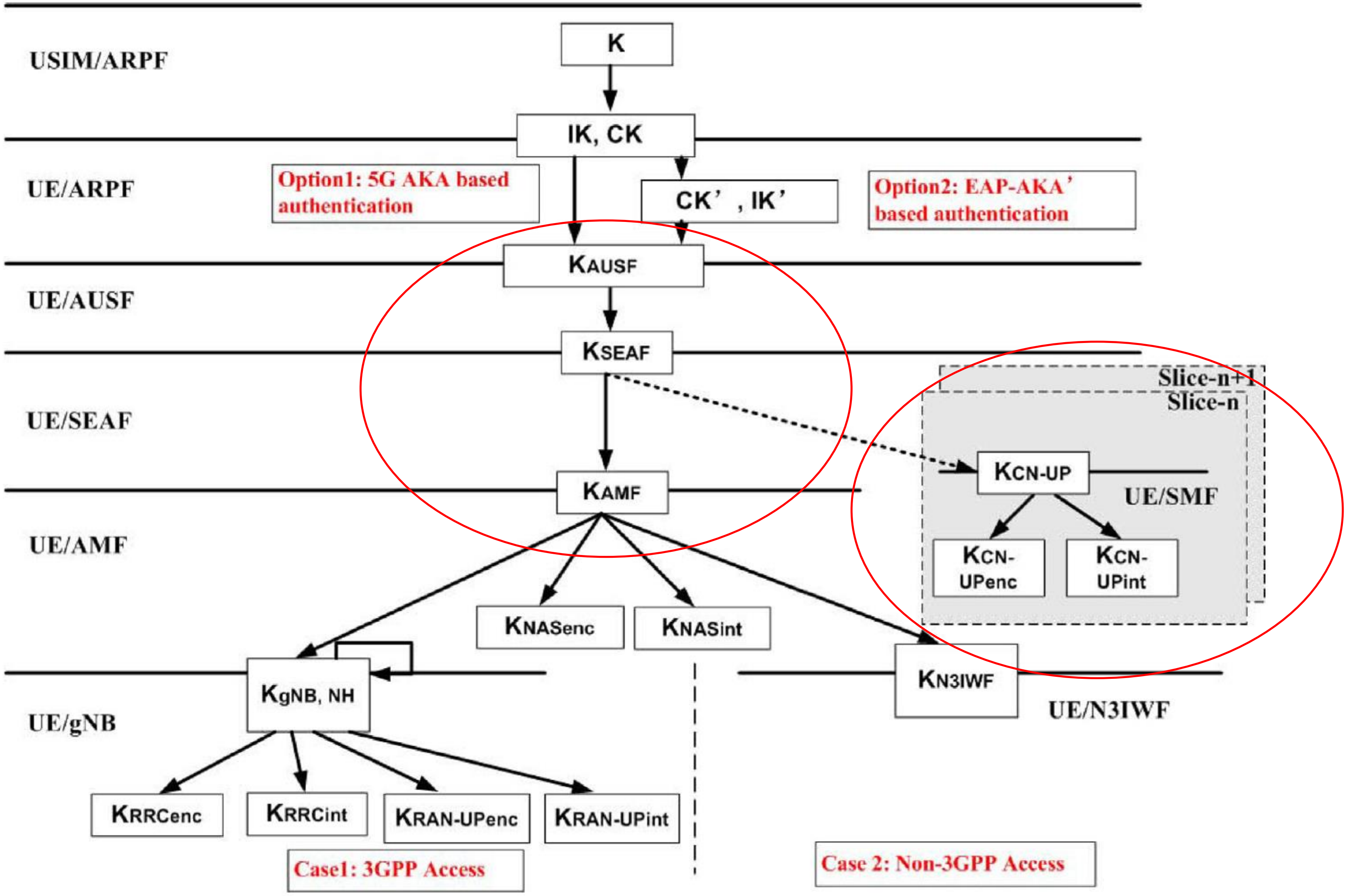
Fig. 6. Non-roaming 5G security architecture.

