Breaking LTE on Layer two

David Rupprecht, Katharina Kohls, Thorsten Holz, Christina Pöpper

IEEE S&P'19

Presentor : Hansung Bae

LTE Security Goals

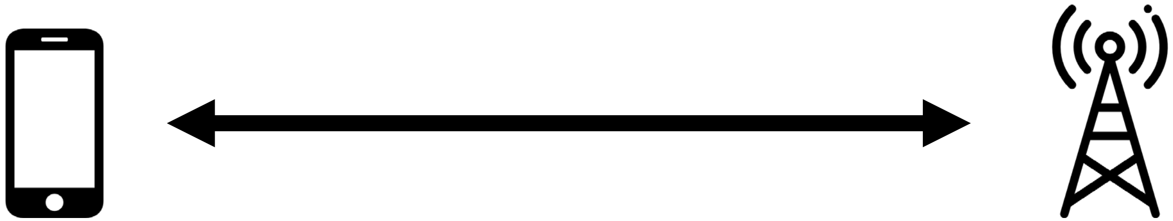
- ❖ Mutual Authentication

- ❖ Traffic confidentiality

- ❖ Identity & Location Confidentiality

Primitive for Security Goals

- AKA : Authentication and Key agreement procedure

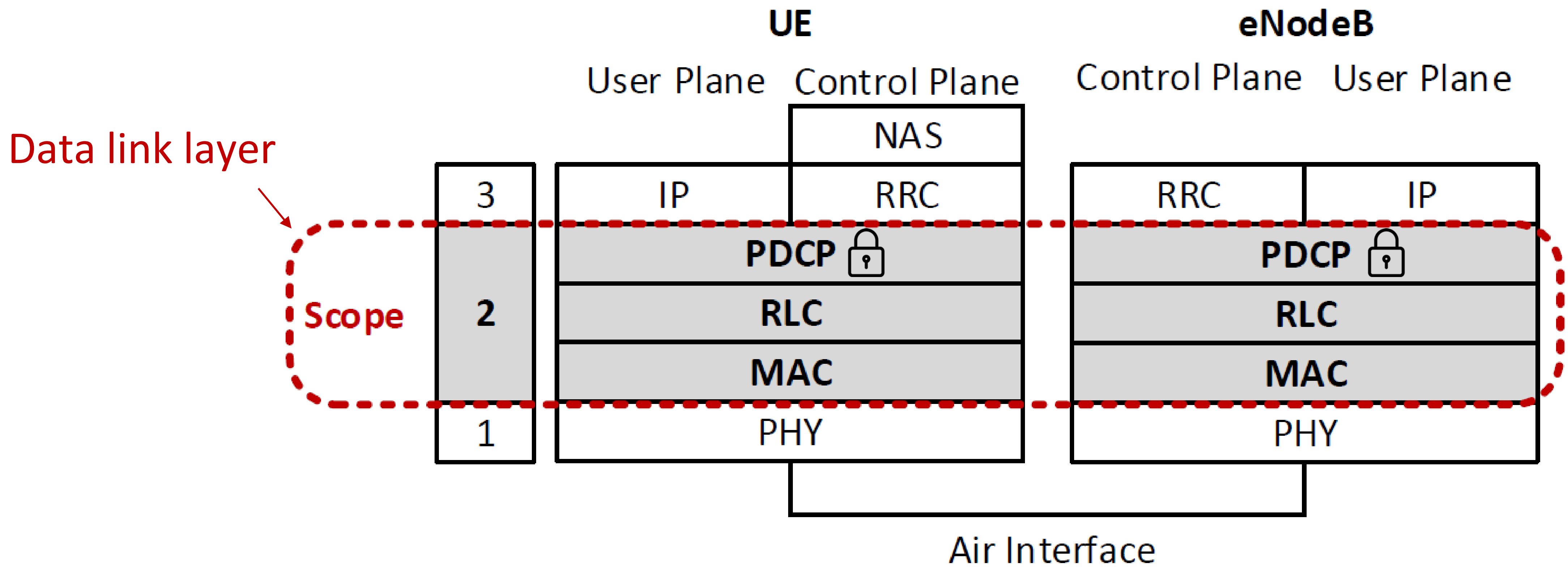


- Mutual authentication + traffic confidentiality (using shared keys).

- Still have problems?

Protection on layer two

- Where are security measures implemented?

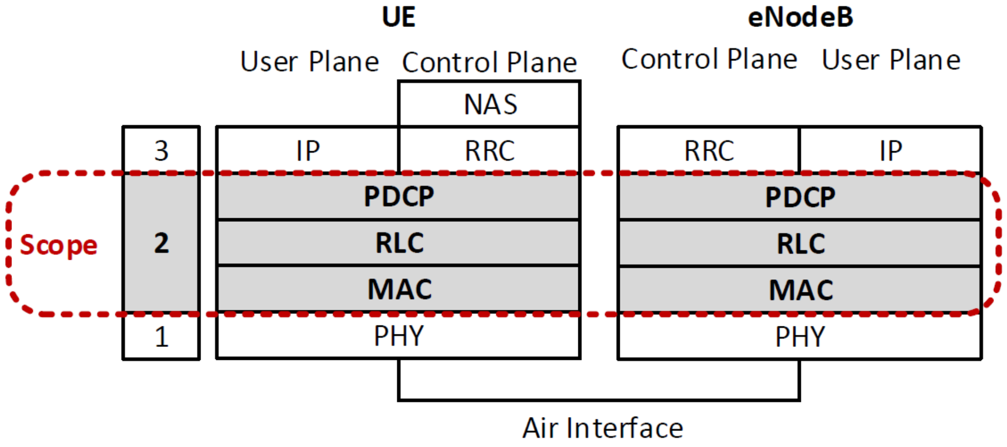


- RLC, MAC, PHY layer traffic is not security protected.

