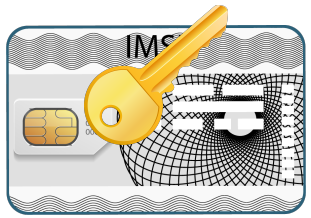
PennState

CSE 543: Computer Security
Module: Cellular Network Security

Prof. Syed Rafiul Hussain
Computer Science and Engineering Department
Pennsylvania State University

Cellular Device or User Equipment

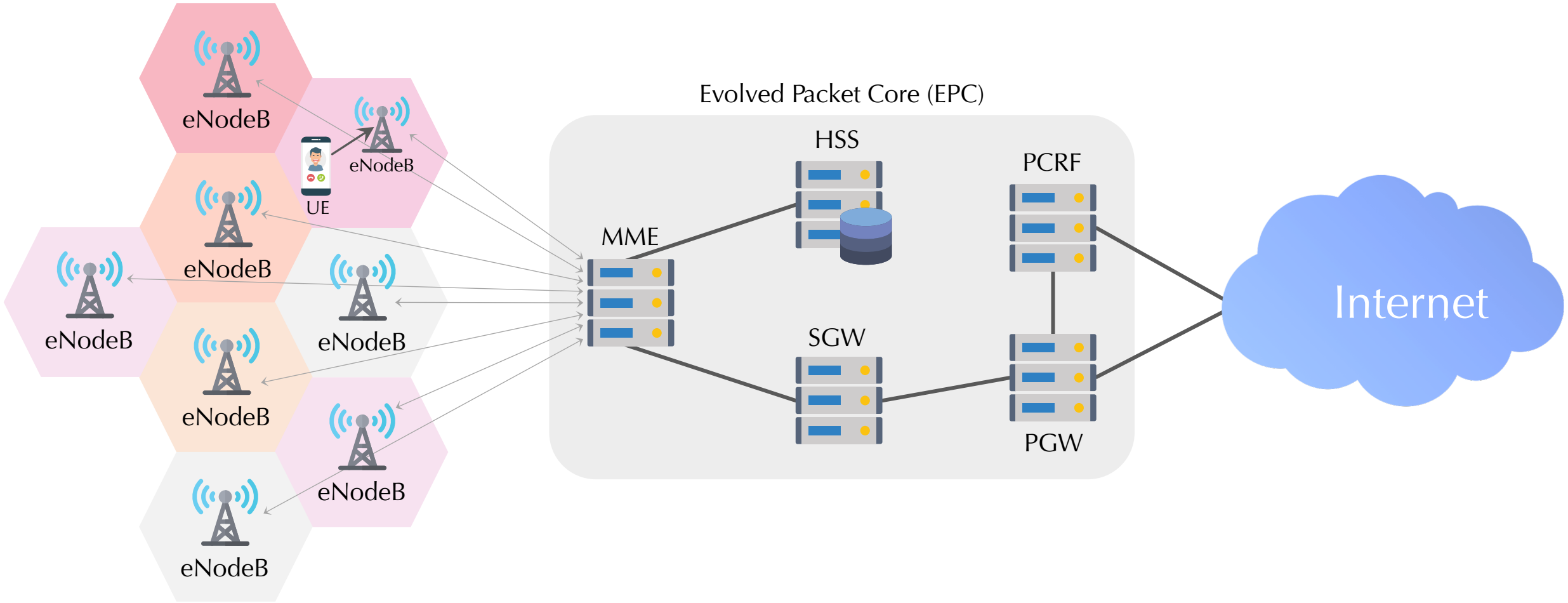
UE



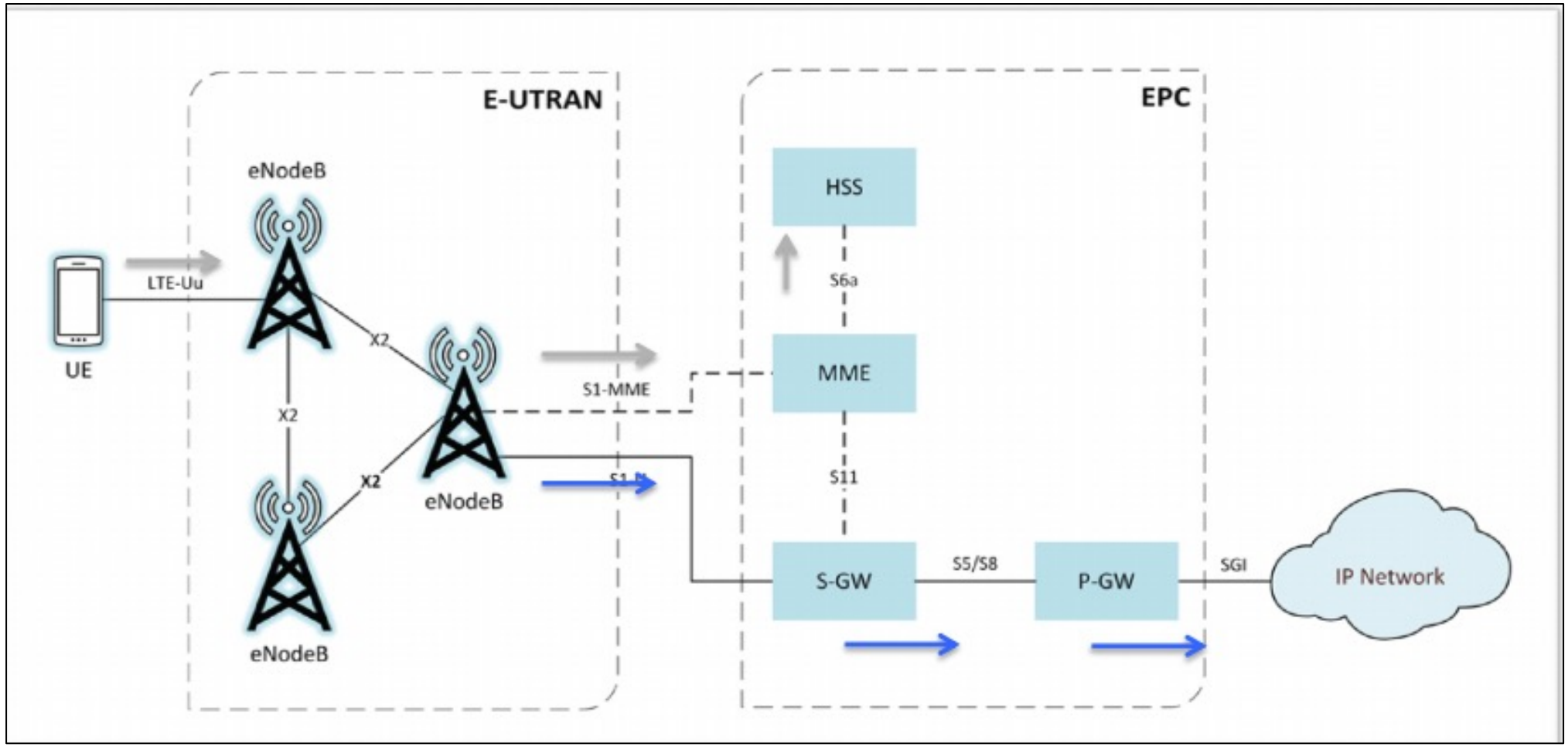
IMSI = International Mobile Subscriber Identity

