NANYANG
TECHNOLOGICAL
UNIVERSITY

Security Investigation in 4G LTE Wireless Networks

Dr. Maode Ma

School of Electrical and Electronic Engineering
Nanyang Technological University, Singapore
emdma@ntu.edu.sg

Outline

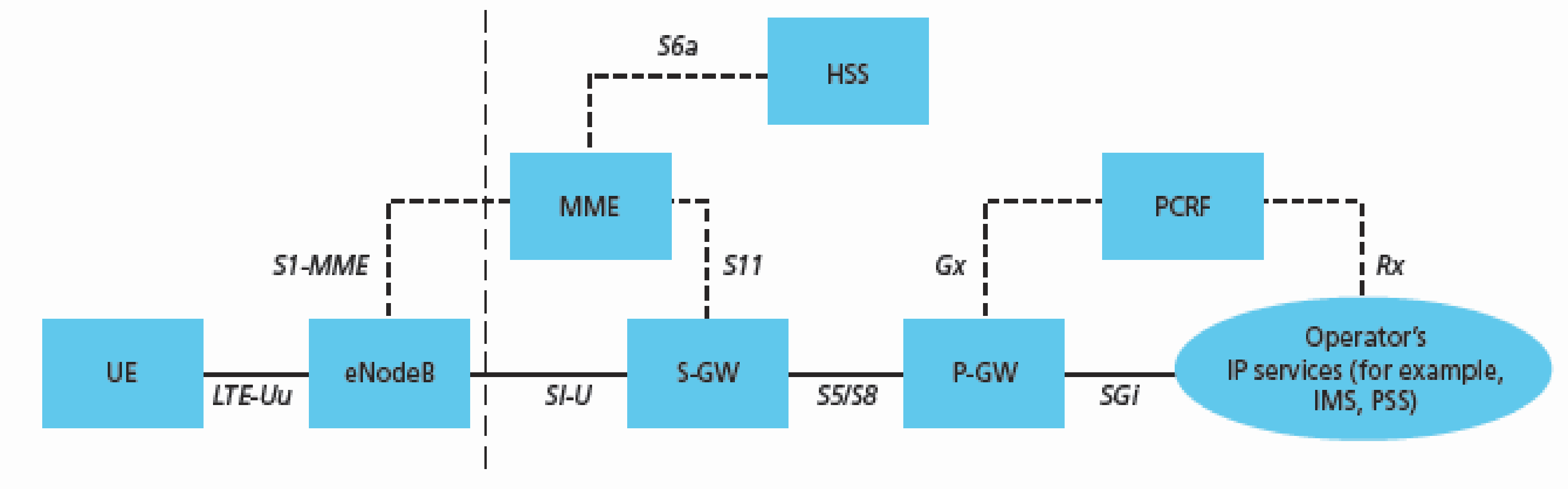
- Introduction
  - Fundamentals of LTE Networks
  - Security Framework
  - Security Mechanisms
- Vulnerabilities
- Existing Solutions
- Open Research Issues
- Conclusion

Long Term Evolution

- Long Term Evolution
  - Long-Term Evolution (LTE) is an emerging radio access network technology standardized in 3GPP and it is evolving as an evolution of Universal Mobile Telecommunications System (UMTS).
  - It aims to provide seamless Internet Protocol (IP) connectivity between user equipments (UE) and the packet data network (PDN) without any disruption to the end users' applications during mobility.
- Systems
  - The system is named evolved packet system (EPS) with two parts:
    - System architecture evolution(SAE)
      - Evolved packet core (EPC) network
    - Long term evolution (LTE):
      - Radio access network (E-UTRAN) supported by radio access technology (E-UTRA)

Architecture of EPS

- EPS
  - EPS is comprised of the CN (EPC) and the access network E-UTRAN.
  - The CN consists of many logical nodes
  - The access network is made up of essentially just one node, the evolved NodeB (eNodeB), which connects to the UEs.
  - Each of these network elements is interconnected by means of interfaces that are standardized in order to allow multi-vendor interoperability.