5. Solutions to secure the 5G system

- In 5G secure architecture,
  - ARPF with UDM is defined to manage the long-term security credential used for authentication and generate authentication vectors.
  - AUSF is introduced to perform primary authentication with UE for connections with different access networks (i.e. the same AUSF can be sued to authenticate a UE from 3GPP access and non-3GPP access).
    - ✓ AUSF is separated from SMF and AMF. The design makes it possible to store keys resulting from the authentication process in a secure location even if AMF functions are placed at the less secure network edge.
  - SEAF is introduced to support the primary authentication process by interaction with UE and AUSF.
  - AMF works together with UE for NAS signaling confidentiality and integrity protection.
  - SMF is defined to perform session management, select and control of UPF, provide traffic steering policy and potential security policy.
  - PCF is to realize customized security protection. PCF may generate security policies based on application level.
- The main point is that each component is separated according to their main functionality (differently in 4G).

5. Solutions to secure the 5G system

❖ Key hierarchy for 5G



Slice-specific key
(This part is
potential solution.)

Fig. 7. Potential Key hierarchy for 5G.

5. Solutions to secure the 5G system

- Flexible security protection
  - The NAS signaling data protection is provided by UE and AMF. The AS level signaling data protection is provided by UE and gNB at packet data convergence protocol (PDCP) layer including confidentiality and integrity (In 4G, confidentiality only).
  - Different integrity and confidentiality protection can be provided to different user plane traffic according to the security policy from control plane functions.

- Enhanced authentication
  - There are two authentications (primary, secondary).
    - ✓ The primary authentication is used to establish the trust between UE and network, which is similar to that of the 4G system.
    - ✓ Depending on the requirement of the 3rd party service providers, the secondary authentication may be performed between the UE and the DN-AAA server in the external data network.

AAA: Authentication, Authorization and Accounting

  - The authentication result is reported to the UDM in the home network.

5. Solutions to secure the 5G system

❖ Core network security

- User privacy protection
  - ✓ combined solution of below two types have been developed (by 3GPP Release 15)
    - Protect the permanent user identifier via encryption (encrypting IMSI).
    - Concealing permanent privacy information.
  - ✓ SUCI (Subscription Concealed Identifier), SIDF(Subscription Identifier De-concealing Function)
    - One-time-user identifier (based on asymmetry-key generation, specifically ECC)
  - ✓ See the figure 8 on next page.

5. Solutions to secure the 5G system

Generating one-time-use identifier (Public-private key pair of ECC)