IMEI = International Mobile Equipment Identity

Background: LTE Architecture

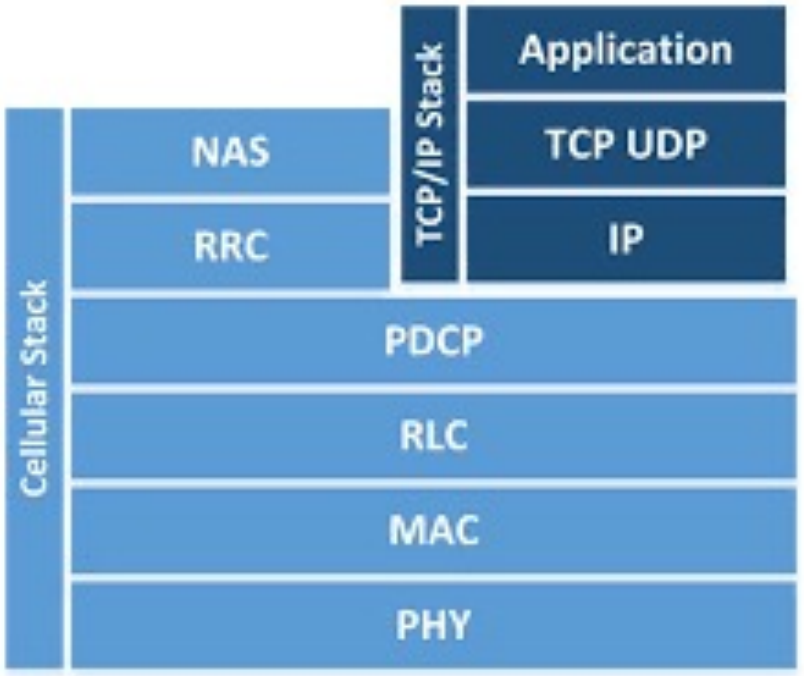


LTE Network

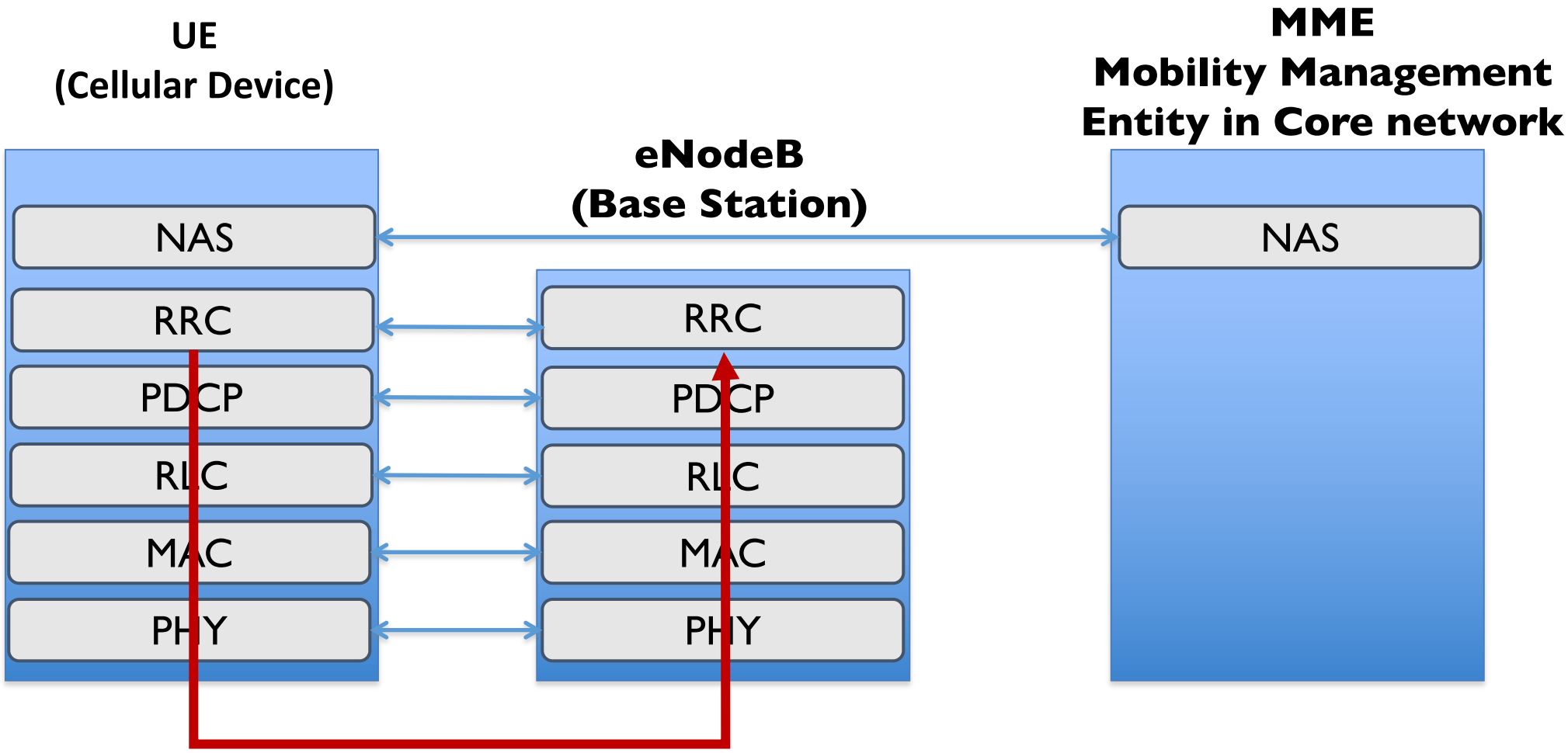

E-UTRAN
EPC
eNodeB
HSS
LTE-Uu
S6a
UE
X2
MME
S1-MME
X2
S11
X2
eNodeB
eNodeB
S-GW
S5/S8
P-GW
SGI
IP Network

Protocol Stack

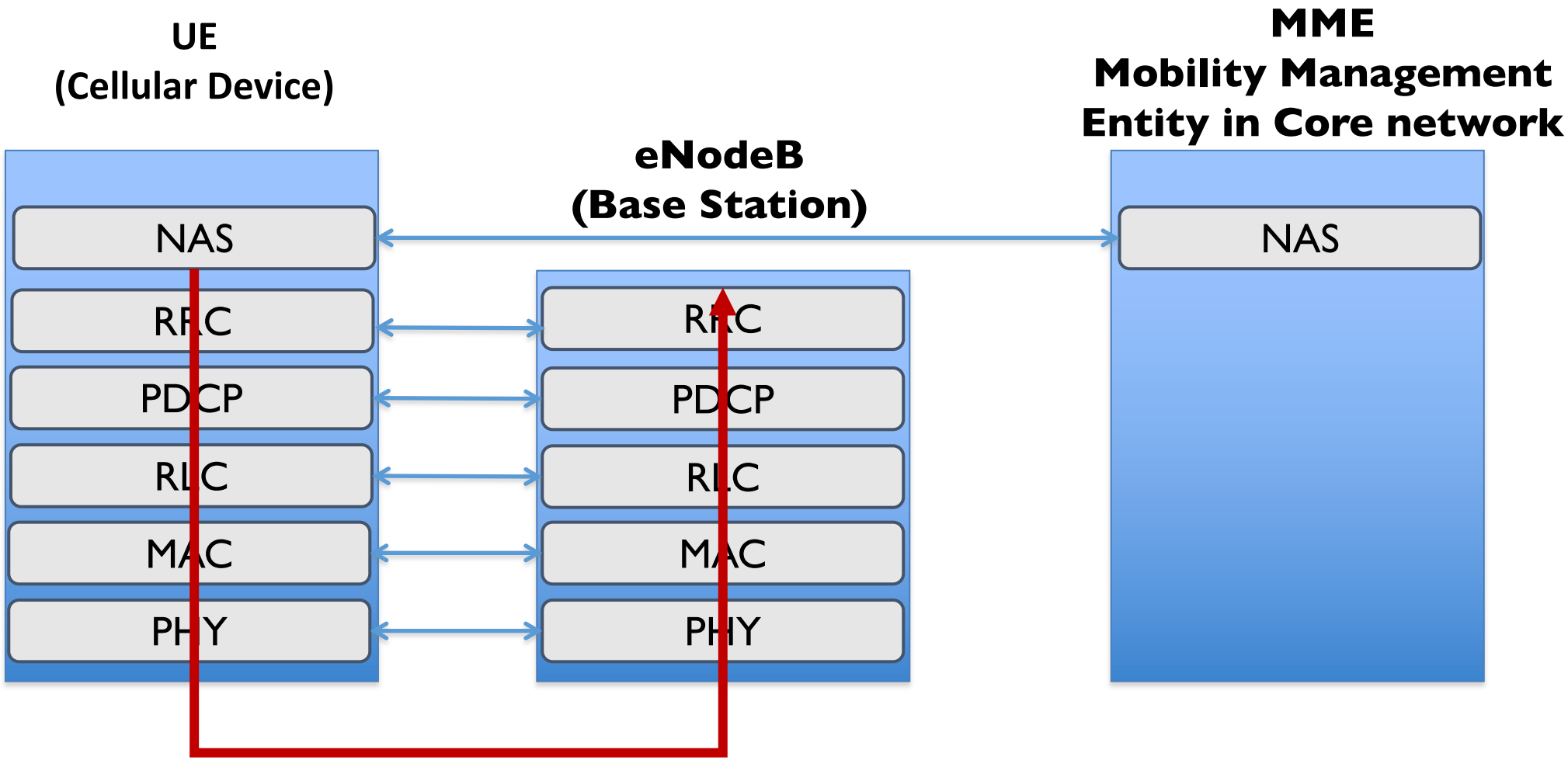
- TCP/IP sits on top of the cellular protocol stack:
- **Radio Resource Control (RRC):** Transfers NAS messages, AS information may be included, signaling, and ECM
- **Packet Data Convergence Protocol (PDCP):** header compression, radio encryption
- **Radio Link Control (RLC):** Readies packets to be transferred over the air interface
- **Medium Access Control (MAC):** Multiplexing, QoS