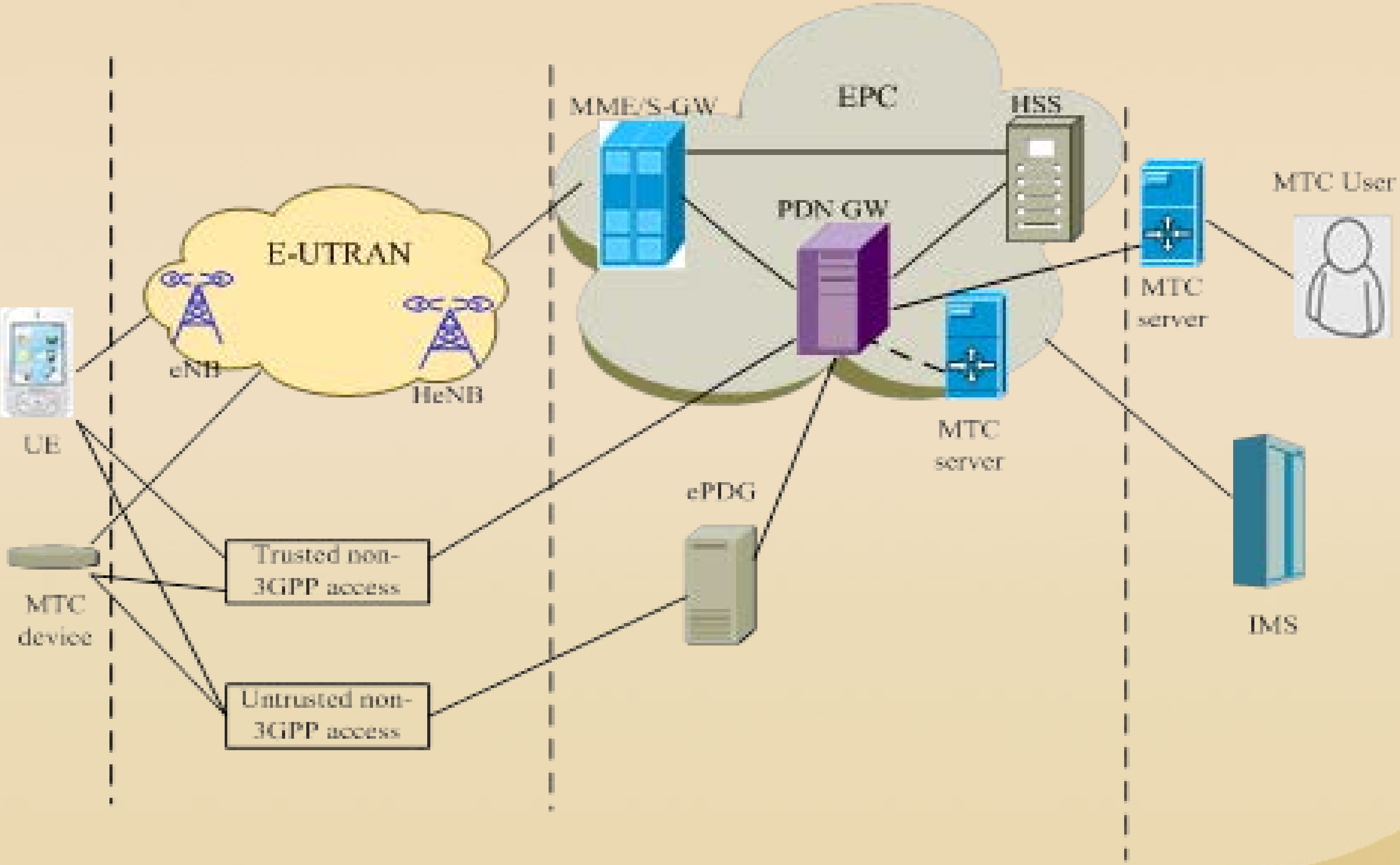
The Core Network

- EPC is responsible for the overall control of the establishment of the bearers and the UE
- The main logical nodes in the EPC:
  - Policy Control and Charging Rules Function (PCRF) responsible for
    - policy control and decision-making,
    - control of the flow-based charging functionalities,
    - QoS authorization provision
  - Home Subscriber Server (HSS) holds
    - users subscription data,
    - information about the PDNs,
    - dynamic information the identity of the MME
  - PDN Gateway (P-GW) is responsible for
    - IP address allocation for the UE,
    - filtering of downlink user IP packets into the different QoS-based bearers,
    - QoS enforcement for guaranteed bit rate bearers

The Core Network

- Serving Gateway (S-GW) serves as
  - local mobility anchor for the data bearers when the UE moves between eNodeBs,
  - buffer of downlink data while the MME paging,
  - administrative functions
- Mobility Management Entity (MME) is the control node that processes the signaling between the UE and the CN
  - Non Access Stratum (NAS) protocols running between the UE and the CN
  - Functions related to bearer management
    - establishment, maintenance and release of the bearers
  - Functions related to connection management
    - establishment of the connection and security between the network and UE

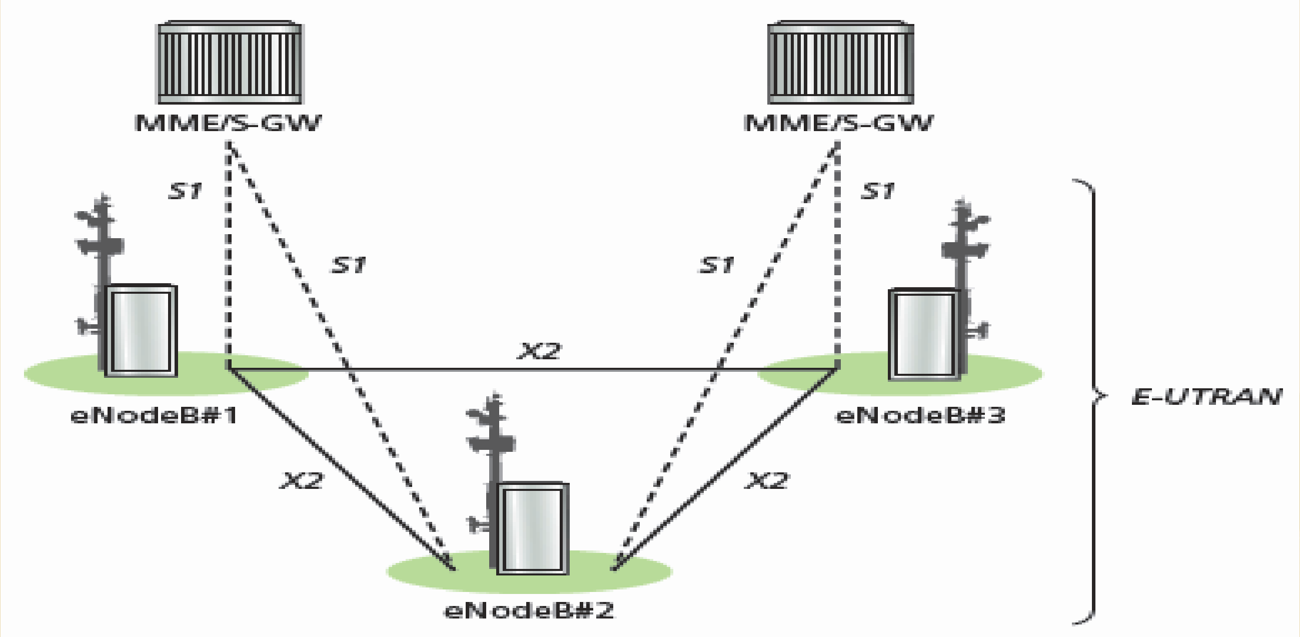
Long Term Evolution



NANYANG TECHNOLOGICAL UNIVERSITY

The Access Network

- E-UTRAN consists of a network of eNodeBs, where there is no centralized controller for normal user traffic
  - – The eNodeBs are normally interconnected with each other by a X2 interface
  - – The eNodeBs are connected to the EPC by a S1 interface
    - connected to the MME by a S1-MME interface
    - connected to the S-GW by a S1-U interface
  - – The protocols run between the eNodeBs and the UE are the air signaling (AS) protocols