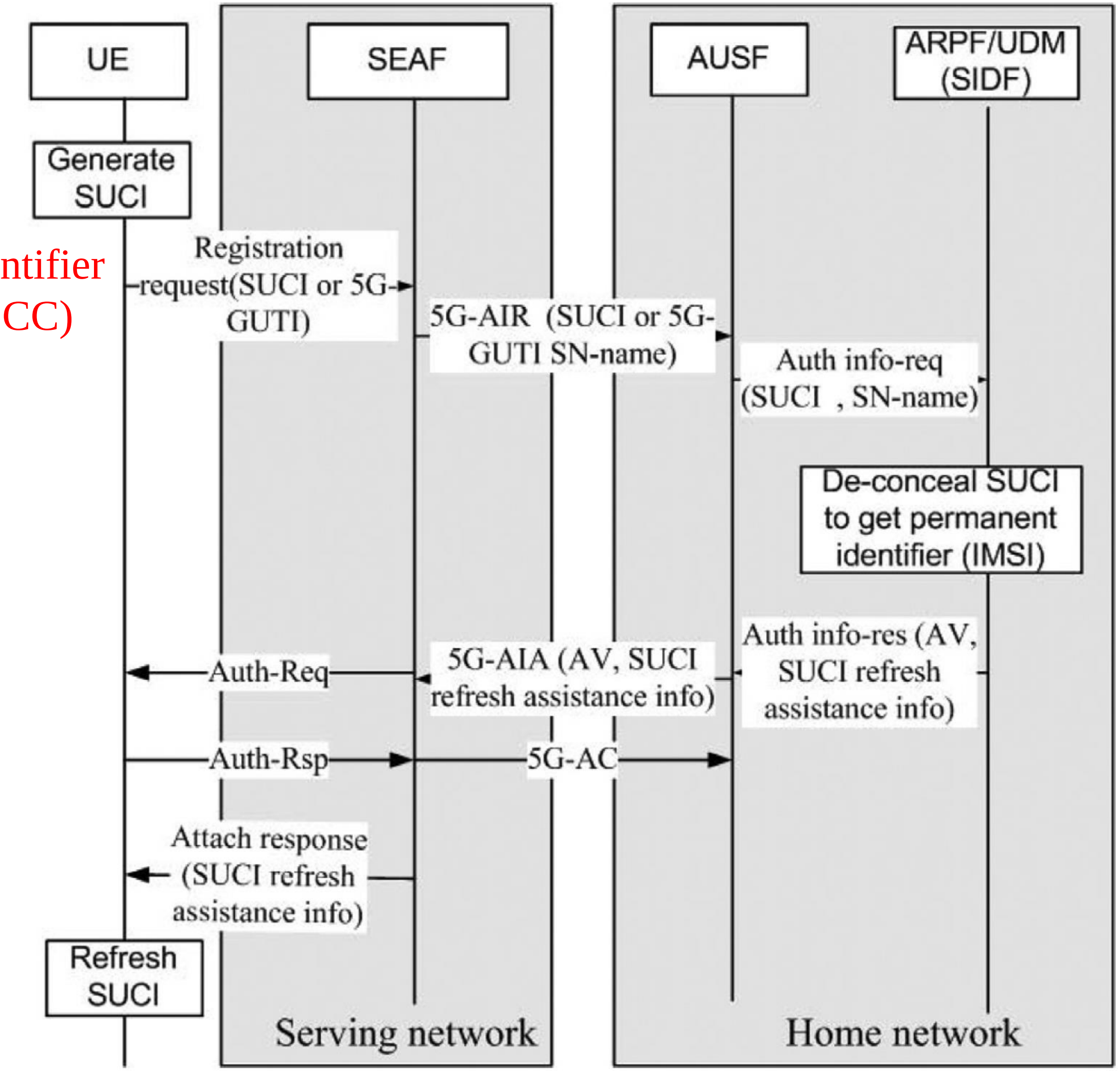

UE
SEAF
AUSF
ARPF/UDM (SIDF)
Generate SUCI
Registration request(SUCI or 5G-GUTI)
5G-AIR (SUCI or 5G-GUTI SN-name)
Auth info-req (SUCI , SN-name)
De-conceal SUCI to get permanent identifier (IMSI)
Auth info-res (AV, SUCI refresh assistance info)
5G-AIA (AV, SUCI refresh assistance info)
Auth-Req
Auth-Rsp
5G-AC
Attach response (SUCI refresh assistance info)
Refresh SUCI
Serving network
Home network

Fig. 8. Subscriber privacy protection process.

5. Solutions to secure the 5G system

- Core network security
  - Secure service based network interface & Secure network exposure
    - ✓ Authentication and authorization mechanisms are required.
      - Authentication: TLS or token based authentication
      - Authorization: OAuth 2.0 framework (NRF: Authentication server, NF service consumer: client, NF service producer: resource server)

5. Solutions to secure the 5G system

- Secure 5G radio access network
  - D2D security protection
    - ✓ Key management – symmetric key based, asymmetric based, group-key based management, and physical layer based key generation(using randomness of wireless channel)
    - ✓ Authentication and authorization – Diffie-hellman key agreement, digital signature, identity based cryptography (but it has a key escrow problem)
    - ✓ Confidentiality and integrity – cryptographic techniques, physical device's noise(interference of D2D)
  - Privacy security protection
    - ✓ Access control – credential and reputation-based trust relation
    - ✓ Anonymity – remove the association between private information and the individual by hiding the user identity
    - ✓ Obfuscation – can be used provide location privacy

5. Solutions to secure the 5G system

- Secure 5G radio access network
  - Secure 5G radio in idle mode
    - ✓Public-key based authentication (digital signature)
    - ✓But it may leads to increased signaling overhead.
  - 5G new radio security
    - ✓Using physical device’s noise (PHY-SEC).
    - ✓Compared to upper layer mechanisms, PHY-SEC provides many advantages in terms of performance and efficiency (It is not affected by computational overhead).
    - ✓Using channel state information (CSI), received signal strength (RSS), phase information to generate and share secret keys.