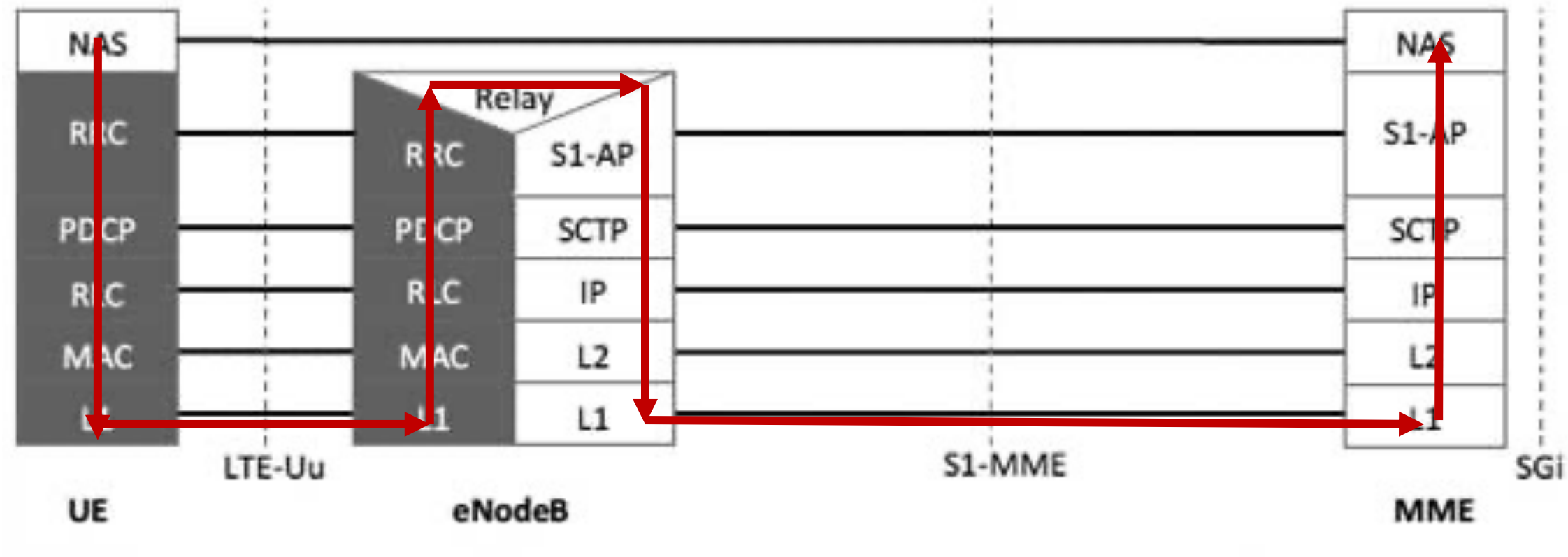
4G Control Plane Protocol Stack



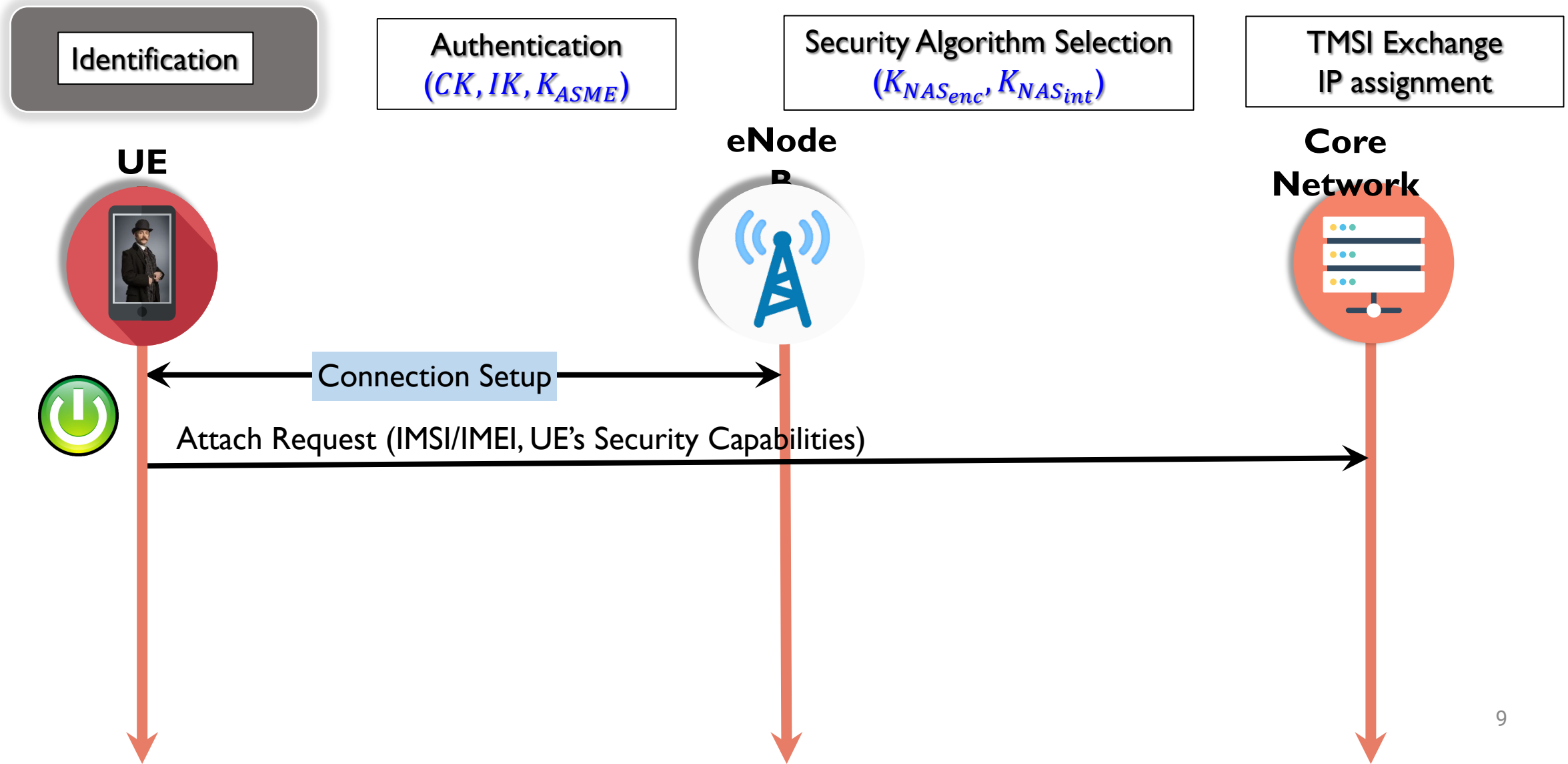
4G Control Plane Protocol Stack



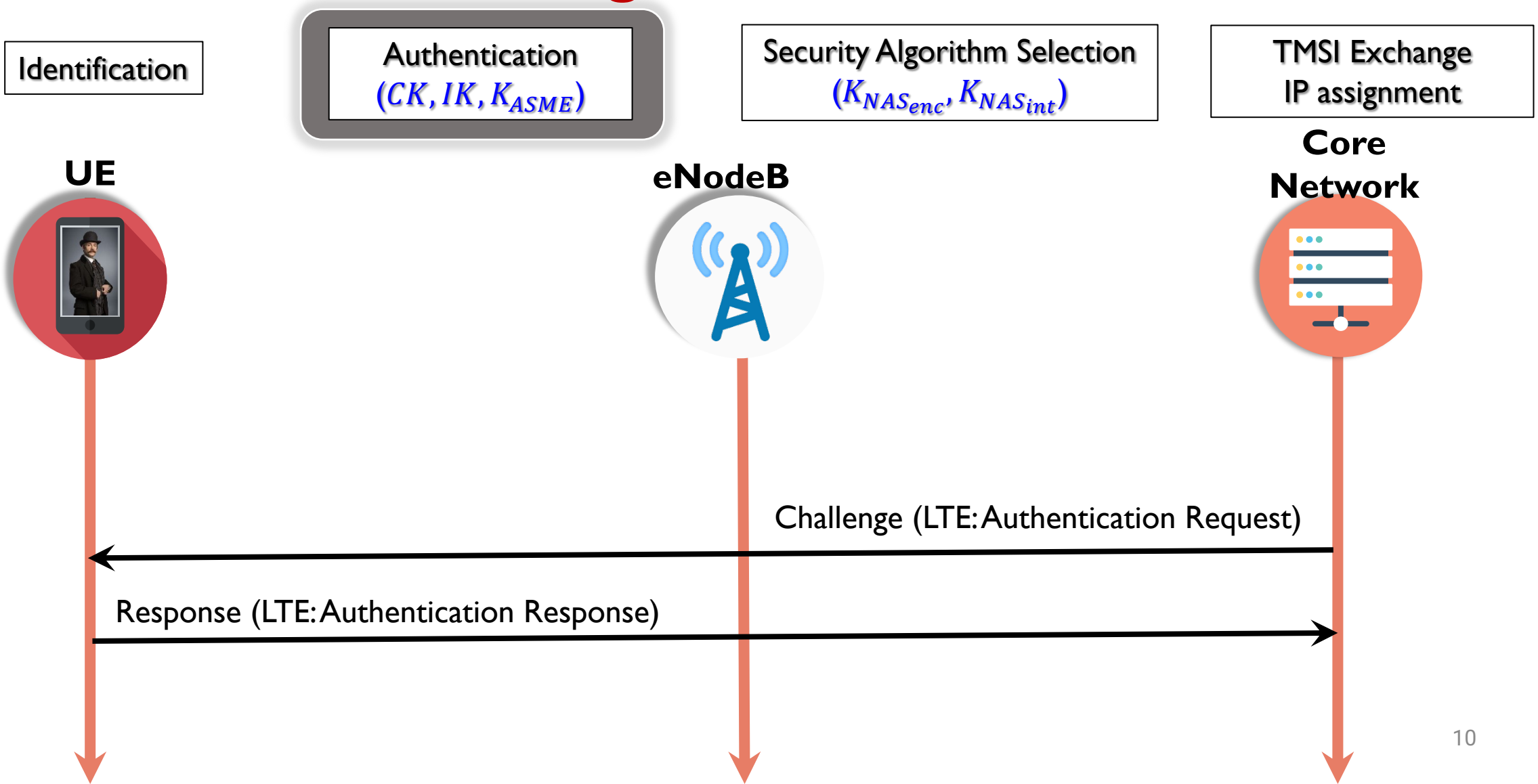
4G Control Plane Protocol Stack