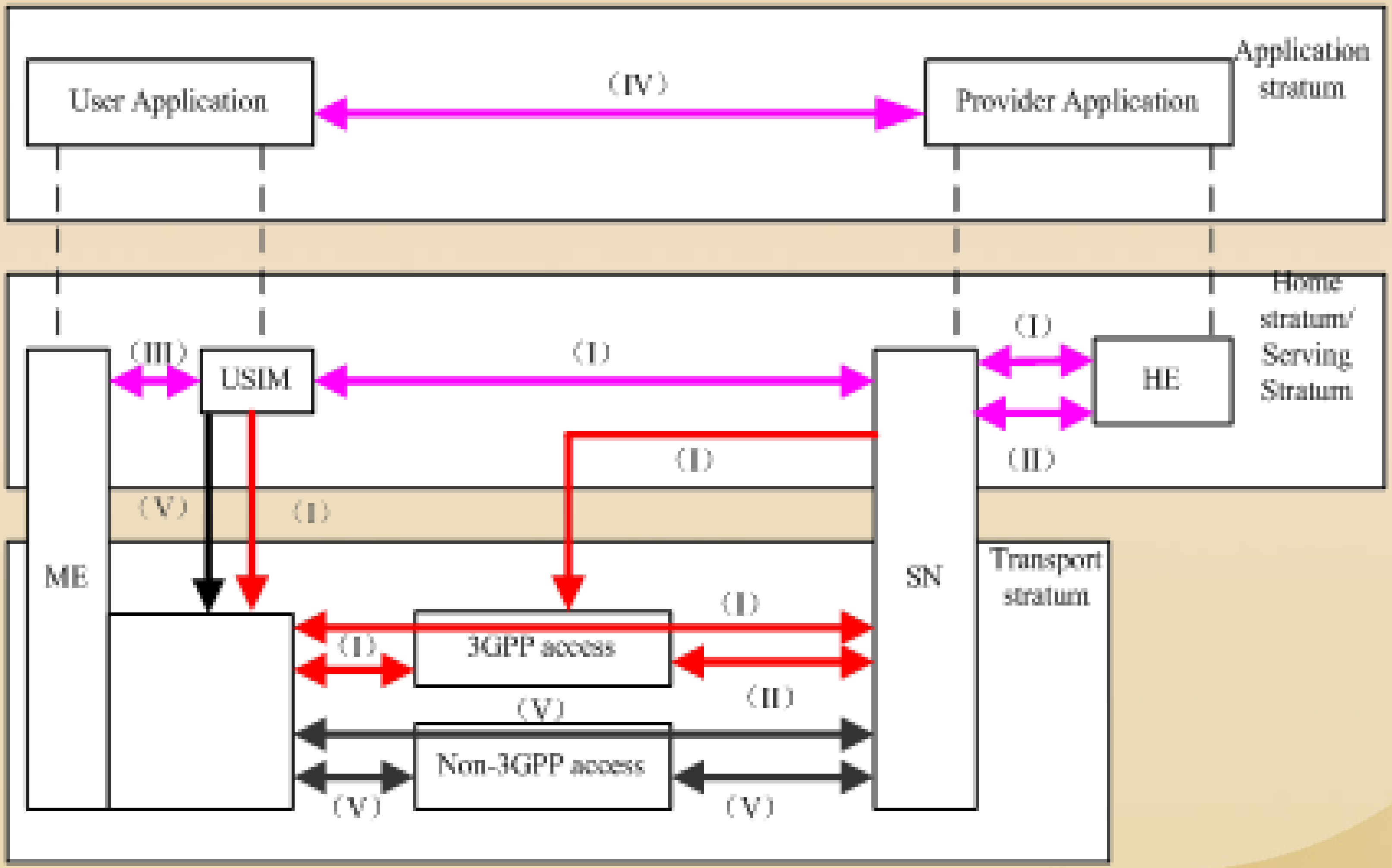
The Access Network

- The E-UTRAN is responsible for all radio-related functions:
  - Radio resource management
    - All functions related to the radio bearers including
      - radio bearer control,
      - radio admission control,
      - radio mobility control,
      - scheduling and dynamic allocation of resources to UEs in both uplink and downlink
  - Header compression
    - Compression of the IP packet headers to reduce overhead
  - Security
    - All data sent over the radio interface is encrypted
  - Connectivity to the EPC
    - The signaling toward MME and the bearer path to the S-GW
- All of the network functions reside in the eNodeBs with all the radio controller function integrated into an eNodeB

LTE Security Architecture

- There are 5 security levels:
  - Network access security (I):
    - The set of security features that provides the UEs with secure access to the EPC and protect against various attacks on the radio link.
  - Network domain security (II):
    - The set of security features that protects against attacks on the wire line network and enable nodes to exchange signalling data and user data in a secure manner
  - User domain security (III):
    - The set of security features that provides a mutual authentication between the USIM and the ME before the USIM access to the ME.
  - Application domain security (IV):
    - The set of security features that enables applications in the UE and in the provider domain to securely exchange messages.
  - Non 3GPP domain security (V):
    - The set of features that enables the UEs to securely access to the EPC via non-3GPP access networks and provides security protection on the radio access link.

LTE Security Architecture



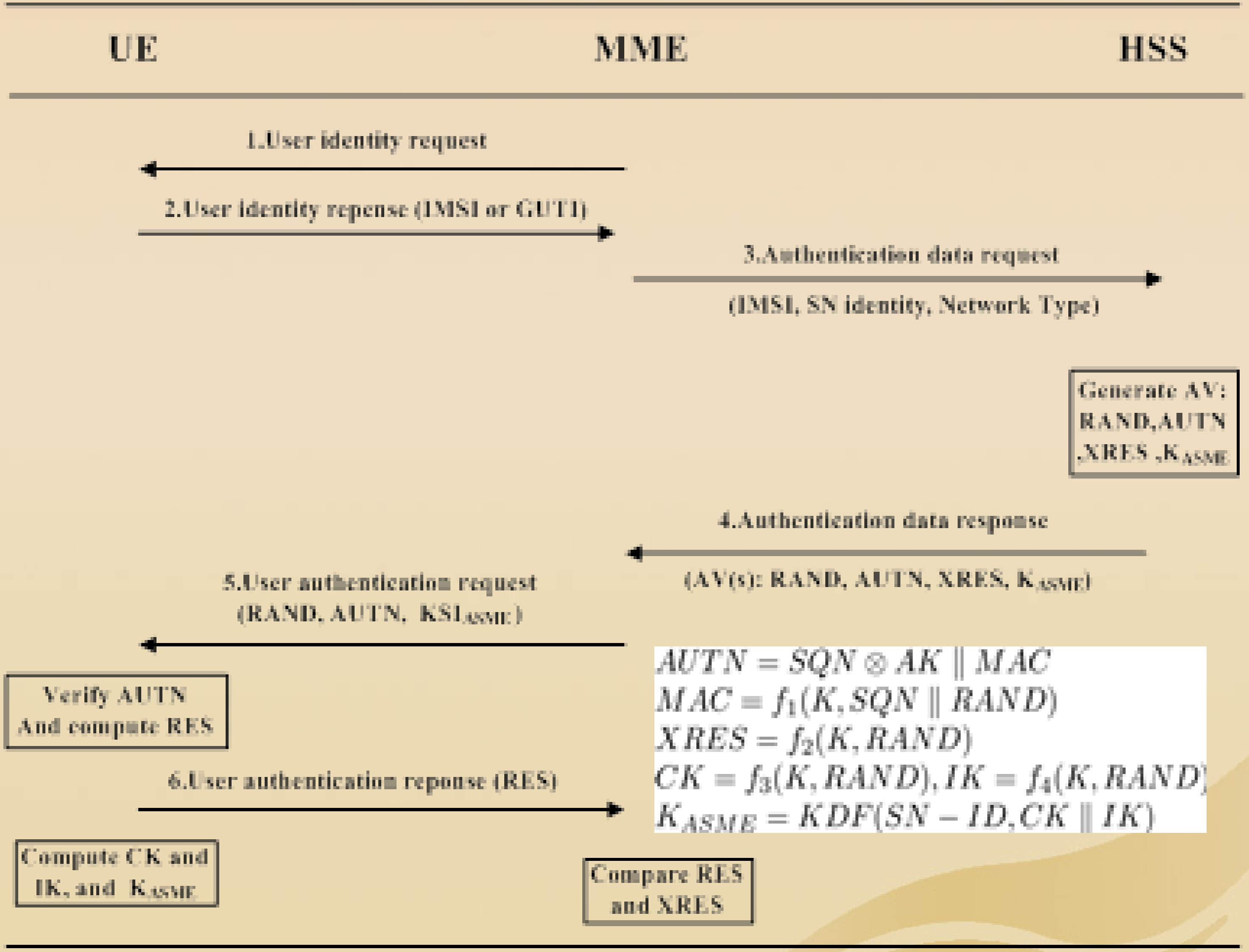
LTE Security Mechanisms

- Focus on 5 aspects of the LTE security at the network access security level
  - LTE cellular security
  - LTE handover security
  - IMS security
  - HeNB security
  - MTC security

Security in a LTE Cellular System

- A mutual authentication between an UE and the EPC is the most important security scheme.
- The AKA procedure to achieve the mutual authentication between the UE and the EPC.
- It generates a ciphering key (CK) and an integrity key (IK) used to derive different session keys for the encryption and the integrity protection.
- When an UE connects to the EPC over the E-UTRAN, the MME represents the EPC to perform a mutual authentication with the UE by the EPS AKA
- For non-3GPP access, several different AKA procedures are implemented.