5. Solutions to secure the 5G system

❖5G radio new technologies security (M-MIMO, mmWave, FD, HetNet, Jamming)

- ➢M-MIMO: The pilot contamination attack not only reduces the achievable secrecy capacity significantly but also is difficult to detect. Potential methods for detecting active attacks have been investigated [12]. Further study is needed to resist active attacks. ([12]: Using physical layer security)
- ➢mmWave: The directional beamforming antenna, which results in more focused array gain, is beneficial for improving the secrecy performance of mmWave networks.
- ➢Full duplex (FD): It brings both opportunities and challenges to 5G security
  - ✓FD enables the receiver to generate additional artificial noise to interfere with eavesdroppers.
  - ✓But, active FD eavesdroppers equipped with multiple antennas can simultaneously eavesdrop and attack the legitimate communication.

5. Solutions to secure the 5G system

- ❖ 5G radio new technologies security (M-MIMO, mmWave, FD, HetNet, Jamming)
  - ➢ HetNet:
    - ✓ The policy for a user to establish communication channels among different types of nodes under security constraints is more challenging.
      - Security-oriented mobile association policies
    - ✓ Inter-and intra-cell interference
      - There is a trade-off between secrecy and connection probabilities in terms of association threshold, base station density, and power allocation between the signal and artificial noise.
    - ✓ User location issues
      - Farhang et al. [14] proposed a differential private Gale-Shapley algorithm to prevent the leakage of user location information.
  - ➢ Jamming:
    - ✓ Jamming can be used to protect communications from eavesdropping
      - The concept of utilizing AN or jamming signals to enhance secrecy was proposed that generating AN on both side transmitter, receiver, and trusted relay nodes to confuse eavesdroppers.

5. Solutions to secure the 5G system

- 5G infrastructure security
  - Secure virtualized and sliced networks
    - ✓ Secure NFVI – secure boot using trusted computing and crash protection, performance isolation, regularly update to latest security patches.
    - ✓ Secure VNF – cryptographically sign VNF images.
    - ✓ Secure MANO – secure orchestrator, identity and role-based access control (especially, it is recommended to separate the admin roles into multiple distributed entities.)
    - ✓ Secure inter-connection interfaces – TLS or IPSec
    - ✓ Avoiding a UE being abused as a bridge – slice authentication and authorization