Attach/Registration Procedure



Attach/Registration Procedure



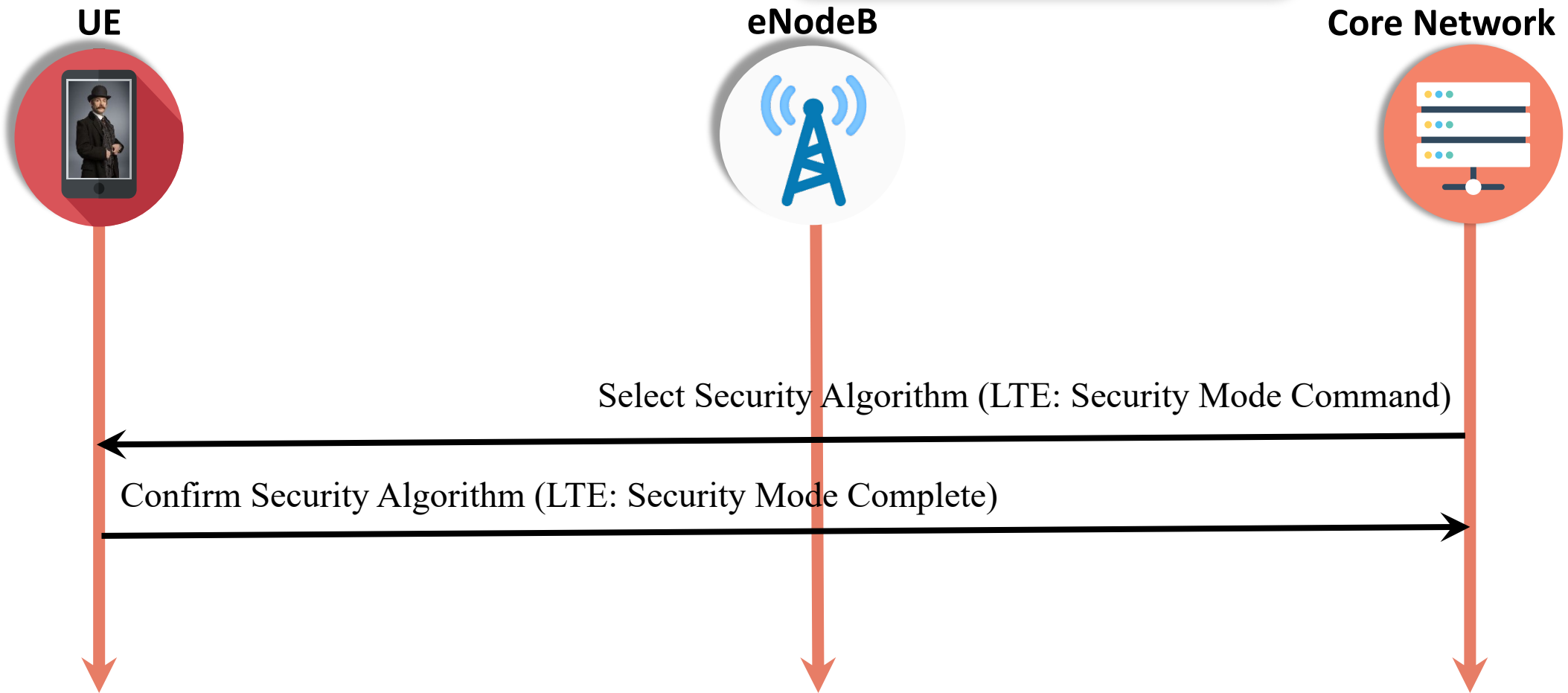
Attach/Registration Procedure

Identification

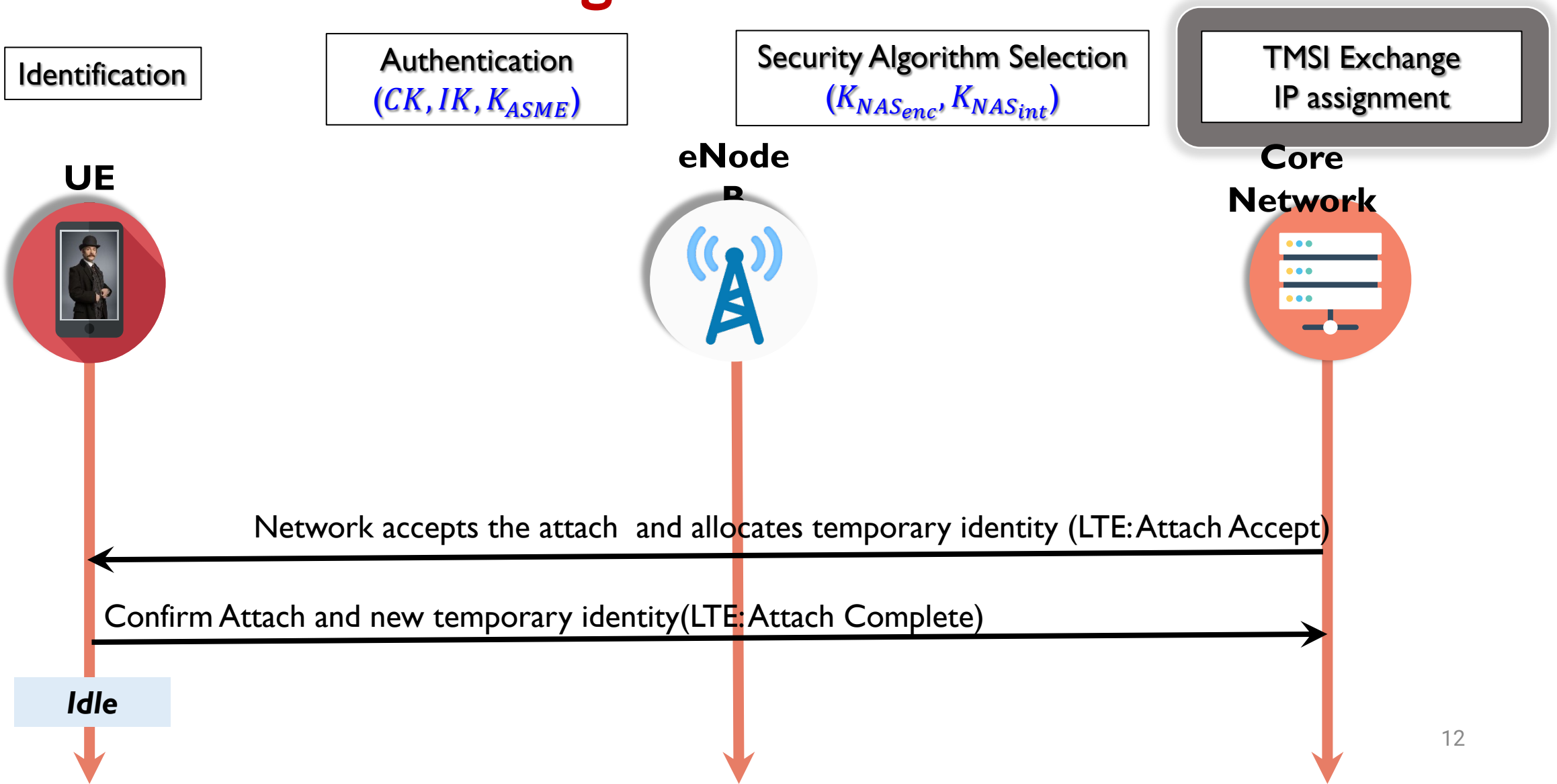
Authentication (CK, IK, K_{ASME})