Control vs User plane protection

- Control Plane : Controls how data packets are forwarded.
- User Plane : Carries the network user data.
- Implementations on PDCP layer

	Control Plane	User Plane
Encryption	O	O
Integrity Protection	O	X



UE

User Plane | Control Plane

NAS

IP | RRC

PDCP

RLC

MAC

PHY

eNodeB

Control Plane | User Plane

RRC | IP

PDCP

RLC

MAC

PHY

3

2

1

Scope

Air Interface

Introduction

- Main vulnerabilities
  - Vuln1: RLC, MAC, PHY layer do not provide confidentiality and integrity.
  - Vuln2: Integrity protection is not implemented on User Plane.

- Attacks
  - Identity Mapping Attack: Vuln1
  - Website Fingerprinting Attack: Vuln1
  - aLTEr Attack: Vuln2

1. Identity Mapping Attack

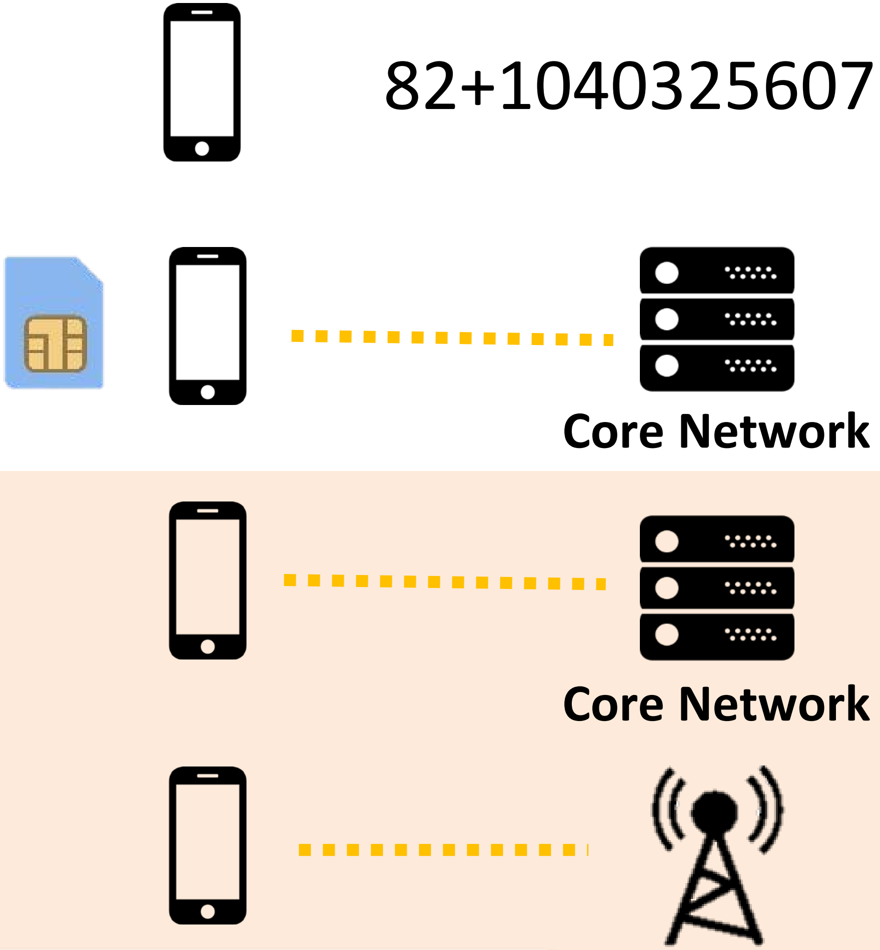
1. Identity Mapping Attack

- Identity mapping attack
  - Match permanent identity and temporary identity.
  - Match temporary identity 1 and temporary identity 2

- Why do we use temporary identities?
  - If only permanent identities are used, user activities can be tracked.