EPS-AKA Authentication


UE
MME
HSS
1.User identity request
2.User identity repense (IMSI or GUTI)
3.Authentication data request
(IMSI, SN identity, Network Type)
Generate AV:
RAND,AUTN
,XRES ,K$_{ASME}$
4.Authentication data response
(AV(s): RAND, AUTN, XRES, K$_{ASME}$)
5.User authentication request
(RAND, AUTN, KSI$_{ASME}$)
Verify AUTN
And compute RES
6.User authentication reponse (RES)
Compute CK and
IK, and K$_{ASME}$
Compare RES
and XRES

$$AUTN = SQN \otimes AK \parallel MAC$$

$$MAC = f_1(K, SQN \parallel RAND)$$

$$XRES = f_2(K, RAND)$$

$$CK = f_3(K, RAND), IK = f_4(K, RAND)$$

$$K_{ASME} = KDF(SN - ID, CK \parallel IK)$$

Outstanding Features

- There are several outstanding features in user access security
  - Serving network identity (SN ID) has been added to the EPS AKA procedure to to avoid attacks such as redirection attacks and false base station attacks.
  - On the top of security functions at the access stratum (AS) level between the UE and the eNB, new security functions at the none access stratum (NAS) level between the UE and the MME have been included.
  - The new root key K_{ASME}, computed by the HSS will be delivered to the MME or the serving network (SN).
  - The key set identifier KSI_{ASME} is embed in the user authentication request message transmitted to the UE by the MME.
  - A new key hierarchy is introduced to protect the security of the signaling and user data traffic

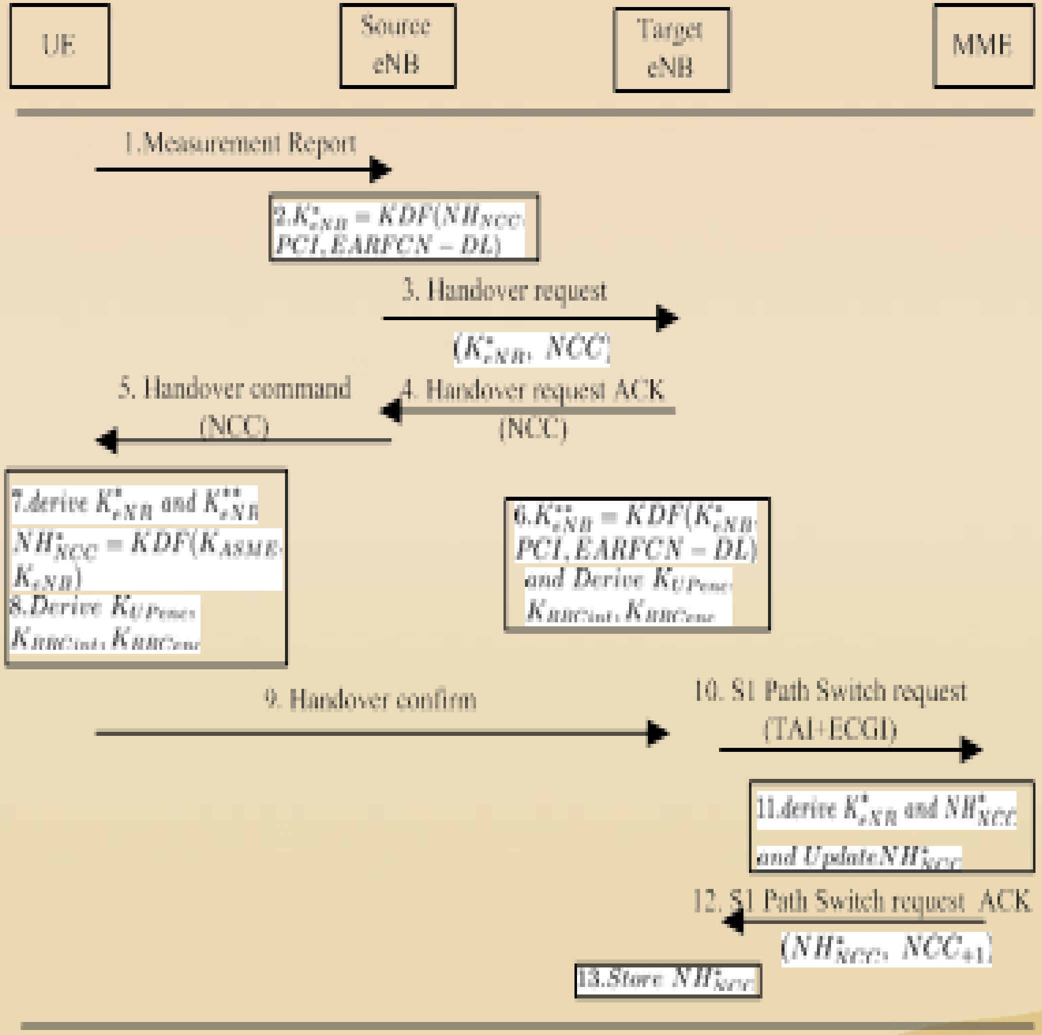
Outstanding Features

- Non-3GPP access authentication is supported between the UE and the AAA server
  - For a trusted non-3GPP access network, which can be pre-configured in the UE, the UE and the AAA server shall implement the Extensible Authentication Protocol-AKA (EAP-AKA) or the Improved EAP-AKA (EAP-AKA') to accomplish the access authentication.
  - If an UE connects to the EPC over an untrusted non-3GP access network, the UE and the ePDG need to perform the IPsec tunnel establishment and further use the Internet Key Exchange Protocol Version 2 (IKEv2) with EAP-AKA or EAP-AKA' to establish the IPSec security associations.

Security in Handover Processes

- Intra E-UTRAN mobility: The current eNB and the target eNB are managed by the same MME
  - A new key management mechanism is designed with different ways to derive the new eNB keys based on vertical or horizontal key derivations.
  - A MME and the UE shall derive a K_{eNB} and a next hop (NH) parameter from the K_{ASME}, which is derived by the UE and the MME after an initial access authentication.
  - In the initial setup, K_{eNB} is derived directly from K_{ASME}, and is then associated with a virtual NH parameter with a NH chaining counter (NCC) value to be zero. The UE and the eNB use the K_{eNB} to secure the communication on the air interface.
  - In handovers, a new session key used between the UE and the target eNB, K^*_{eNB}, is derived from either the active K_{eNB} or from the NH parameter.

Inter-eNB Handover


UE
Source eNB
Target eNB
MME
1.Measurement Report
2.$K^*_{eNB} = KDF(NH_{NCC}, PCI, EARFCN - DL)$
3. Handover request
(K^*_{eNB}, NCC)
4. Handover request ACK
(NCC)
5. Handover command
(NCC)
6.$K^{**}_{eNB} = KDF(K^*_{eNB}, PCI, EARFCN - DL)$ and Derive K_{UPenc}, K_{RRCint}, K_{RRCenc}
7.derive K^*_{eNB} and K^{**}_{eNB}
$NH^*_{NCC} = KDF(K_{ASME}, K_{eNB})$
8.Derive K_{UPenc}, K_{RRCint}, K_{RRCenc}
9. Handover confirm
10. S1 Path Switch request
(TAI+ECGI)
11.derive K^*_{eNB} and NH^*_{NCC} and UpdateNH^*_{NCC}
12. S1 Path Switch request ACK
(NH^*_{NCC}, NCC_{+1})
13.Store NH^*_{NCC}

Security in Handover Processes

- Mobility between the E-UTRAN and UTRAN/GERAN
  - For the handover from the E-UTRAN to the UTRAN or the GERAN:
    - the UE and the MME shall first derive a *CK'* and *IK'* from the K_{ASME}
    - Upon receiving *CK'* || *IK'* with *KSI'* from the MME, the target Service GPRS Supporting Node (SGSN) and the UE shall replace all stored parameters *CK*, *IK*, *KSI*, *with CK'*, *IK'*, *KSI'*.
    - the UE and the target SGSN shall use *CK'* and *IK'* to derive the General Packet Radio Service (GPRS) *Kc*.
  - For the handover from the UTRAN/GERAN to the E-UTRAN:
    - The target MME shall derive K'_{ASME} from *CK* and *IK* or GPRS *Kc* received from the SGSN.
    - The UE shall also execute the above same procedure as the MME to derive K'_{ASME}.
    - The target MME and the UE shall derive K_{eNB} and the corresponding NAS keys according to the key hierarchy of LTE.