Security Algorithm Selection $(K_{NAS_{enc}}, K_{NAS_{int}})$

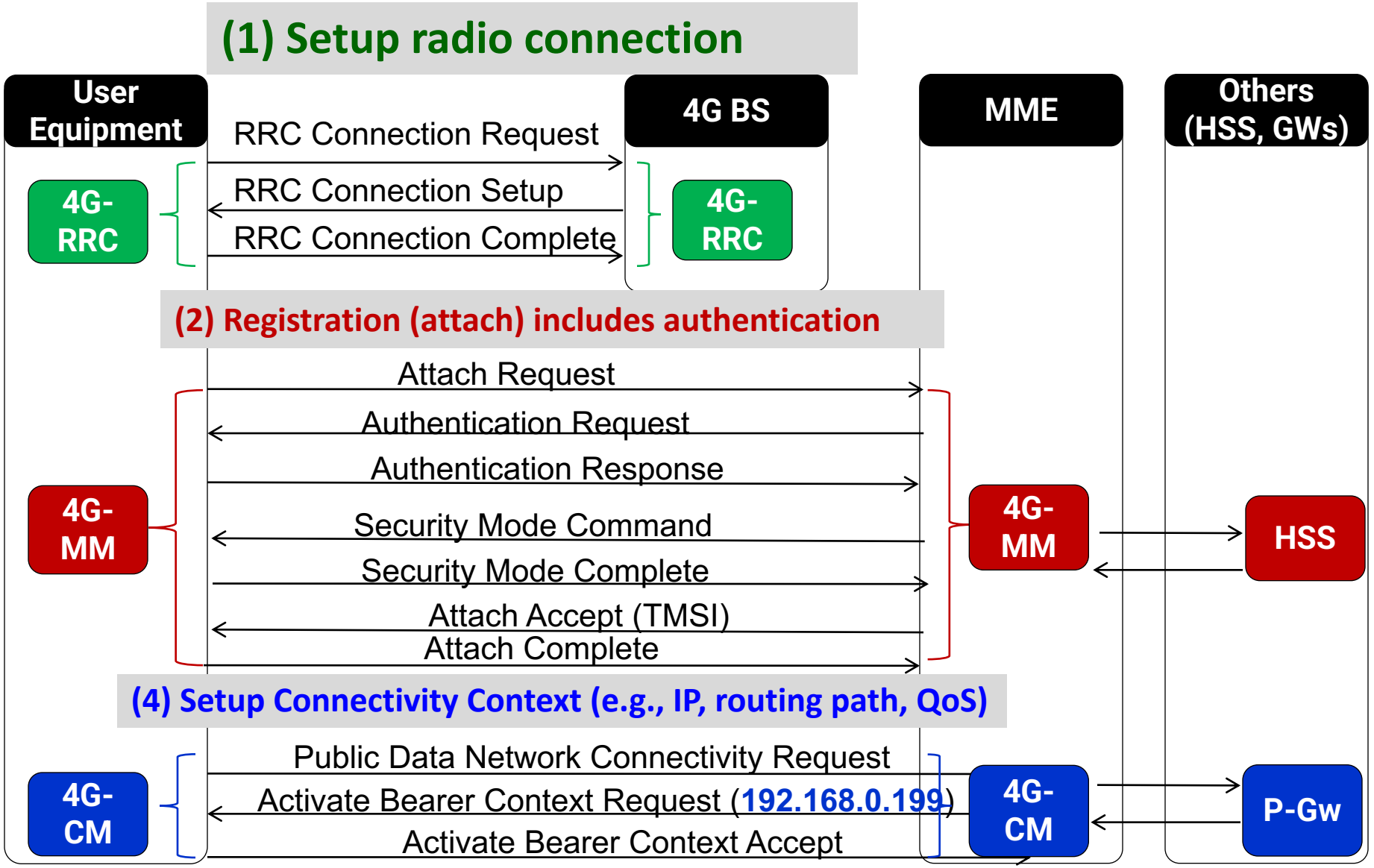
TMSI Exchange
IP assignment



Attach/Registration Procedure

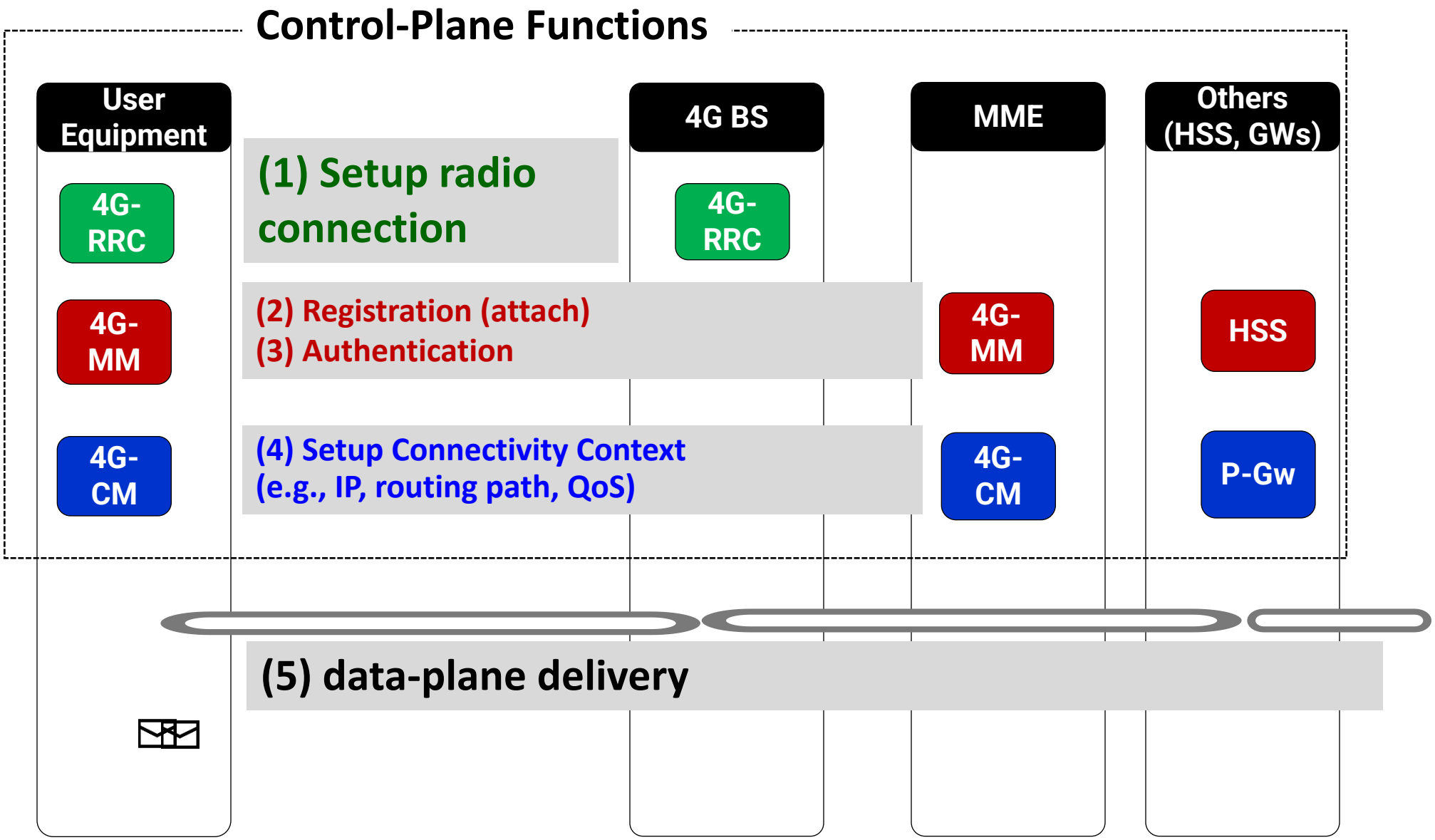


Setting Up Data Service in 4G

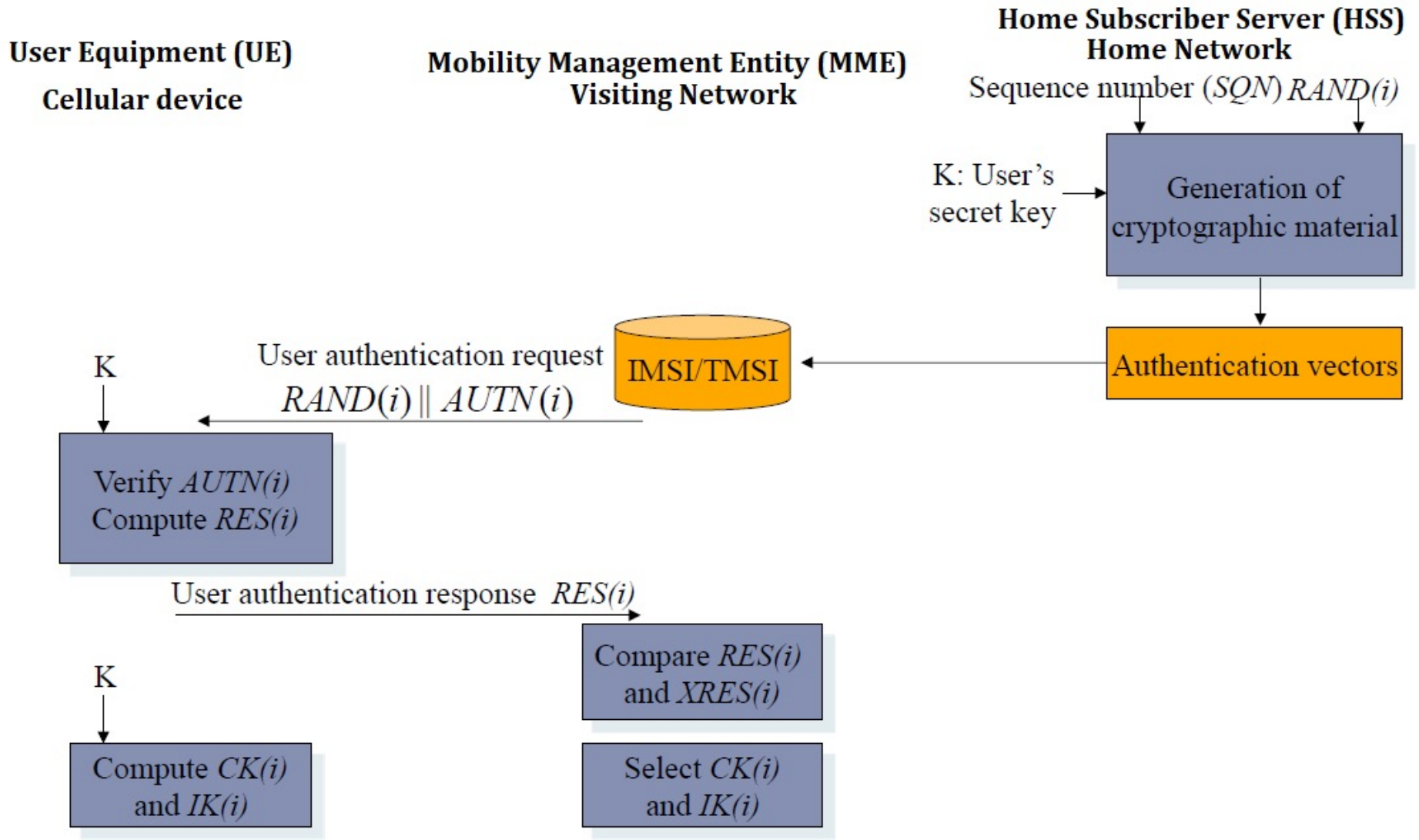


PDN: Public Data Network EPS: Evolved Packet System

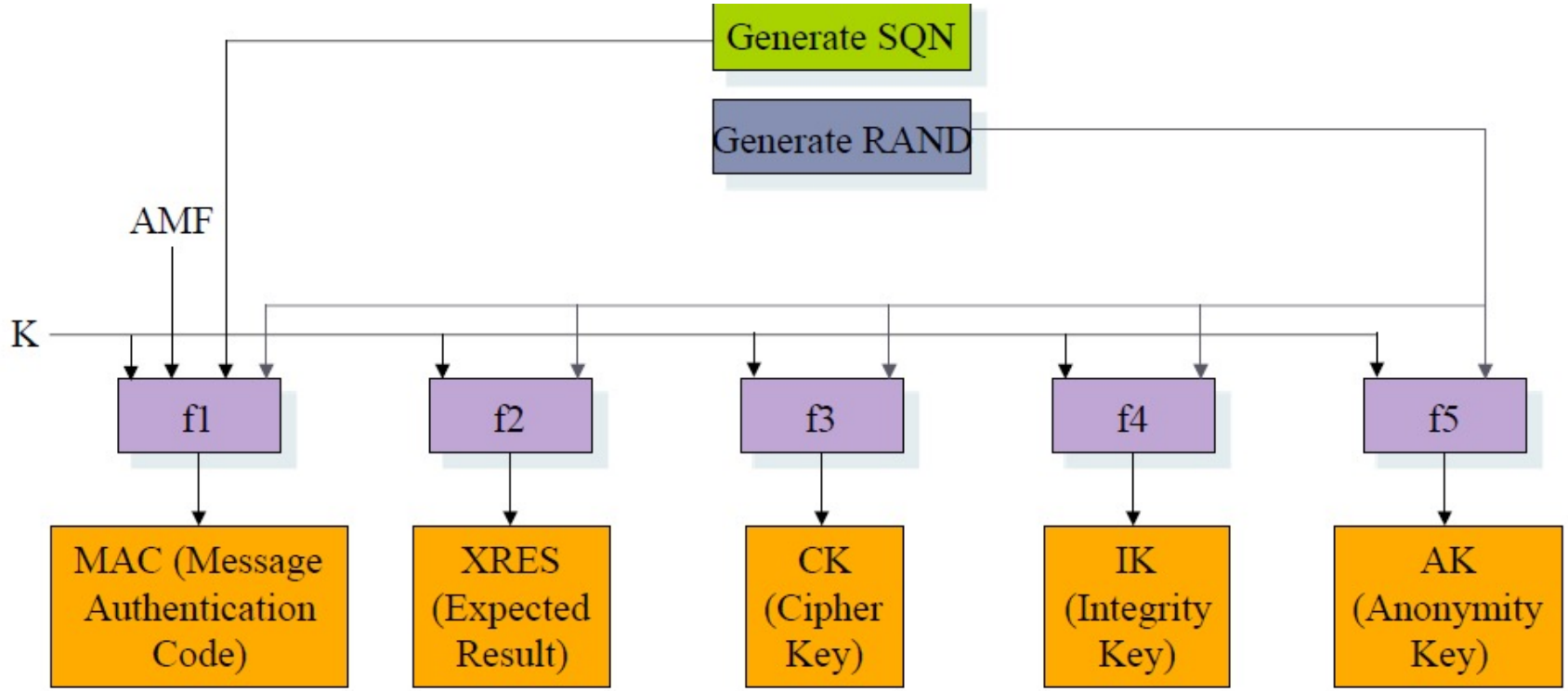
Setting Up Data Service in 4G



4G Authentication



Generation of Authentication Vector or Challenge

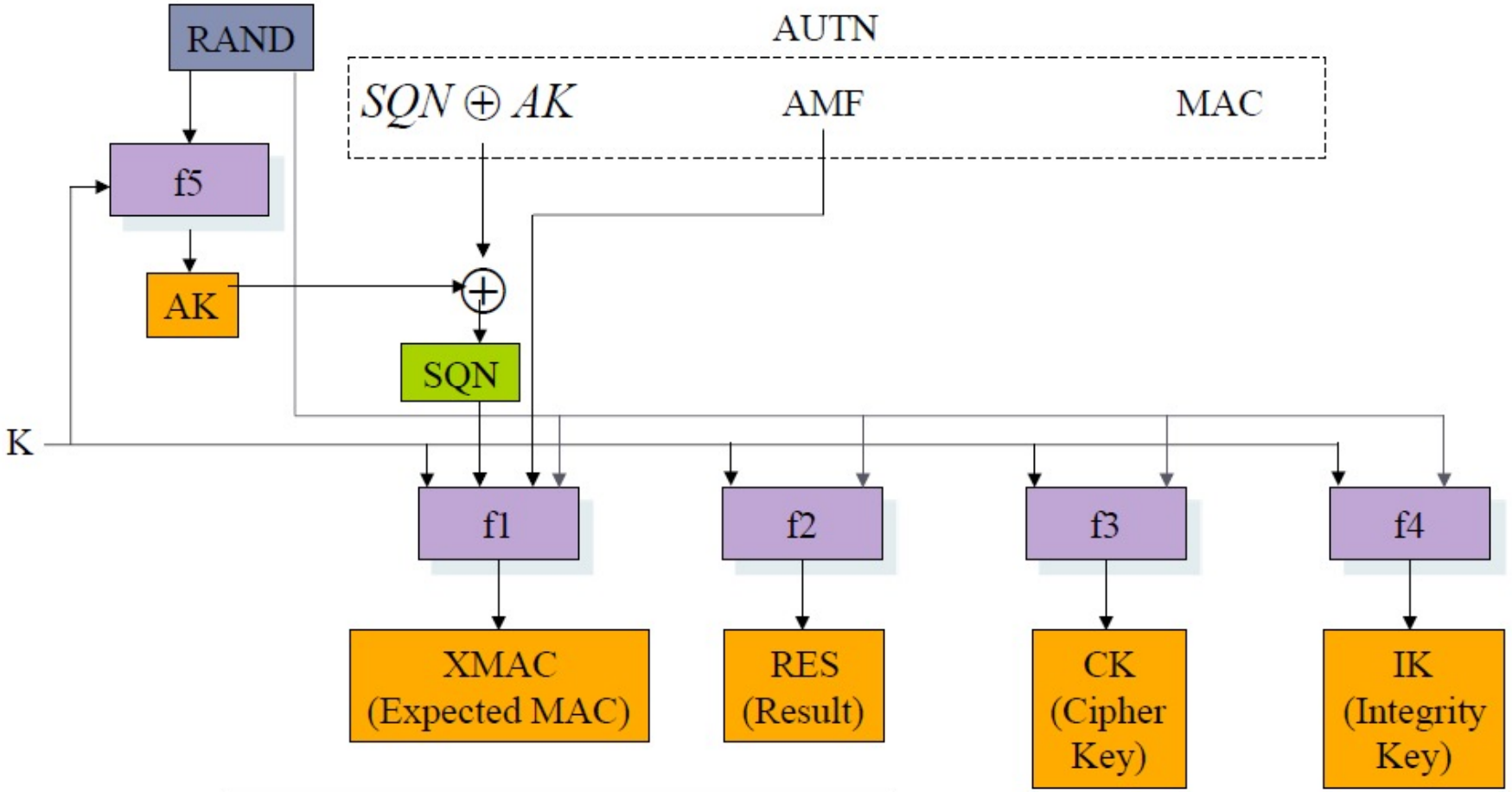


$AUTN := (SQN \oplus ACK) \| AMF \| MAC$

$AV := RAND \| XRES \| CK \| IK \| AUTN$

AMF: Authentication and Key Management Field
AUTN: Authentication Token
AV: Authentication Vector

User Authentication Function in USIM



- Verify MAC = XMAC
- Verify that SQN is in the correct range

USIM: User Services Identity Module

Authentication in 4G