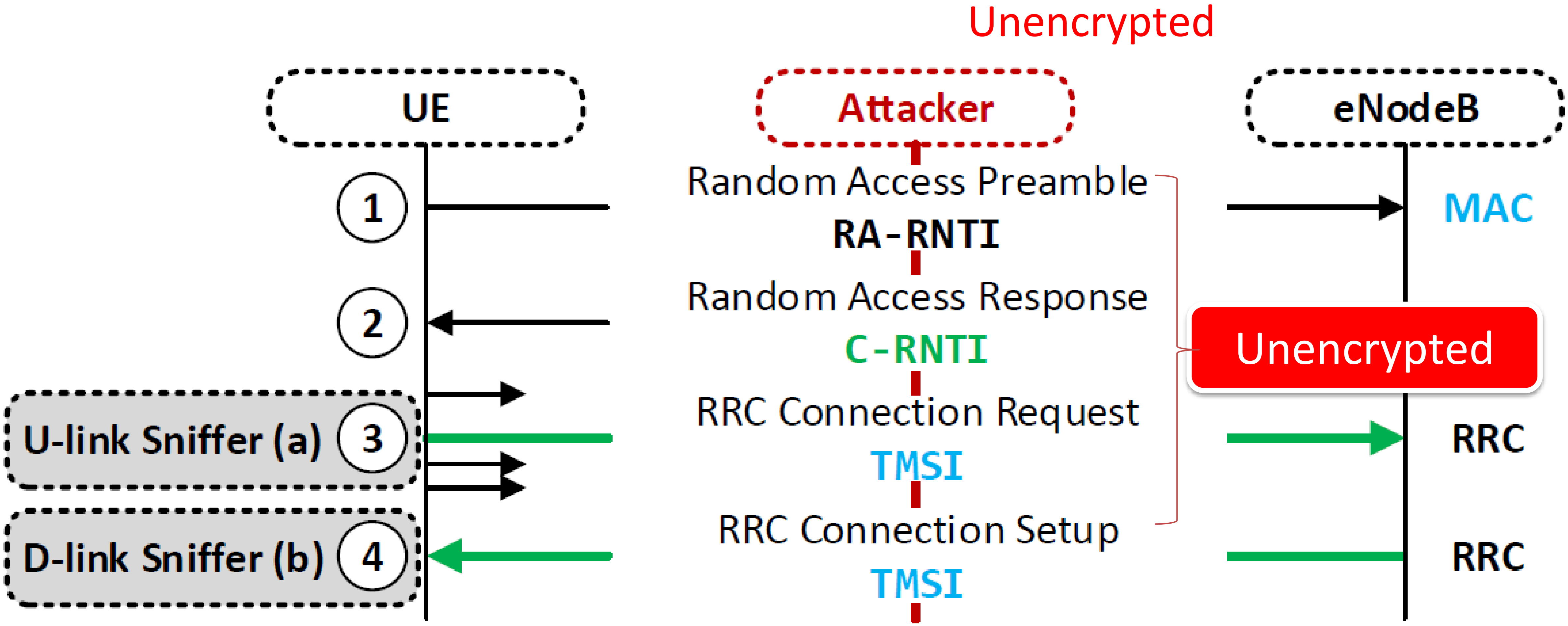
1. Identity Mapping Attack

- ❖ Phone Number
- ❖ Permanent identity IMSI
- ❖ Temporary network identity TMSI
- ❖ Temporary radio identity RNTI