Security in Handover Processes

- Mobility between E-UTRAN and non-3GPP access networks
  - There are several different mobility scenarios between heterogeneous access systems in the LTE networks:
    - Handovers from trusted or untrusted non-3GPP access networks to the E-UTRAN
    - Handovers from the E-UTRAN to trusted or untrusted non-3GPP access networks
  - The UE, the target access network and the EPC will implement a full access authentication procedure before the UE handovers to the new access network.
  - Different access authentication procedures will be executed in distinct mobility scenarios.

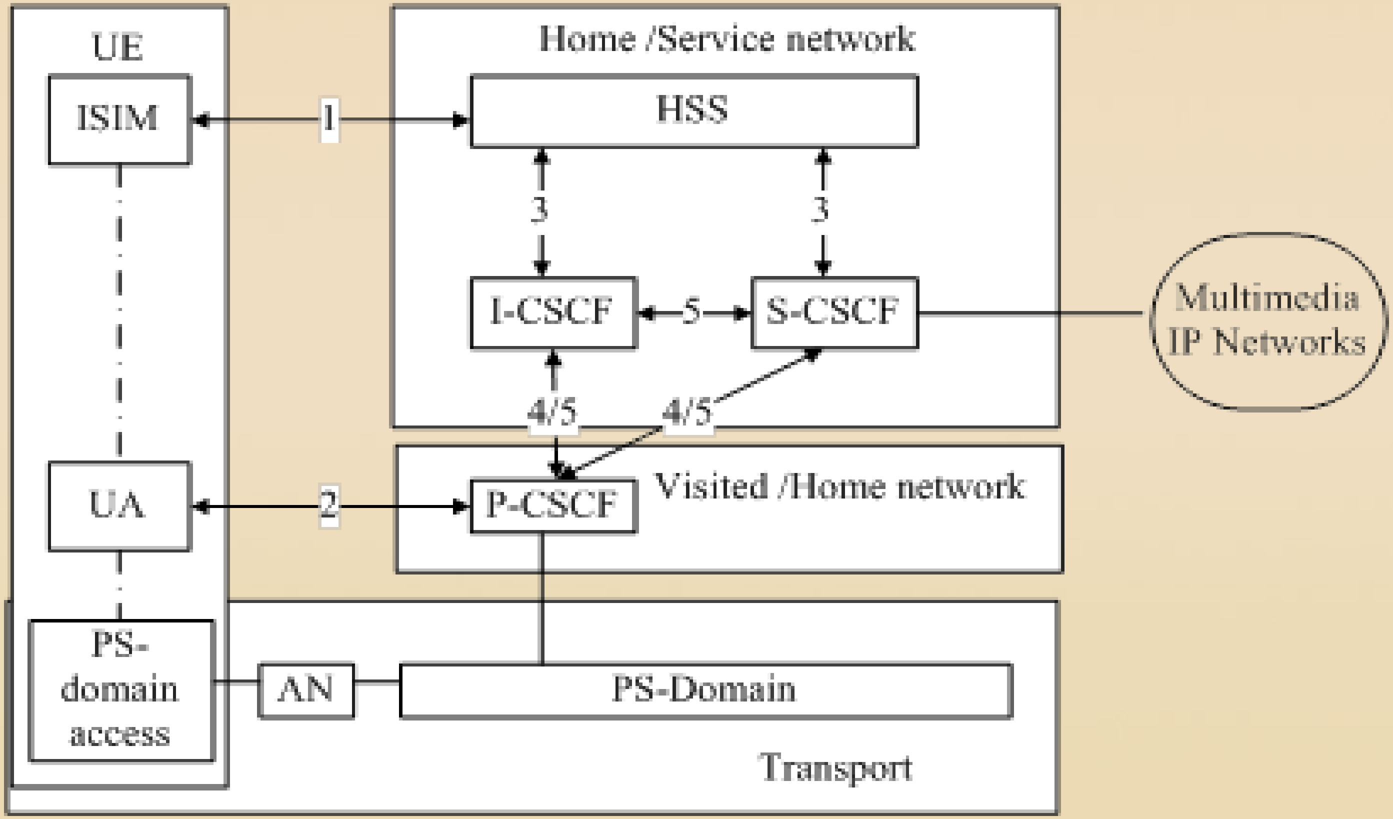
Security in IMS

- IMS is an overlay architecture to provide the LTE/LTE-A networks with multimedia services
  - An UE needs a new IMS Subscriber Identity Module (ISIM) located within the Universal Integrated Circuit Card (UICC) for multimedia services.
  - The IMS authentication keys and functions at the user side shall be stored at the ISIM.
  - The main architectural elements in the IMS are the Session Initiation Protocol (SIP) proxies, Call Service Control Functions (CSCF), which consists of Proxies-CSCF (P-CSCF), Interrogating-CSCF (I-CSCF) and Serving-CSCF (S-CSCF).
  - Receiving a request from an UE, the P-CSCF redirects and forwards the SIP message to the I-CSCF within the UE's home network. Then, I-CSCF contacts the HSS for an appropriate S-CSCF to forward the registration request to.

Security in IMS

  - Upon the receipt of the request, the S-CSCF contacts the HSS to obtain the user's authentication data to authenticate the UE and provide the session control of the multimedia services.
  - Once the UE has successfully established a security association with the network and a separate security association the IMS, an access will be granted to multimedia service.
- The IMS security architecture includes a few different security associations and different requirements for the security protection for the IMS.
  - A mutual authentication. The S-CSCF represents the HSS to authenticate the UE.
  - A secure link and a security association between the UE and a P-CSCF.
  - Security within the network domain.