5. Solutions to secure the 5G system

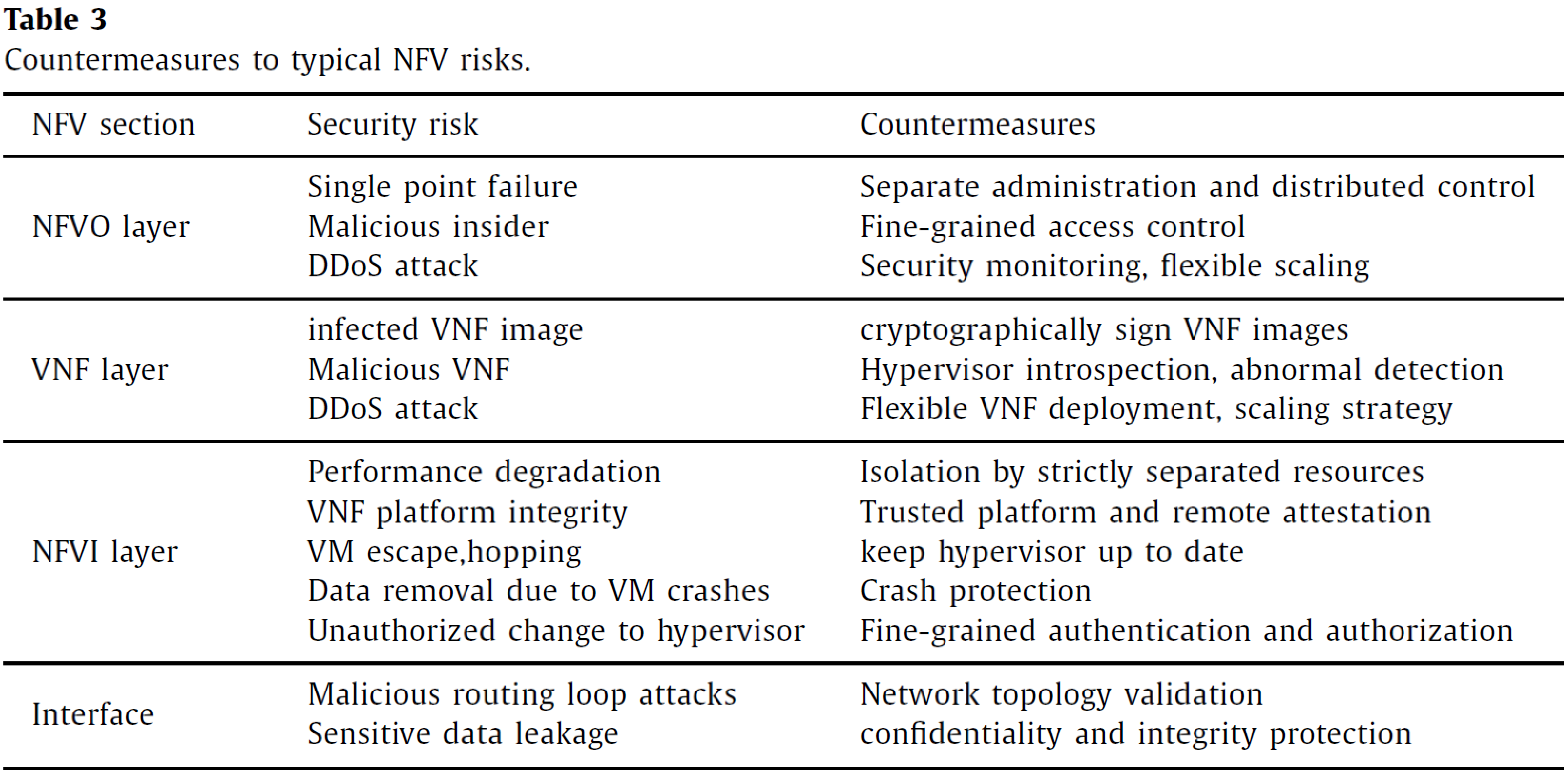


Table 3
Countermeasures to typical NFV risks.

NFV section	Security risk	Countermeasures
NFVO layer	Single point failure Malicious insider DDoS attack	Separate administration and distributed control Fine-grained access control Security monitoring, flexible scaling
VNF layer	infected VNF image Malicious VNF DDoS attack	cryptographically sign VNF images Hypervisor introspection, abnormal detection Flexible VNF deployment, scaling strategy
NFVI layer	Performance degradation VNF platform integrity VM escape,hopping Data removal due to VM crashes Unauthorized change to hypervisor	Isolation by strictly separated resources Trusted platform and remote attestation keep hypervisor up to date Crash protection Fine-grained authentication and authorization
Interface	Malicious routing loop attacks Sensitive data leakage	Network topology validation confidentiality and integrity protection

5. Solutions to secure the 5G system

- 5G infrastructure security
  - Secure SDN based network
    - ✓Many network programming languages, such as Frentic [147], Procera [148], FRESCO [149] are proposed for development of security applications.
    - ✓Many fine access and permission control mechanism are proposed (150-155).
    - ✓Network security applications leveraging from SDN can respond to network anomalies and spurious traffic at run-time.
  - Secure MEC
    - ✓5G security architecture introduces a new function named as the SEAF, which is independent and always deployed in the core network.
    - ✓Conventional encryption techniques (AES, DES, RSA), Identity-based encryption, attributed-based encryption, Homomorphic encryption.
    - ✓Fine-grained and dynamic access control system is important.