Adversary maps TMSI and RNTI

1. Identity Mapping Attack

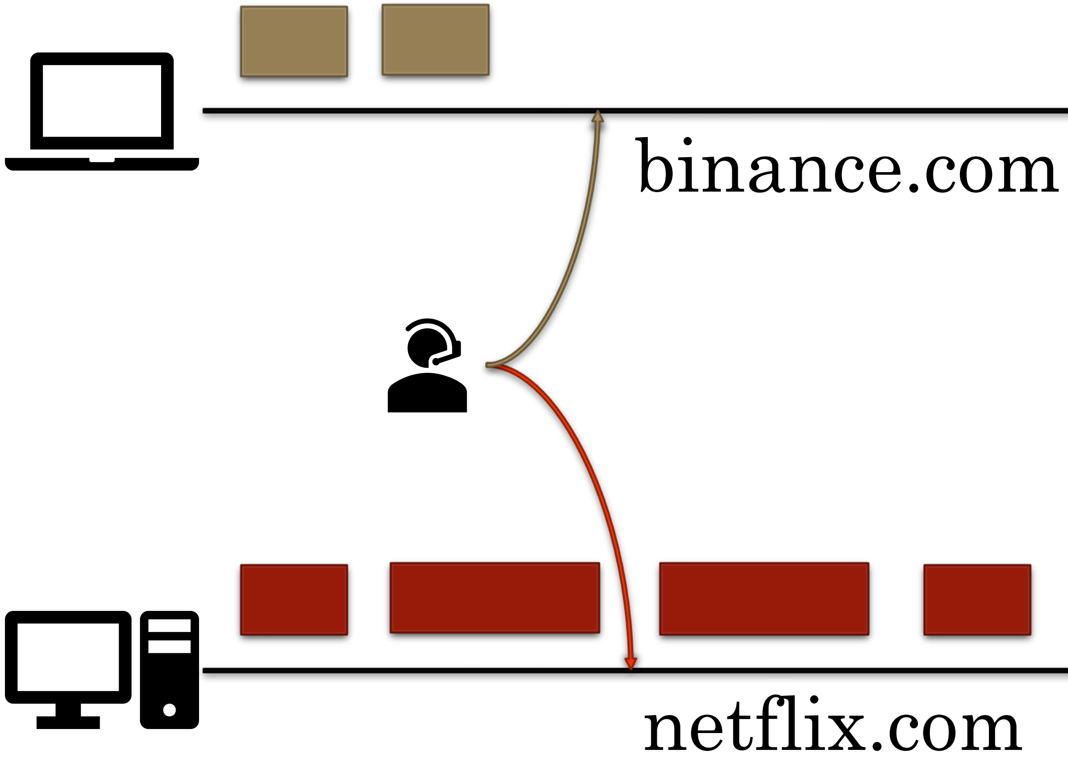


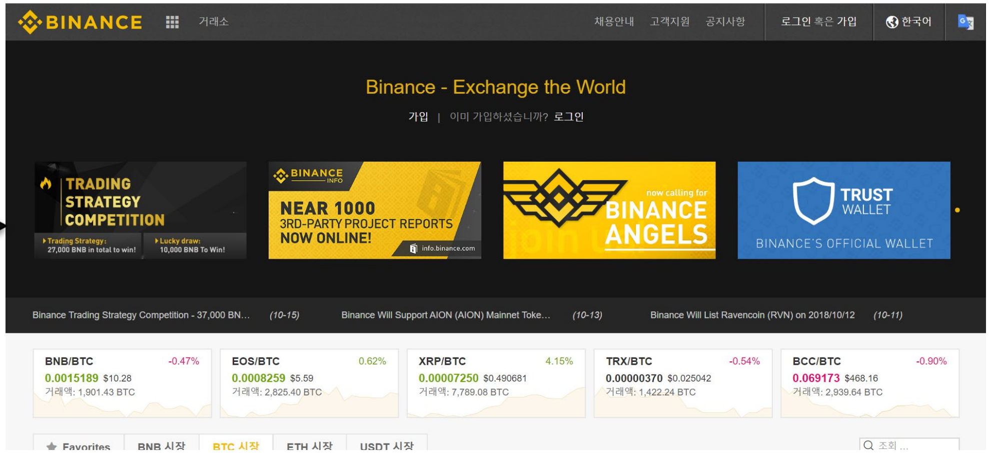
1. Identity Mapping Attack

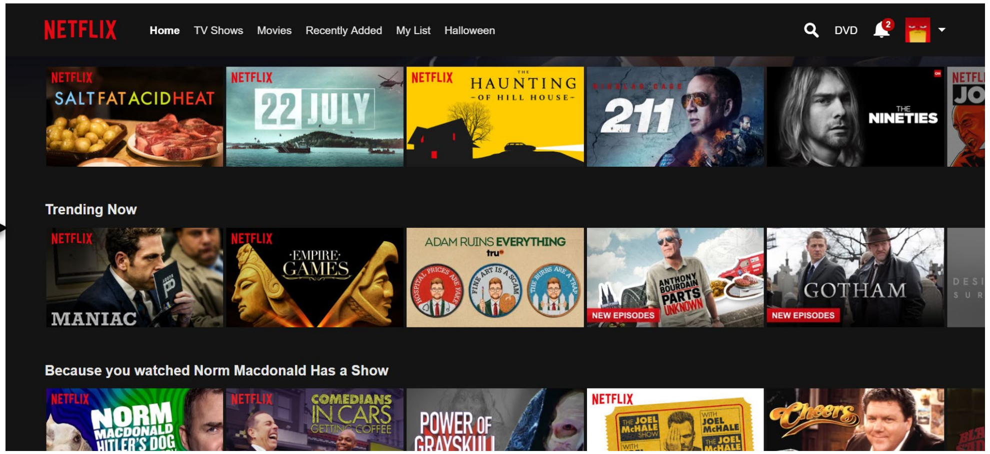
- Experiments & Results
  - Authors recorded about 96000 connection establishment procedures.
    - Using downlink sniffer
    - Eavesdropped RAR packet for C-RNTI, and RRC Connection setup message for TMSI.
  - About 95% of success.

2. Website Fingerprinting Attack

2. Website Fingerprinting Attack




BINANCE
거래소
채용안내 고객지원 공지사항
로그인 혹은 가입
한국어
Binance - Exchange the World
가입 | 이미 가입하셨습니까? 로그인
TRADING STRATEGY COMPETITION
NEAR 1000 3RD-PARTY PROJECT REPORTS NOW ONLINE!
BINANCE ANGELS
TRUST WALLET
BINANCE'S OFFICIAL WALLET
Binance Trading Strategy Competition - 37,000 BN... (10-15)
Binance Will Support AION (AION) Mainnet Toke... (10-13)
Binance Will List Ravencoin (RVN) on 2018/10/12 (10-11)
BNB/BTC -0.47% 0.0015189 $10.28 거래액: 1,901.43 BTC
EOS/BTC 0.62% 0.0008259 $5.59 거래액: 2,825.40 BTC
XRP/BTC 4.15% 0.00007250 $0.490681 거래액: 7,789.08 BTC
TRX/BTC -0.54% 0.00000370 $0.025042 거래액: 1,422.24 BTC
BCC/BTC -0.90% 0.069173 $468.16 거래액: 2,939.64 BTC
Favorites
BNB 시장
BTC 시장
ETH 시장
USDT 시장