Security in IMS



IMS Security Architecture

Security in IMS

- In order to access the multimedia services, LTE users have to be authenticated in both the LTE network layer and the IMS service layer.
  - An IM subscriber needs the mutual authentication with the LTE network by the EPS-AKA before the access to multimedia services.
  - An IMS AKA is executed between the ISIM and the Home Network (HN) for authentication and key agreement for the IMS

Security at HeNB

- A HeNB is a femtocell access point installed by a subscriber in residence or small office to increase indoor coverage for voice and high speed data service.
  - Three types of access for the HeNB include closed access, hybrid access and open access.
  - A HeNB connects to the EPC over the Internet via the broadband backhaul.
- Five security features of the HeNB designed in LTE networks:
  - H(e)NB access security
  - Network domain security
  - H(e)NB service domain security
  - UE access control domain security
  - UE access security domain

NANYANG TECHNOLOGICAL UNIVERSITY

Security in MTC

- MTC is the Machine to Machine (M2M) communication, which is a form of data communication between entities without human interaction.
  - The MTC devices can communicate with one or more MTC servers via the LTE networks.
  - The MTC devices can also communicate directly with each other without contacting with the MTC servers.
- MTC security architecture includes 3 security areas.
  - A. Security for the MTC between the MTC device and 3GPP network.
    - (A1) Security for the MTC between the MTC device and the Radio Access Network, E-UTRAN/UTRAN/GERAN
    - (A2) Security for the MTC between the MTC device and the MME
    - (A3) Security for the MTC between the MTC device and the MTC-IWF for 3GPP access/ ePDG for non-3GPP access

Security in MTC

- B. Security for the MTC between the 3GPP network and the MTC server/MTC user, MTC application.
  - (B1) Security for the MTC between the MTC server and the 3GPP network, which can be further divided into security aspects when the MTC server is within and outside the 3GPP network
  - (B2) Security for the MTC between the MTC user, MTC application, and the 3GPP network
- C. Security for the MTC between the MTC server/MTC user, the MTC application, and the MTC device
  - (C1) Security for the MTC between the MTC server and the MTC device
  - (C2) Security for the MTC between the MTC user, MTC application, and the MTC device

- To enable the secure communication, the MME represents the network to implement mutual authentications with the MTC device by the EPS AKA.

Vulnerability in Security Framework

- There could be vulnerability existing in 6 aspects on LTE security framework as follows.
  - Vulnerability in LTE System Architecture
  - Vulnerability in the LTE Access Procedure
  - Vulnerability in LTE Handover Procedure
  - Vulnerability in IMS Security Mechanism
  - Vulnerability in HeNB Security Mechanism
  - Vulnerability in MTC Security Architecture

Vulnerability in System Architecture

- The flat IP-based architecture of the 3GPP LTE networks results in more security risks
  - vulnerability to the injection, modification, eavesdropping attacks, IP address spoofing, DoS attacks, viruses, worms, spam mails, etc
- The all-IP network provides a direct path to the base stations for malicious attackers because an MME manages numerous eNBs in the flat architecture.
  - Due to the introduction of low-cost base stations, HeNBs, an attacker can easily obtain it to create his own rogues.
- New risks exist due to several different mobility scenarios when an UE moves away from an eNB/HeNB to a new HeNB/eNB

Vulnerability in Access Procedure

- The EPS-AKA scheme lacks a privacy protection. There are some instances resulted in disclosure of the IMSI because
  - The IMSI cannot be retrieved from Globally Unique Temporary Identity (GUTI). The current MME cannot be contacted or cannot retrieve the IMSI
- DoS attacks cannot be prevented because
  - The MME must forward the UE's requests to the HSS/AuC even before the UE has been authenticated by the MME. And the MME can only authenticate the UE after an RES has been received.
- Bandwidth consumption and authentication signaling overhead between the SN and the HN will be caused because
  - The SN must turn back to the HN for a request of another set of authentication vectors when the UE stays in the SN for a long period and exhausts its set of AVs for the authentication

Vulnerability in Access Procedure

- The EPS-AKA protocol lacks the ability of online authentications.
  - The HN is off-line with respect to the authentication process between the UE and the SN, which can be traced back
- The EAP-AKA protocol has several shortcomings
  - such as the disclosure of user identity, vulnerability to MitM attacks, sequence number (SQN) synchronization, and additional bandwidth consumption
  - Because the LTE system reuses the EAP-AKA or EAP-AKA’ to provide a secure access authentication.

Vulnerability in Handover Procedure

- Lack of backward security
  - Since the key chaining architecture is used, the current eNB may derive new keys for multiple target eNBs by chaining the current key with the eNB specific parameters. Once an attacker compromises the current eNB, the subsequent session keys will be obtained.
- Vulnerability to desynchronization attacks
  - By a rogue eNB, an attacker can disrupt refreshing of the NCC value by either manipulating the handover request message between the eNBs or the S1 path switch acknowledgement message from an MME to a target eNB.
- Vulnerability to the replay attacks
  - The security connection between the UE and the target eNB will not be set and the UE has to launch a new handover procedure

Vulnerability in IMS Security

- Energy consumption of an UE and system complexity increased
  - An IMS UE needs to execute two AKA protocols, which are the EPS AKA in the LTE access authentication and the IMS AKA in the IMS authentication
- The IMS AKA is vulnerable to the MitM attacks, lack of SQN synchronization, and extra bandwidth consumption.
- Vulnerable to several types of DoS attacks.
  - On receiving a register request from an IMS UE, the P-CSCF/MME sends the request to the core network (I-CSCF/S-CSCF/HSS) to implement an access authentication, where an adversary could flood the I-CSCF/S-CSCF/HSS by sending correct packets with invalid IMSI/IMPI

Vulnerability in HeNB Security

- Most vulnerability comes due to the insecure wireless links.
  - the links between the UE and the HeNB and the backhaul between the HeNB and the EPC, which are susceptible to many kinds of attacks because the data and conversations are vulnerable to interception and eavesdropping over them.
- Lack of a vigorous mutual authentication between the UE and the HeNB and the HeNB is not sufficiently a trust party.
  - So that current HeNB security mechanism cannot prevent various protocol attacks including eavesdropping attacks, MitM attacks, masquerading attacks and compromising subscriber access list.
- Vulnerable to several types of DoS attacks.
  - Due to the exposure of the entrance points of core network to the public Internet, it is vulnerable to Internet-based attacks, such as DoS attacks.

Vulnerability in MTC Security

- The MTC lacks security schemes for the communication between the MTC device and the ePDG
  - for non-3GPP access, that between the MTC applications and for the 3GPP networks and that between the MTC applications and the MTC devices.
- The MTC devices are extremely vulnerable to several attacks.
  - such as physical attacks, compromise of credentials, protocol attacks and the attacks to the core network because the MTC devices are typically required to be low capabilities in terms of both energy and computing resources.
- Simultaneous authentication of a number of MTC devices can incur signalling overhead between an HSS and the MME when they simultaneously requests to access to the network.

Existing Solutions

- There are some existing solutions to overcome the vulnerability in LTE security framework in the current literature as follows.
  - Solutions to the Security in Access Procedure
  - Solutions to the Security in Handover Procedure
  - Solutions to the IMS Security
  - Solutions to the HeNB Security
  - Solutions to the MTC Security

Solutions to Access Procedure

- Security provisioning in network access procedure mainly addresses effective authentication and key management.
  - A slightly modified version of the EPS-AKA protocol has been presented in [1].
    - It introduces a new subscriber module ESIM instead of the USIM to provide a direct online mutual authentication between the ESIM and the MME/HSS to overcome the shortcomings of the EPS-AKA protocol.
  - An enhanced EPS-AKA protocol has been proposed in [2] to improve the performance by increasing a little computation in the SN.
    - By the scheme, the SN/MME generates and stores many authentication vectors (AVs) from the original AVs at the HN/HSS. It can largely reduce the authentication signalling exchange between the SN and the HN to saves the bandwidth consumption at the HSS/HN.