User Equipment (UE)

$IMSI, K, SQN$

MME

Home Subscriber Server

$AMF, S = \{s|\forall i \in I\}$ where $s = \langle i, K, SQN \rangle$

Attach Request ($IMSI/TMSI$, ue_capabilities)

$IMSI$

$K, SQN \leftarrow s \in S$ $where i = IMSI$
$RAND \leftarrow \{0,1\}^{128}$
$MAC \leftarrow f_1(K, SQN, AMF, RAND)$
$XRES \leftarrow f_2(K, RAND)$,
$CK \leftarrow f_3(K, RAND)$, $IK \leftarrow f_4(K, RAND)$, $AK \leftarrow f_5(K, RAND)$
$AUTN \leftarrow (SQN \oplus AK, AMF, MAC)$
$s_{SQN} \leftarrow SQN + 1$

Authentication Request $(RAND, AUTH)$

$RAND, AUTN, XRES, CK, IK$

$AK \leftarrow f5(K, RAND)$
$XSQN \leftarrow AK \oplus AUTN_{SQN \oplus AK}$
$XMAC \leftarrow f_1(K, XSQN, AUTN_{AMF}, RAND)$
Verify: $XMAC = AUTN_{MAC}$
Verify: $SQN \leq XSQN \leq (SQN + range)$
$SQN \leftarrow XSQN + 1$
$SRES \leftarrow f_2(K, RAND)$
$CK \leftarrow f_3(K, RAND)$, $IK \leftarrow f_4(K, RAND)$