2. Website Fingerprinting Attack

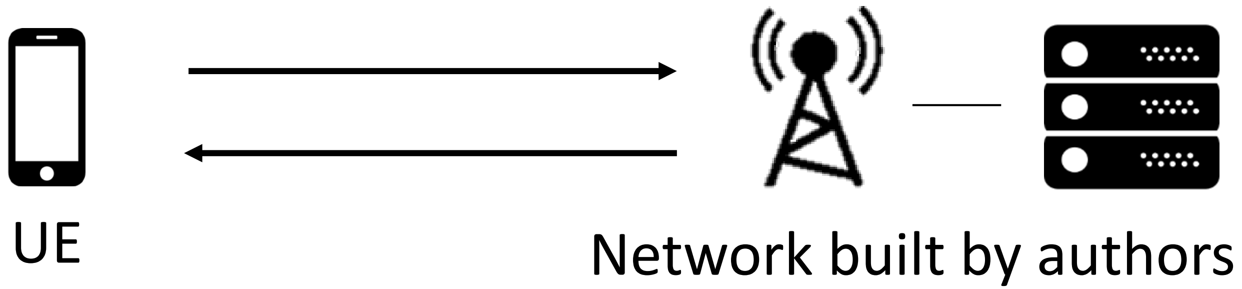
- Vulnerability : Absence of data encryption on MAC layer
  - Passive adversary can decode DCI information on MAC layer.
  - From DCI, attacker learns user data traffic and gain metadata features.
    - Can distinguish requests to different websites.
    - E.g. Length of PDCP packet, timing patterns of transmissions

- Attack procedure
  1) Create a training set of user traffic, accessing to multiple websites.
  2) Apply Fast Dynamic Time Warping (DTW) to the set.
  3) Classification attack

Computes similarity of two time series

2. Website Fingerprinting Attack

- Experiments



  - Collected user plane traffic at eNB.
  - Used 3 Android phones.
  - Accessed to Alexa top 50 websites, overall 100 times with each phone.

- Result : About 90% success rate for both uplink and downlink.

3. aLTEr Attack

3. aLTEr Attack

- aLTEr attack
  - Manipulates known part of encrypted LTE user traffic.

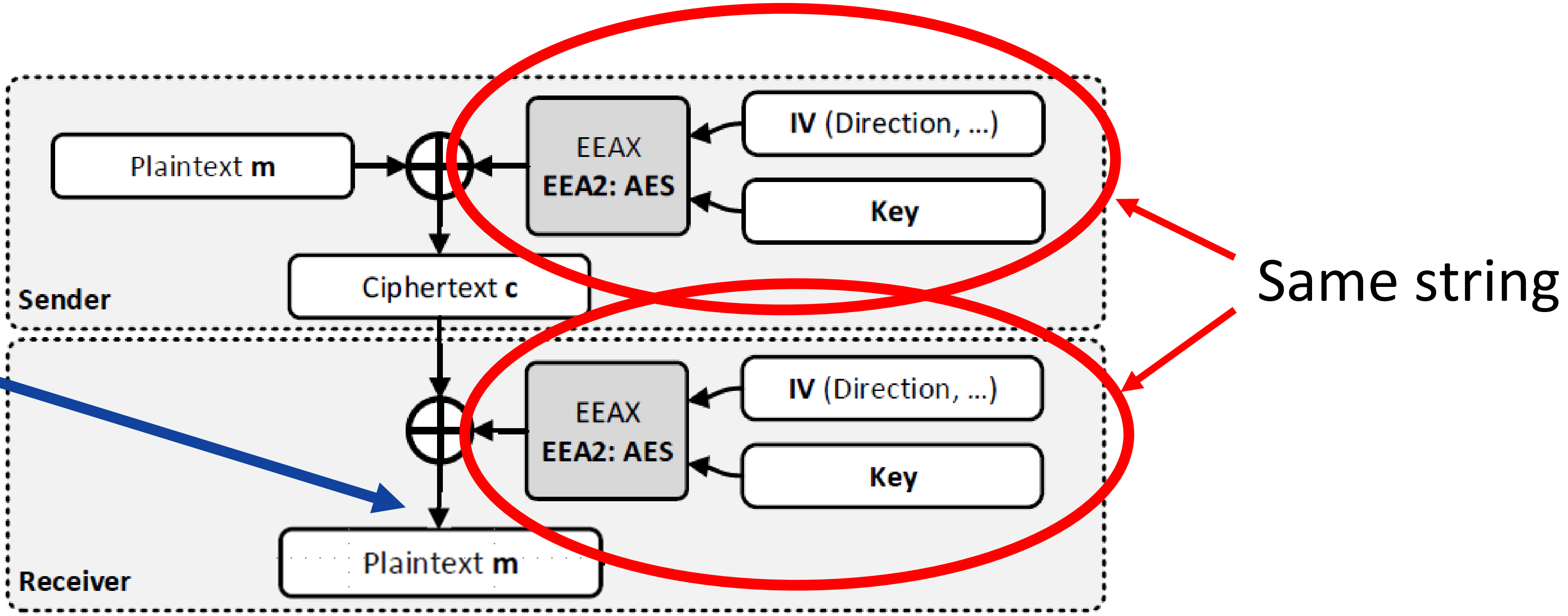
- Vulnerability
  - Lack of integrity protection on user plane.
  - Encryption on LTE user data is performed by block ciphering in counter mode.