Solutions to Access Procedure

- A hybrid authentication and key agreement scheme based on Trust Model Platform (TMP) and Public Key Infrastructure (PKI) has been proposed in [3].
  - It can provide considerable robustness for mobile users to access sensitive service and data, while passwords are associated with the fingerprint and public key to achieve mutual authentication between UEs and the HN over the TMP.
- An authentication and key agreement scheme based on self-certified public key (SPAKA) has been proposed in [4].
- It uses a public key broadcast protocol for an UE to identify the genuine BS to overcomes the shortcomings of 3G AKA.
- An EAP-Archie method in [5] has been introduced to ensure the access layer security.
  - By using the AES ciphering, a mutual authentication and key agreement between the users and the network access layer can be achieved.

Solutions to Access Procedure

- A Security Enhanced Authentication and Key Agreement (SE-EPS AKA) based on Wireless Public Key Infrastructure (WPKI) has been proposed in [6].
  - It ensures the security of user identity and the exchanged message with limited energy consumption by using Ellipse Curve Cipher (ECC) encryption.
- In [7], to provide a stronger security protection, the use of the password authentication key exchange by Juggling (J-PAKE) protocol in authentication process instead of the EPS-AKA protocol has been proposed.
  - The J-PAKE is a password authentication keying agreement protocol to provide zero-knowledge proof using a shared key that is never sent over the transmission medium.
- An ensured confidentiality authentication and key agreement (EC-AKA) has been proposed in [8] to enhance the user's confidentiality.
  - By the scheme, all the AKA messages are fully protected on the integrity by encryption, which can prevent the disclosure of identity of the users and the users being tracked.

Solutions to Handover Procedure

- Security provisioning in handover procedure addresses efficient authentication between eNBs or HeNBs with less overhead.
  - A simple and robust handover authentication scheme based on the improved proxy signature has been proposed in [9].
    - By the scheme, an UE and the target eNB or HeNB can directly accomplish a mutual authentication and set up a session key with their long term secret keys.
    - It can be applied to all of the mobility scenarios including the handovers between the HeNBs, the handovers between the eNBs and the HeNBs, the handovers between the eNBs and the inter-MME handovers.
  - A hybrid authentication and key agreement scheme has been proposed to support globe mobility with low computational power and secure communications in [10].
    - It associates a dynamic password with a public-key to provide lightweight authentication and non-repudiation service. By adopting a public key broadcast protocol, a mutual authentication between the UE and foreign network (FN) can be achieved without the use of certificate.

Solutions to Handover Procedure

- A fast and secure handover authentication scheme has been proposed to achieve seamless handovers between heterogeneous access systems in the LTE networks [11].
  - It can provide a robust security protection and ideal efficiency and can be applied to all of the mobility scenarios.
- A security roaming and vertical handover scheme between several different access technologies has been proposed in [12].
  - It designs a global authentication protocol to enable a vertical handover between heterogeneous access systems including GSM, UMTS, WiFi and WiMAX without requiring a prior subscription to the visited network.
- A new re-authentication protocol to secure interworking and roaming between LTE and the WLAN has been proposed in [13].
  - It improves the EAP-AKA protocol and adopts hybrid unit to provide the secure 3GPP LTE-WLAN interworking.

Solutions to Handover Procedure

- An optimized fast handover mechanism has been presented in [14] to handle handovers between the 3GPP and the non-3GPP networks.
  - It employs a security context transfer mechanism for handovers between the 3GPP networks and the trusted non-3GPP networks and a pre-authentication scheme for handover between the 3GPP and the untrusted non-3GPP networks to reduce the handover latency without compromising the security level.
- Five fast and secure re-authentications protocols for the LTE subscribers to perform handovers between the WiMAX and the WLAN have been proposed in [15].
  - The schemes improve the EAP-AKA protocol to derive the HO-related keys and other parameters to speed re-authentications in the future WiMAX-WLAN HOs. They can achieves an outstanding performance in terms of the re-authentication signalling traffic and the re-authentication delay compared with the current 3GPP standard protocols and with several security features including forward and backward secrecy.

Solutions to IMS Security

- An improved one-pass AKA procedure has been presented in [16].
  - The scheme makes the security key binding between the initial authentication and the second authentication, which can reduce significantly the authentication overhead compared to the multi-pass authentication procedure without compromising the security services.
- A new IMS service authentication scheme has been proposed in [17] using Identity Based Cryptography (IBC) to enhance the security of the IMS authentication process.
  - By the IBC and ECC, it allows the personalization of the IMS services through authenticating the users in a personal manner during the services access and provides a robust security protection efficiently.
- An Improved AKA (I-AKA) authentication protocol has been addressed in [18] to reduce energy consumption.
  - A secure binding of the network layer and the IMS layer authentication by using the IMPI is utilized to avoid the double execution of the AKA protocol.

Solutions to HeNB Security

- A vigorous mutual authentication and access control mechanism has been proposed to guarantee secure communication for the HeNB by adapting a proxy-signature [19].
  - By the scheme, the OAM and the core network (CN) have a contractual agreement on the installation, operation and management of the HeNB by issuing a proxy-signature to each other. Then, the OAM and CN re-delegates their proxy-signing capability to a HeNB and the CN signature is issued to an UE. Finally, the mutual authentication between the UE and the HeNB can be achieved with the proxy signature on behalf of the OAM and the CN.
- A solution to identity and location tracking at the air interface by assigning and changing identifiers based on context has been proposed in [20]. In addition, a protection scheme against DoS attacks with a HeNB deployment in the LTE has been presented.

Solutions to MTC Security

- It is suggested in [21] that the Trust Environment (TrE) can be embedded within the MTC devices to protect the security of the MTC devices.
  - It can provide more robust protected functions for the access authentication and support several cryptographic capabilities including the symmetric and asymmetric encryption and decryption.
  - An algorithm to detect the compromised MTC devices by establishing an interactive key among nodes has been proposed in [22].
- A group-based authentication and key agreement approach for a group of UEs roaming from the same home network (HN) to a serving network (SN) has been presented in [23].
  - By it, multiple UEs belong to the same HN, can form a group. When the first UE in a group moves to the SN, the SN obtains the authentication information for the UE and other members from the concerned HN by performing a full authentication. Thus, when other group members visit, the SN can authenticate them locally without the HN.

Open Research Issues

- Many security issues for the LTE/LTE-A networks are still open research issues without perfect resolutions.
- The design of the MTC security mechanisms in the LTE/LTE-A networks will be the major future research on LTE security.
- There are also some other open security issues to be addressed.
  - MTC Security
  - Security Architecture
  - Security in Handover Procedure
  - IMS Security
  - HeNB Security

MTC Security

- Security with higher performance is required
  - For real-time applications, the MTC device is required to directly deliver real-time information over reliable high-speed link. Thus, the security mechanism cannot incur massive operational overhead.
- The trade-off between encryption and less transmission is required
  - MTC devices have small amount of data transmission. However, the cost of encryption and integrity checking operations could be greater than the data transmission. The trade-off should be achieved.
- Various mobility should be supported
  - The mobile service requirements of the restricted mobility and the high speed mobility of the MTC devices have not been addressed.
  - Extra low power consumption for the MTC devices is required in the design of security mechanism.

MTC Security

- Machine-to-Machine communication is required
  - Secure communication among MTC devices without an MTC server is likely to become a dominant communication paradigm.
  - Thus, the LTE networks need to establish end-to-end secure mechanisms for machine-to-machine communication between two MTC devices.
- The group authentication is required
  - It is possible that a mass of devices could become active at the same time resulting in much signalling overload and congestion over the networks. To combat the congestions, the preferred way is to make a large number of MTC devices to form a MTC group and the network can handle the MTC group orderly instead of messy individual devices.
  - Group access authentication scheme for the simultaneous authentication of multiple devices at the same time is required.