5. Solutions to secure the 5G system

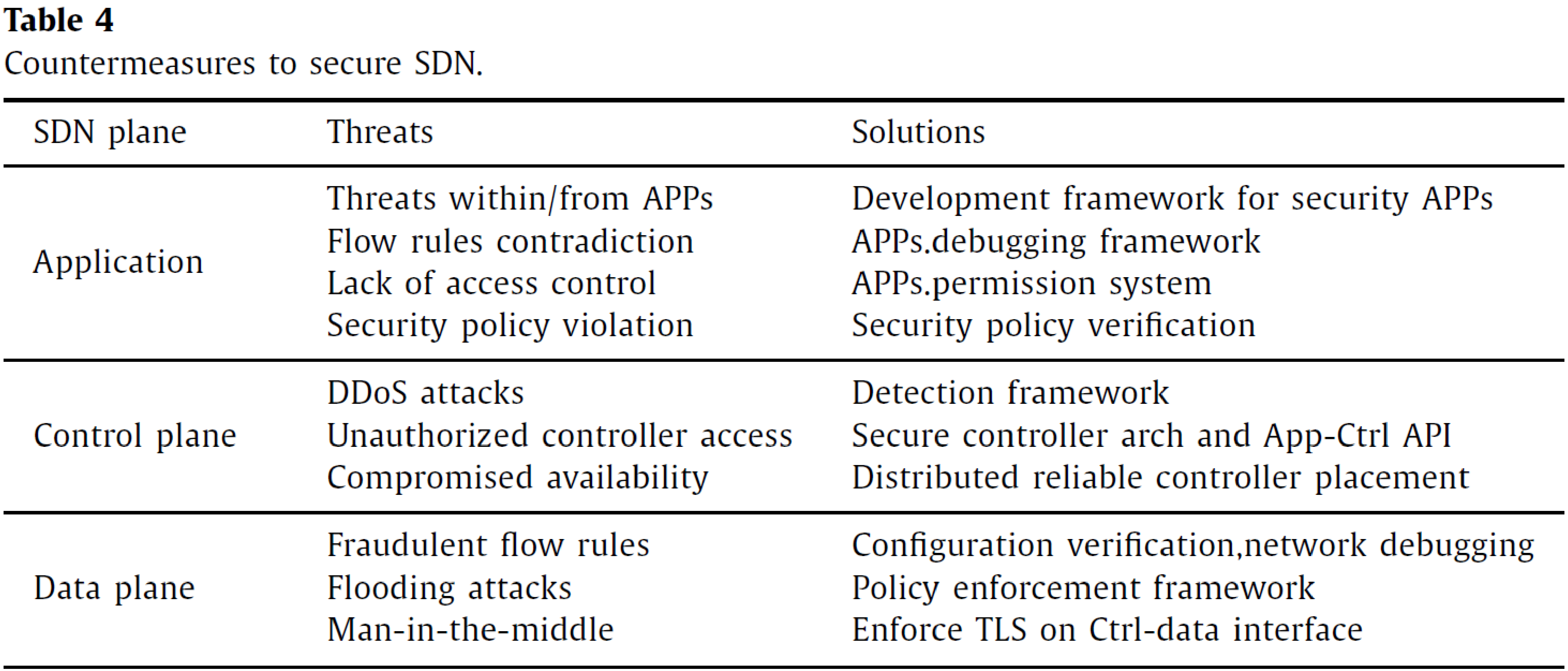


Table 4
Countermeasures to secure SDN.

SDN plane	Threats	Solutions
Application	Threats within/from APPs Flow rules contradiction Lack of access control Security policy violation	Development framework for security APPs APPs.debugging framework APPs.permission system Security policy verification
Control plane	DDoS attacks Unauthorized controller access Compromised availability	Detection framework Secure controller arch and App-Ctrl API Distributed reliable controller placement
Data plane	Fraudulent flow rules Flooding attacks Man-in-the-middle	Configuration verification,network debugging Policy enforcement framework Enforce TLS on Ctrl-data interface

5. Solutions to secure the 5G system

❖ Security for IoT

- Security and privacy protection for IoT applications can be provided from the application layer or 5G mobile network layer.
- Mechanism for application layer can provide end-to-end security and privacy protection
- Two categories for IoT solutions
  - ✓ Industry solutions
  - ✓ Academic proposals

5. Solutions to secure the 5G system

❖ Industry solutions

- ➢ Protect networks
  - ✓ To avoid device trigger related attacks, the MTC-UE in the detached state could validate the network identity when it receives a trigger indication.

- ➢ User privacy protection:
  - ✓ To address the user privacy issue, the MTC-UEs may be detached from the network when no data is exchanged to prevent unnecessary tracking of location information.

- ➢ Small data protection:
  - ✓ On the control plane based solutions, partially ciphering small data method introduces a new signaling message, and requires a change to 4G key hierarchy. As for the fast path-based solution, the security endpoint at the network side is proposed to move from BS to the core network, the existing 4G key hierarchy needs to be changed.
  - ✓ To protect small data traffic delivered by the control plane between the MTC device and core network, it is suggested that the NAS level integrity and confidentiality protection mechanism is applied.