	Control Plane	User Plane
Encryption	O	O
Integrity Protection	O	X

3. aLTEr Attack

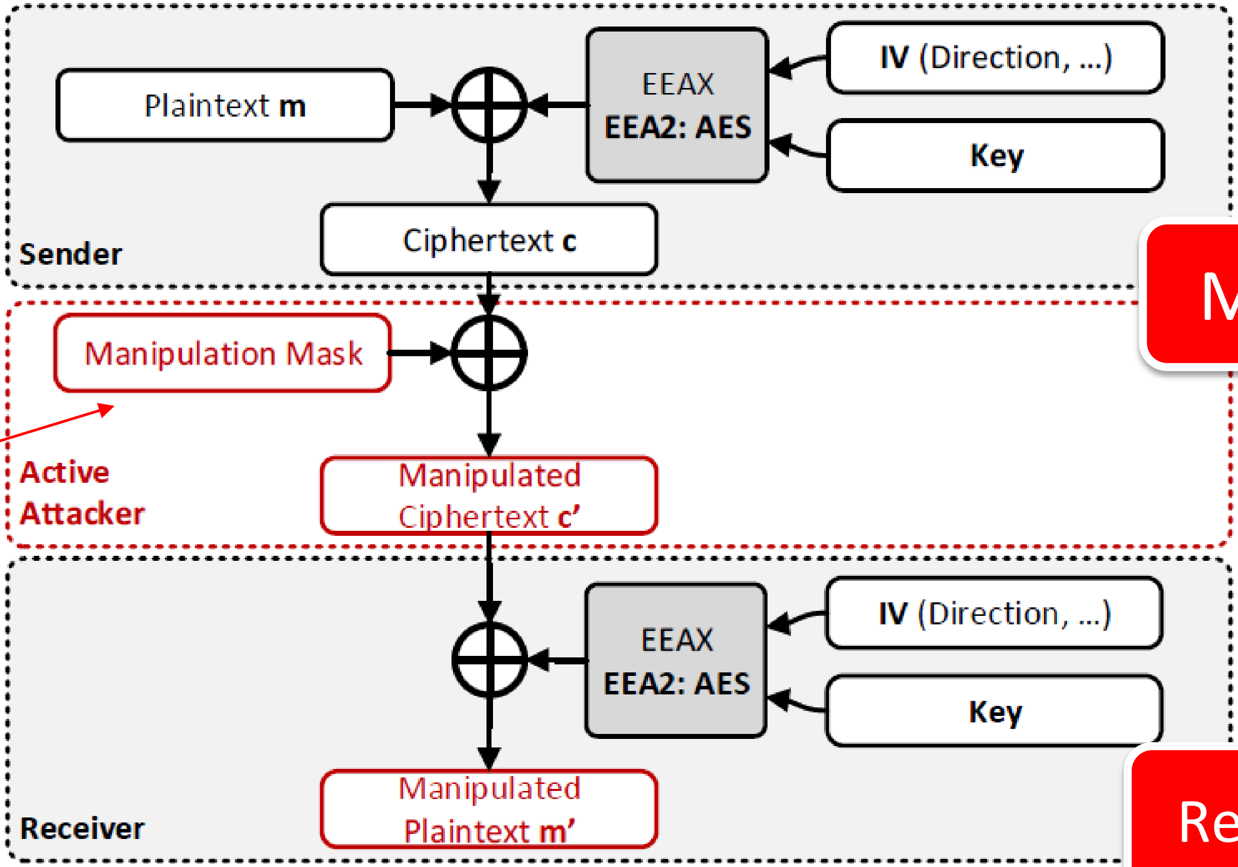
- Data encryption – AES CTR

$X \oplus X \oplus Y = Y$



3. aLTEr Attack

- Packet modification
  - Known plaintext m, manipulated text m’.



Inserted block by an attacker

Mask = m ⊕ m'