Other Security Issues

- More security mechanisms need to be designed to protect the communication between the UEs, eNBs (HeNB) and the EPC from traditional protocol attacks and physical intrusions in the LTE networks.
- The EPS-AKA scheme in the LTE networks needs to be further enhanced to be able to prevent the disclosure of user identity, the DoS attacks and other malicious attacks with much better performance of the authentication, especially when an UE access to the EPC via non-3GPP networks.

Other Security Issues

- More efficient handover authentication architecture needs to be designed to achieve the secure seamless handovers between the HeNBs and the eNBs and the handovers between 3GPP networks and non-3GPP networks with aims to overcome the inefficiency and incompatibility of the current solutions.
- The key management mechanisms and handover authentication procedures need to be further enhanced in the LTE networks to prevent several protocol attacks including desynchronization attacks and reply attacks.

Other Security Issues

- Fast and robust IMS access authentication mechanisms need to be designed to simplify the authentication process and prevent DoS attacks and other malicious attacks.
- Simple and robust mutual authentication mechanisms between the UEs and the HeNBs need to be designed to prevent various protocol attacks with less computation overhead while to be compatible to the LTE architecture by the current 3GPP standard.

Conclusion

- In this speech, we have overviewed the security framework and various security mechanisms designed in the LTE networks by the 3GPP standard.
- We have further explored various vulnerabilities existing in the security framework and the security mechanisms of 4G LTE networks.
- Moreover, we have extensively reviewed various current existing solutions to enhance the security provisioning in the LTE networks.
- Furthermore, we have summarized a few open research issues for future research with aims to attract and promote further research on this topic.
- We expect that all addressed issues could help to promote further academic research in this field.

Reference

1. G. M. Koien, "Mutual Entity Authentication for LTE," *Proceedings of 7th International Wireless Communications and Mobile Computing Conference (IWCMC)*, July 2011, pp.689-694.
2. M. Purkhiabani and A. Salahi, "Enhanced Authentication and Key Agreement Procedure of Next Generation Evolved Mobile Networks," *Proceedings of IEEE 3rd International Conference on Communication Software and Networks (ICCSN)*, May 2011, pp.557-563.
3. Y. Zheng, D. He, X. Tang, and H. Wang, "AKA and Authorization Scheme for 4G Mobile Networks Based on Trusted Mobile Platform," *Proceedings of Fifth International Conference on Information, Communications and Signal Processing*, 2005, pp.976-980.
4. D. He, J. Wang, and Y. Zheng, "User Authentication Scheme Based on Self-certified Public-key for Next Generation Wireless Network," *Proceedings of Biometrics and Security Technologies (ISBAST 2008)*, April 2008, pp.1-8.
5. Z. Shi, Z. Ji, Z. Gao, and L. Huang, "Layered Security Approach in LTE and Simulation," *Proceedings of Anti-counterfeiting, Security, and Identification in Communication (ASID 2009)*, August 2009, pp.171-173.
6. X. Li, and Y. Wang, "Security Enhanced Authentication and Key Agreement Protocol for LTE/SAE Network," *Proceedings of Wireless Communications, Networking and Mobile Computing (WiCOM)*, September 2011, pp.1-4.
7. C. Vintila, V. Patriciu, and I. Bica, "Security Analysis of LTE Access Network", *Proceedings of The Tenth International Conference on Networks (ICN 2011)*, January 2011, pp. 29-34.

Reference

8. J. Abdo, H. Chaouchi, and M. Aoude, "Ensured Confidentiality Authentication and Key Agreement Protocol for EPS," *Proceedings of Broadband Networks and Fast Internet (RELABIRA 2012)*, May 2012, pp.73-77..
9. J. Cao, H. Li, M. Ma, Y. Zhang, and C. Lai, “A Simple and Robust Handover Authentication between HeNB and eNB in LTE Networks,” *Computer Networks*, Vol. 56, No. 8, May 2012, pp. 2119-2131.
10. Y. Zheng, D. He, L. Xu, and X. Tang, "Security Scheme for 4G Wireless Systems," *Proceedings of Communications, Circuits and Systems*, May 2005, pp. 397- 401.
11. J. Cao, M. Ma, and H. Li, “An Uniform Handover Authentication between E-UTRAN and Non-3GPP Access Networks,” *IEEE Transaction on Wireless Communications*, accepted for publication.
12. N. Krichene and N. Boudriga, "Securing Roaming and Vertical Handover in Fourth Generation Networks," *Proceedings of Network and System Security (NSS '09)*, October 2009, pp.225-231.
13. I. Bouabidi, I. Daly, and F. Zarai, "Secure Handoff Protocol in 3GPP LTE Networks," *Proceedings of Third International Conference on Communications and Networking (ComNet)*, March 2012, pp.1-6.
14. R. Rajavelsamy and S. Choi, "Security Aspects of Inter-access System Mobility between 3GPP and Non-3GPP networks," *Proceedings of Communication Systems Software and Middleware and Workshops (COMSWARE)*, January 2008, pp.209-213.
15. A. A. Al Shidhani and V. C. M. Leung, "Fast and Secure Reauthentications for 3GPP Subscribers during WiMAX-WLAN Handovers," *IEEE Transactions on Dependable and Secure Computing*, Vol.8, No.5, Septmber-Octomber 2011, pp.699-713.

Reference

16. C. Ntantogian, C. Xenakis, and I. Stavrakakis, "Efficient Authentication for Users Autonomy in Next Generation All-IP Networks," *Proceedings of Bio-Inspired Models of Network, Information and Computing Systems*, December 2007, pp.295-300.
17. M. Abid, S. Song, H. Moustafa, and H. Afifi, “Efficient Identity-based Authentication for IMS Based Services Access,” *Proceedings of the 7th International Conference on Advances in Mobile Computing and Multimedia (MoMM '09)*, 2009, pp. 260-266.
18. L. Gu and M.A. Gregory, "A Green and Secure Authentication for the 4th Generation Mobile Network," *Proceedings of Australasian Telecommunication Networks and Applications Conference (ATNAC)*, November 2011, pp.1-7.
19. C. K. Han, H. K. Choi and I. H. Kim, “Building Femtocell More Secure with Improved Proxy Signature”, *Proceedings of IEEE GLOBECOM 2009*, USA, December 2009, pp. 1-6.
20. I. Bilogrevic, M. Jadliwala and J-P. Hubaux, “Security and Privacy in Next Generation Mobile Networks: LTE and Femtocells,” *Proceedings of Femtocell Workshop*, June 2010.
21. H. Chen, Z. Fu, and D. Zhang, "Security and Trust Research in M2M System," *Proceedings of IEEE International Conference on Vehicular Electronics and Safety (ICVES)*, July 2011, pp.286-290.
22. R. Lu, X. Li, X. Liang, X. Shen, and X. Lin, "GRS: The Green, Reliability, and Security of Emerging Machine to Machine Communications," *IEEE Communications Magazine*, Vol.49, No.4, April 2011, pp.28-35.
23. Y. W. Chen, J. T. Wang, K. H. Chi, and C. C. Tseng, “Group-Based Authentication and Key Agreement”, *Wireless Personal Communications*, 2010, pp. 1-15.