5. Solutions to secure the 5G system

- Industry solutions
  - Security for URLCC
    - ✓ To ensure the reliability of URLCC traffic transmission, it is proposed that two duplicated N3 tunnels can be established between 5G RAN and 5G core network to achieve redundant data transmission at Release 16.
    - ✓ Data traffic protection policy using encryption and integrity protection.
    - ✓ Authentication and access control for URLCC service es.
  - Differentiated security by network slicing
    - ✓ To provide customized security service, each slice can have service-specific security mechanisms including special authentication protocols or security functions, cryptographic algorithms, and security policy configurations such as key length, key update period, etc.

5. Solutions to secure the 5G system

❖ Academic proposals

- ➢ Authentication
  - ✓ To reduce signaling overhead during the access of a large number of MTC devices, group-based aggregate authentication mechanisms are especially important for 5G.
- ➢ Key management
  - ✓ Emerging cryptographic techniques such as attribute-based cryptography can be considered to design privacy-preserving group management solutions.
- ➢ Confidentiality and integrity
  - ✓ Usually, cryptographic solutions are used to ensure data confidentiality and integrity. Especially, lightweight IBE and attribute-based encryption (ABE)

5. Solutions to secure the 5G system

❖ Academic proposals

- ➢ Lightweight security based on physical layer
  - ✓ By utilizing the intrinsic randomness of the radio channels, physical layer security mechanism can fulfill many security demands with reduced computational resource and signaling overhead associated with conventional cryptographic algorithms. Therefore, they provide promising solutions for achieving lightweight and efficient security required by 5G IoT scenarios.

- ➢ Emerging approaches
  - ✓ Recently, the emerging blockchain technology has been leveraged to bring values to the IoT security domain due to some unique features, including decentralization, pseudosymmetry and the security of transactions.

6. Future research opportunities

❖ Leverage virtualization and slicing

- One of the key issues on correlation is building and maintaining the system model encompassing the infrastructure, network services, and dynamic mapping between network services, virtual resources, and physical resources.

- the DoS attack to sensitive network elements such as network slice selection function (NSSF), which is common to all slices.

- the privacy protection mechanism

- network slicing brings new opportunities to provide customized security protection to different slice tenants.

6. Future research opportunities

❖Integrated D2D security design

- ➢Efficient key management and authentication: Network dependent authentication is problematic in case D2D devices are out of coverage of cellular networks.
- ➢Efficient D2D data security protection: Upper layer mechanisms result in big overhead, therefore, more effort is needed to explore efficient lower layer protocol security mechanisms for D2D.
- ➢Incentive mechanisms for cooperation: D2D users are selfish in nature, which may negatively impact the feasibility of some security solutions, such as key generation and distribution.
- ➢D2D user privacy protection: How to figure out preferred neighbors to set up D2D communication without disclosing private information is challenging.

6. Future research opportunities

❖ Security based on 5G new radio

- ➢ M-MIMO: The technology has the potential to be used to detect intruders by focusing on the energy of artificial noise

- ➢ mmWave: Active eavesdroppers can jeopardize the channel estimation process for desired users, which represents a serious security threat. More effort is needed to find countermeasures to defend against active eavesdroppers in mmWave communications.

- ➢ Full duplex: The technology itself is still under developing, the self-interference mitigation of a full duplex relies on space division and precoding technologies, which is a great challenge for further study.

- ➢ UDN: In UDN and D2D-assisted multi-tier HetNet, novel power allocation and interference alignment with security considerations should be further investigated to increase the secrecy capacity per cell without impacting other cells.

- ➢ Coordinate security and green: For the most constrained, battery-dependent IoT devices with a long target lifetime, there may be a need to consider even more lightweight physical layer solutions from the energy perspective.

7. Conclusion

- This article identifies typical security issues from several perspectives, including lessons from the existing 4G network, requirements from new scenarios and models, challenges from new technologies and architectures.

- The potential solutions to ensuring 5G security and privacy from several perspectives including overall security architectures, core networks, new radio technologies, cloud infrastructure, and IoT applications

- However, 5G security still have many security challenges.

8, Opinion

- This paper mentioned physical layer’s noise for confidentiality of data. Also, they mentioned it have advantage including performance.

- This noise can be used also in homomorphic encryption(because homomorphic encryption needs some noise for encryption).

- Also, the implementation and performance analysis of LWC is good research direction. Especially, optimized implementation.

CIS LAB

Thank you for your attention