Result = MASK ⊕ m

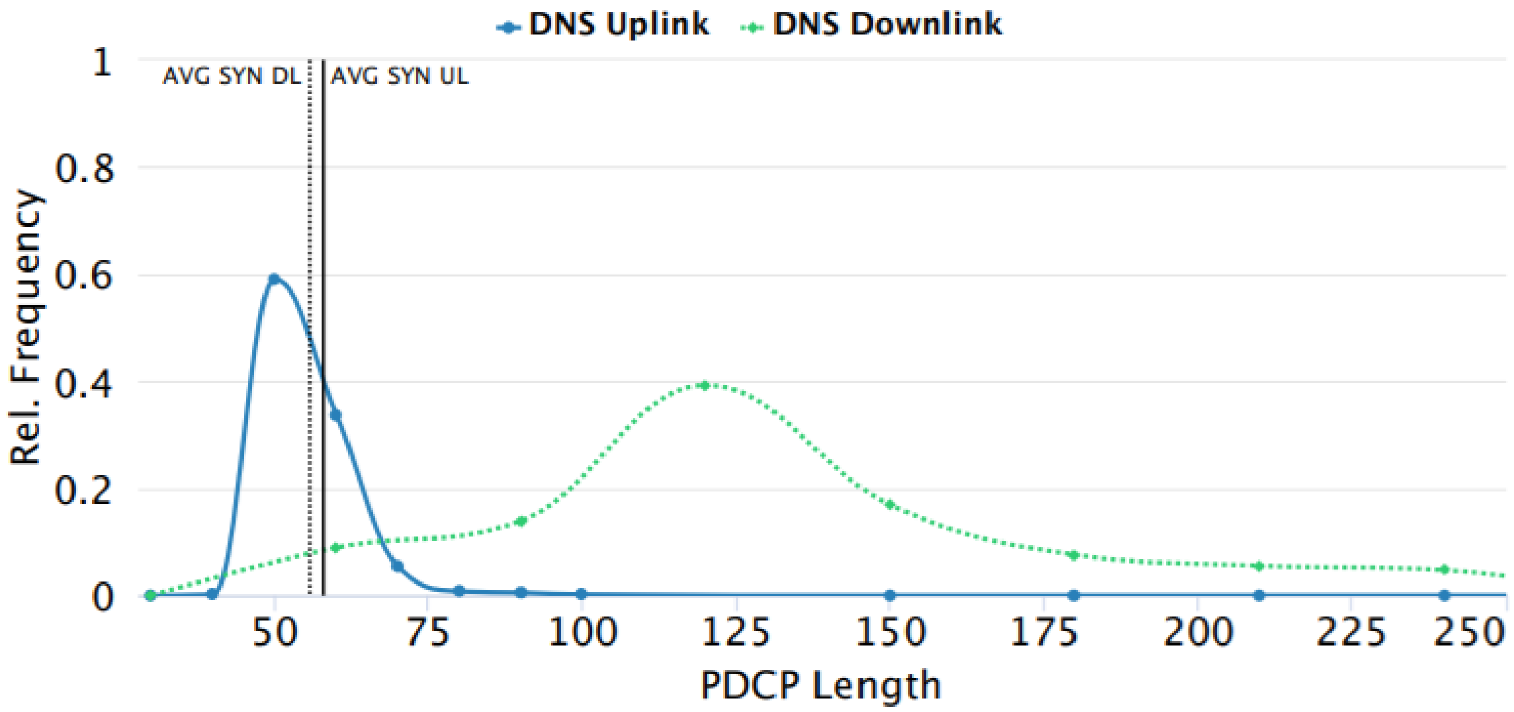
3. aLTEr Attack

- Found that adversary can deliver manipulated user plane traffic to receiver.
  - But original text should be known.

- Two challenges to design attack.
  - Chall1 : Selection of target traffic
    - How to distinguish target from encrypted user traffic?
  - Chall2 : Selection of target text to manipulate
    - Original text should be known.
    - Attack should be performed by the modification.

3. aLTEr Attack

- Overcome challenge 1 : Select DNS request/response as target.
  - DNS requests/responses are distinguishable from user traffic.
  - Using PDCP length as a feature, about 96% of accuracy.



3. aLTEr Attack

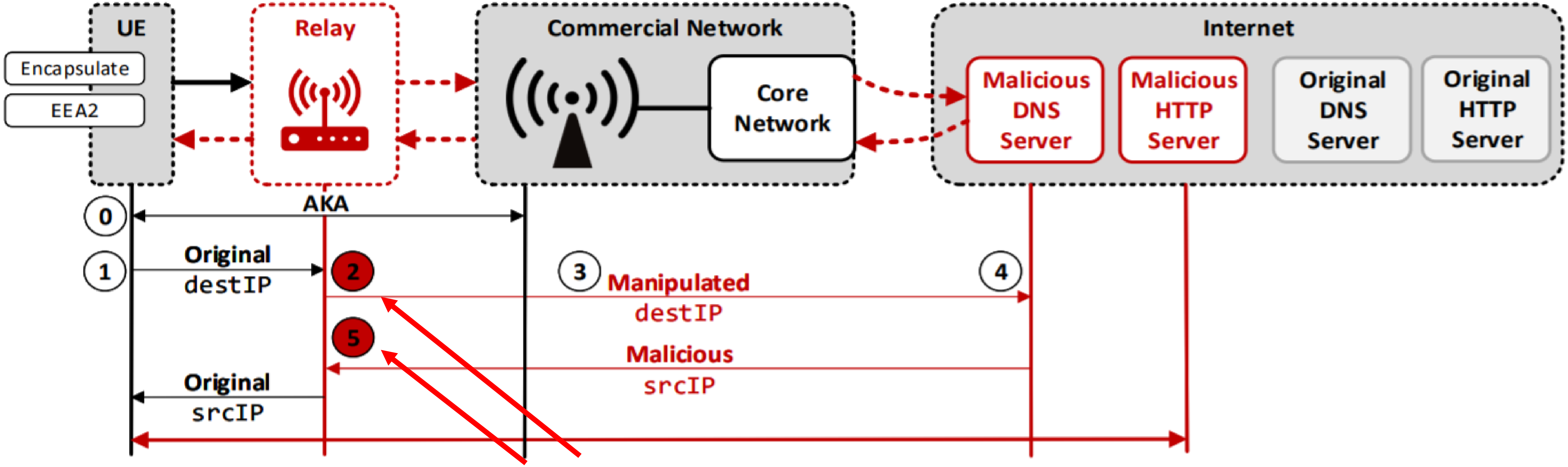
- Overcome challenge 2 : Modify IP address
  - By changing IP address, DNS redirection attack can be performed.

	DNS request	DNS response
Destination IP address	Known	
Source IP address		Known

- Modify IP address to redirect DNS request.
  - Also hide source of DNS response.

3. aLTEr Attack

- Overview of the attack procedure



MASK applied

3. aLTEr Attack

3. aLTEr Attack

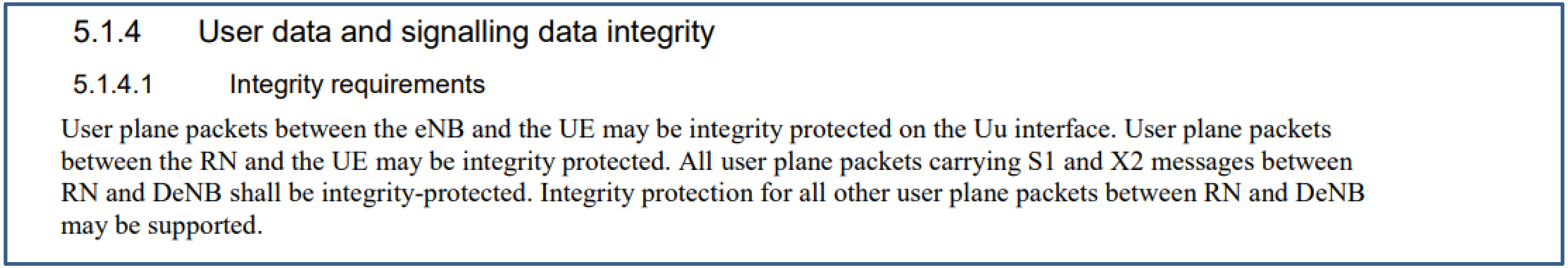
- Defense
  - Update standard so that integrity protection is provided to user plane data.
    - Why integrity protection is not used on user plane?
    - Increase of packet size, due to MAC.

IMP4GT Attack – Follow up study

- D. Rupprecht, K. Kohls, T. Holz, and C. Popper, “IMP4GT: Impersonation attacks in 4G networks,” in Proc. ISOC NDSS, Feb. 2020
  - Impersonation attack
    - Send packet to HTTP server with victim’s identity.
  - First perform aLTEr attack and use encryption/decryption oracle authors made.
    - Attack is possible due to same vulnerabilities.

User Plane Integrity Protection

- Taking a look on standard : 3GPP standard of LTE & 5G
  - **LTE : 33.401**

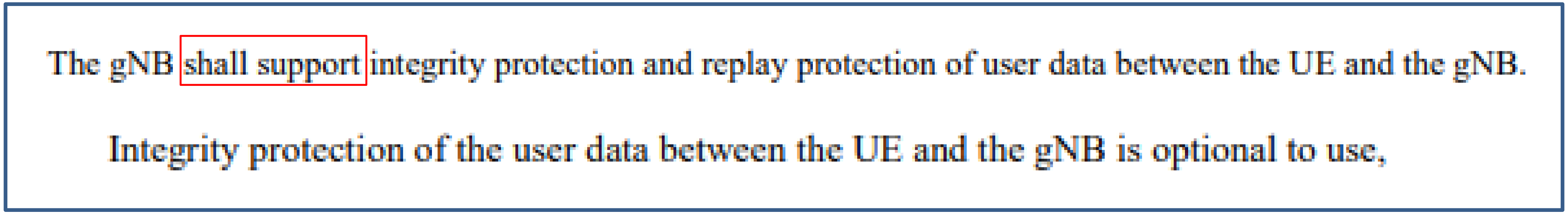


5.1.4 User data and signalling data integrity

5.1.4.1 Integrity requirements

User plane packets between the eNB and the UE may be integrity protected on the Uu interface. User plane packets between the RN and the UE may be integrity protected. All user plane packets carrying S1 and X2 messages between RN and DeNB shall be integrity-protected. Integrity protection for all other user plane packets between RN and DeNB may be supported.

  - **5G : 33.501**



The gNB shall support integrity protection and replay protection of user data between the UE and the gNB.

Integrity protection of the user data between the UE and the gNB is optional to use,

Related Works

- Cryptanalysis of the GPRS Encryption Algorithms GEA-1 and GEA-2 (Eurocrypt `21)
  - Vulnerability of encryption algorithms
- Call Me Maybe: Eavesdropping Encrypted LTE Calls With ReVoLTE (USENIX Security `20)
  - Vulnerability of counter mode in block cipher
  - A reset of counter value causes the keystream reuse
- Touching the untouchables: Dynamic Security Analysis of the LTE Control Plane (IEEE S&P 2019)
  - Bypassing key agreement procedure

Conclusion – Wrap up

- Identity Mapping Attack
  - Map RNTI and TMSI.
  - Identify and localize users in network.

- Website Fingerprinting Attack
  - Learn accessed website from metadata of encrypted traffic.
  - Distinguish accessed websites.

- ALTER Attack
  - Manipulates known part of encrypted LTE user traffic.
  - Redirection of DNS request from user.

Good Question

- Because the attack targets Layer 2, only network operators may be potential attackers. So, why would a network provider want to launch such an attack against a customer?

Best Question

- Is there any reason that integrity protection for the user plane is insufficient? (from 허현)

Best Question

- Is there a way or research to detect possible passive attack vectors from cellular network specifications or implementations? (from 김동욱)

Best Question

- During packet encryption, will using another block cipher method instead of AES-CTR mode help prevent ALTER attacks? (from 박승민)

Thank you