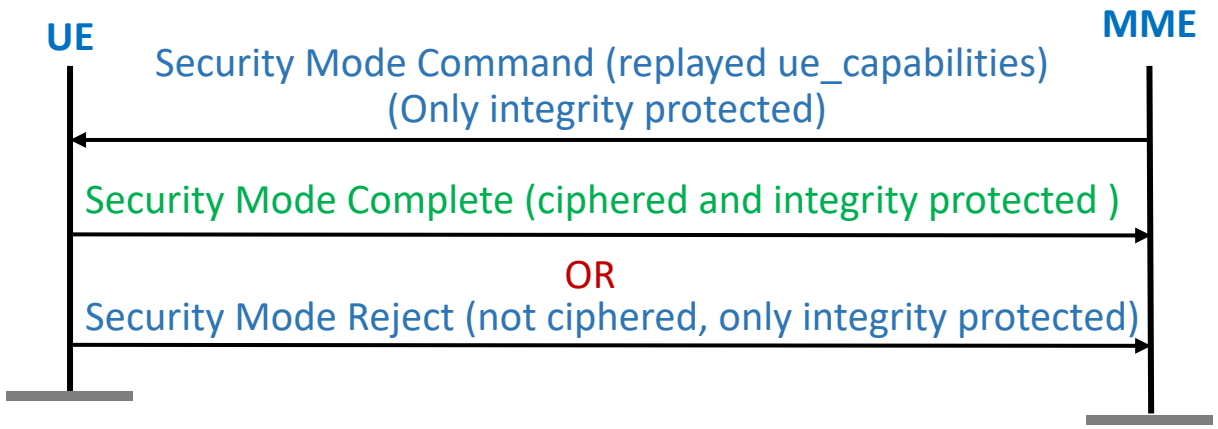
Authentication Response $(SRES)$

Verify: $SRES = XRES$

Encrypted with CK

Authenticity Protected with IK

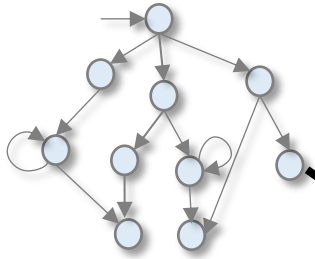
Security Mode Command Procedure



Authentication and Key Generation (AKA)

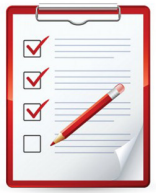
- In addition to f1, f2, f3, f4 and f5, two more functions are defined: f1* and f5*, used in case the authentication procedure gets desynchronized (detected by the range of SQN).
- f1, f1*, f2, f3, f4, f5 and f5* are operator-specific
- However, 3GPP provides a detailed example of algorithm set, called MILENAGE
- MILENAGE is based on the Rijndael block cipher. In MILENAGE, the generation of all seven functions f1…f5* is based on the Rijndael algorithm

Model Checking

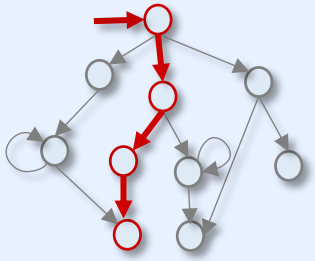


Model, ***M***:

Abstract normal behavior of the system



Property, ***φ***



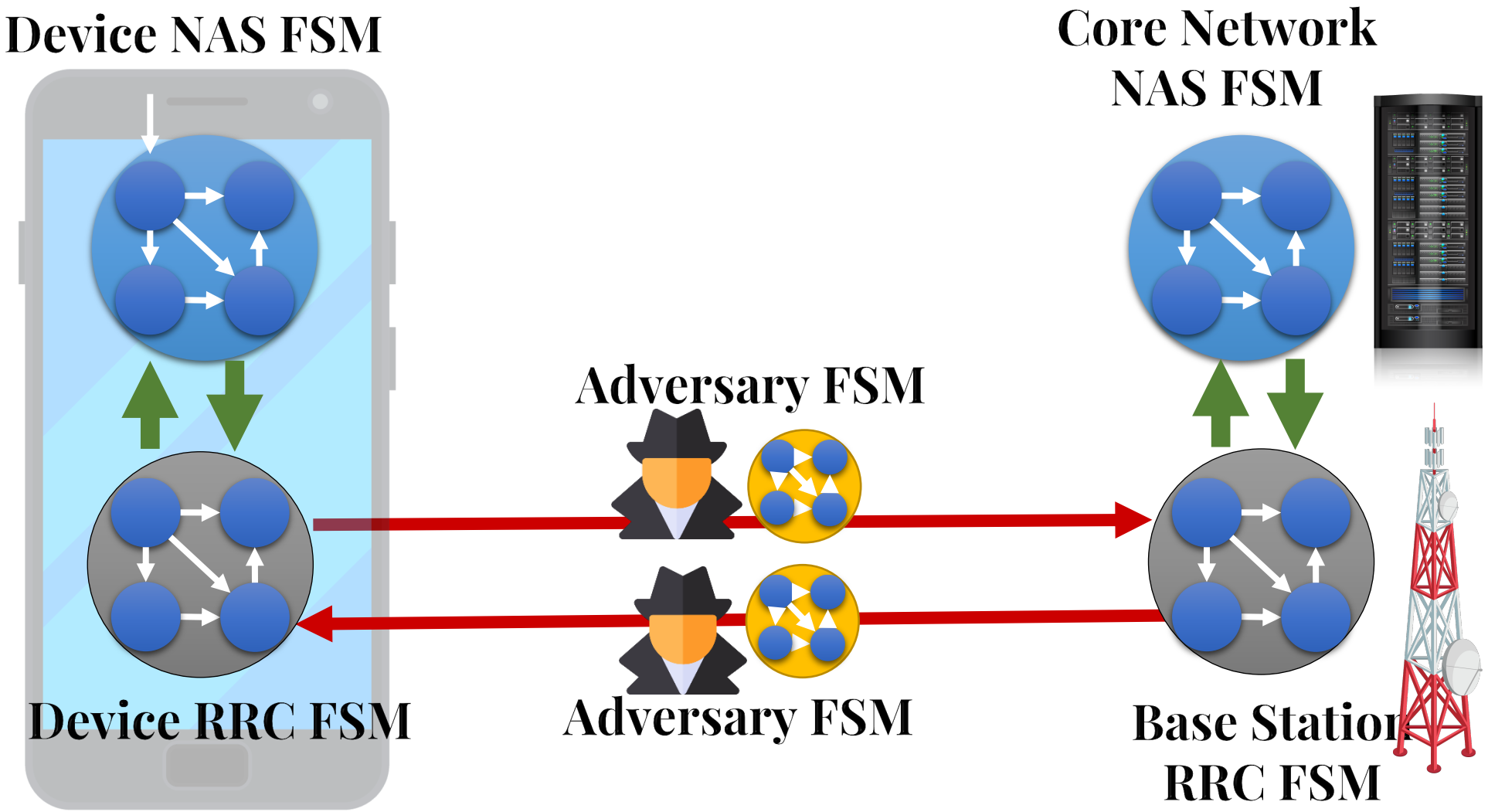
Model Checker

$M \models \varphi$

Verified

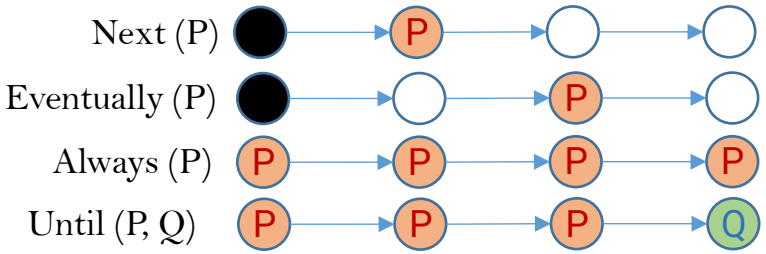
Violated, Not verified

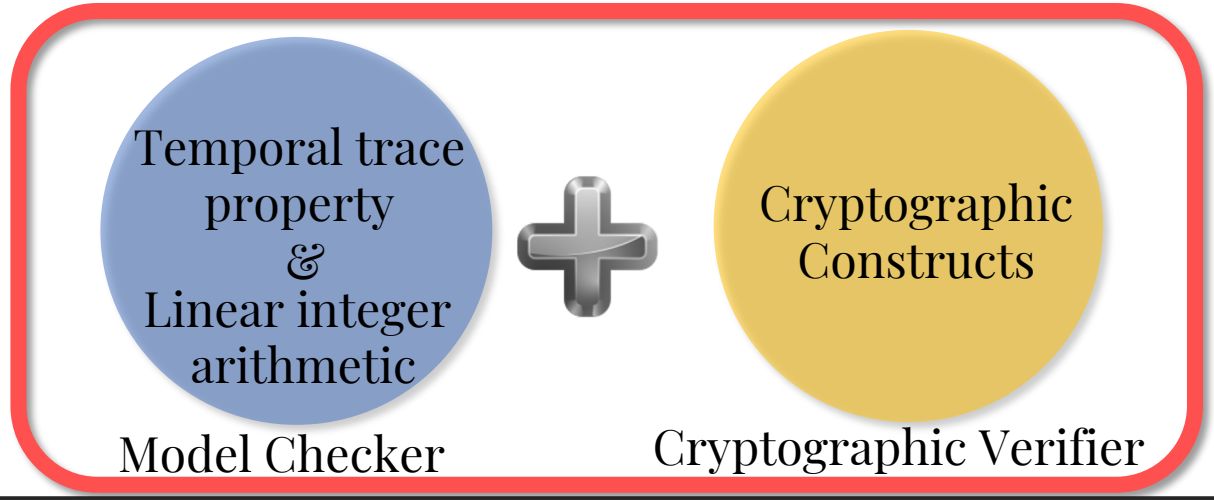
Dolev-Yao Adversary Model



Key Insight of Our Adversarial Testing Framework

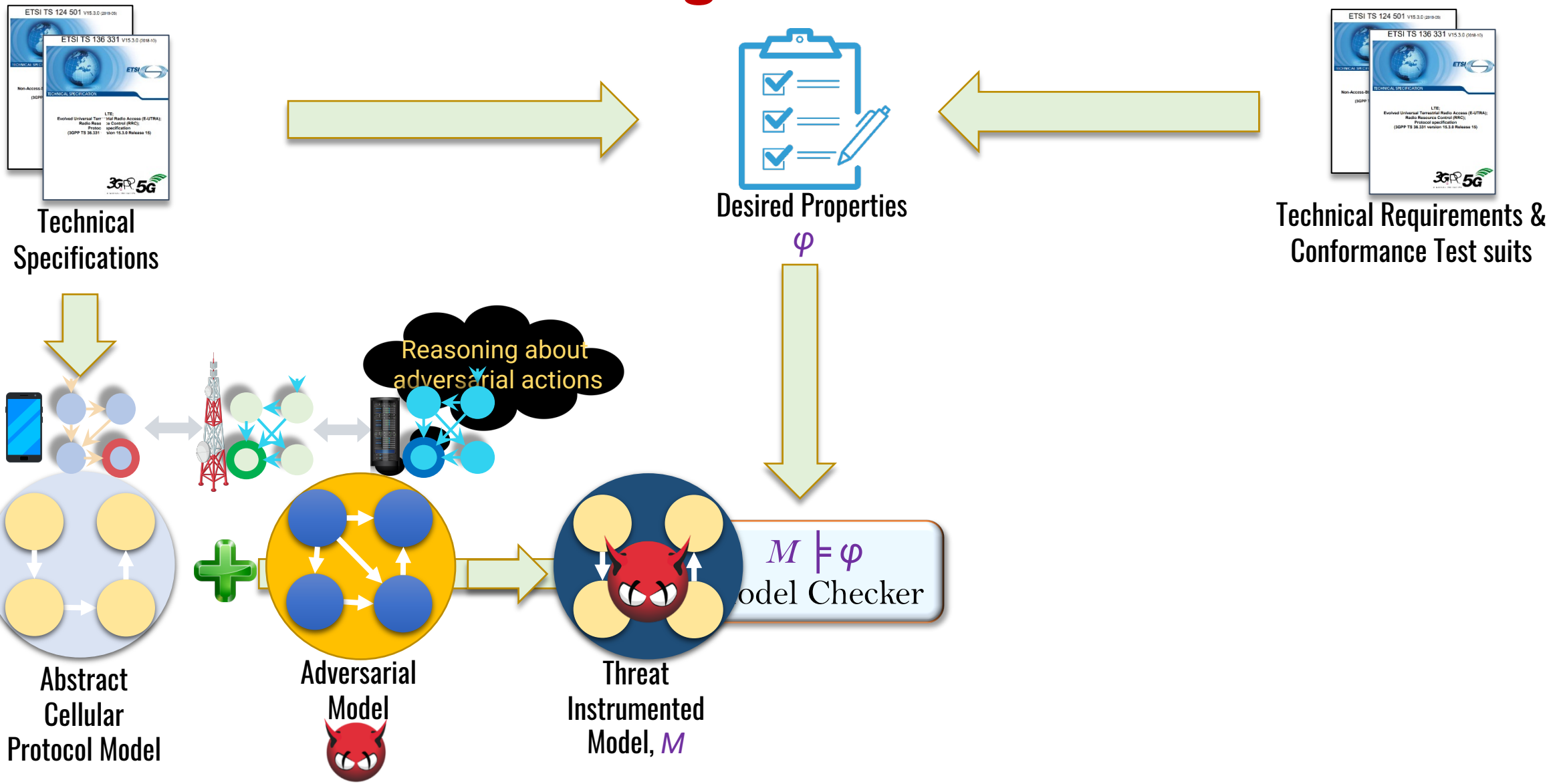
- Property characteristics
  - ✓Temporal ordering of events
  - ✓ Cryptographic constructs
  - ✓ Linear integer arithmetic and other predicates
    - SQN++ and verify SQN ≤ XSQN ≤ (SQN + range)



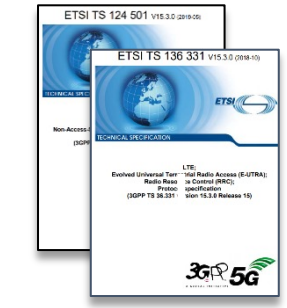


How can we leverage reasoning power of these two?

Adversarial Testing Framework: 5GReasoner



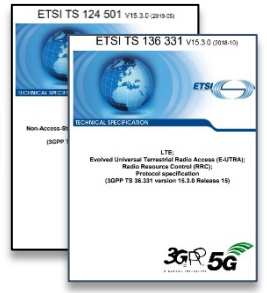
Adversarial Testing Framework: 5GReasoner



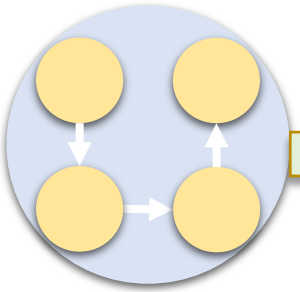
Technical Specifications

Desired Properties

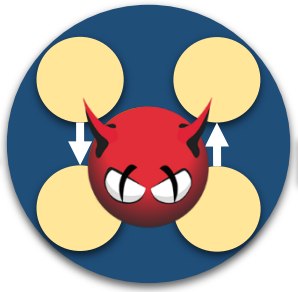
φ



Technical Requirements & Conformance Test suits



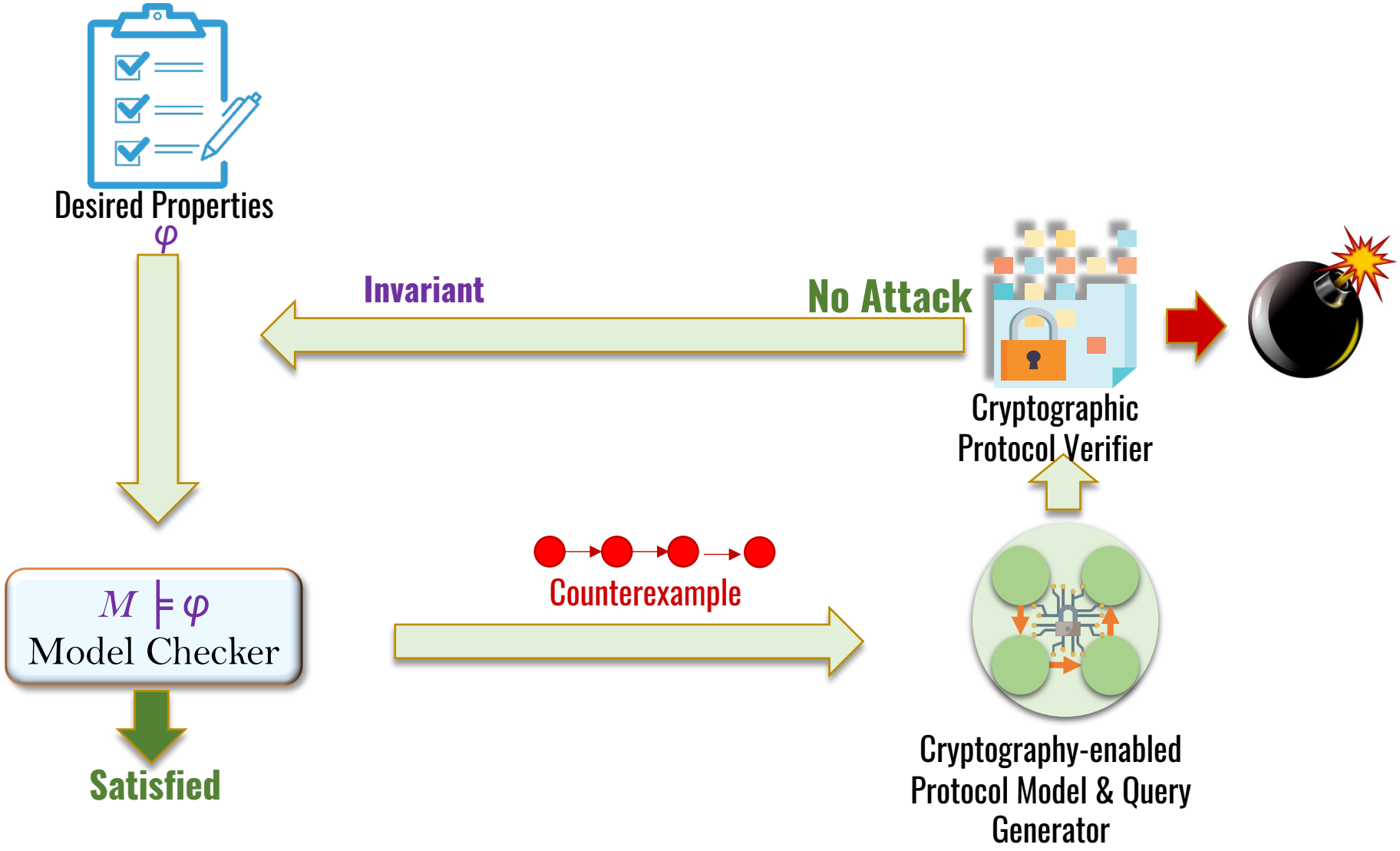
Abstract Cellular Protocol Model



Threat Instrumented Model, M

$M \models \varphi$
Model Checker

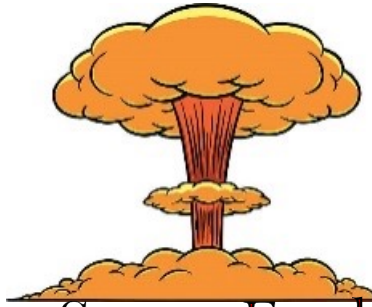
Adversarial Testing Framework: 5GReasoner



Addressing State Space Explosion

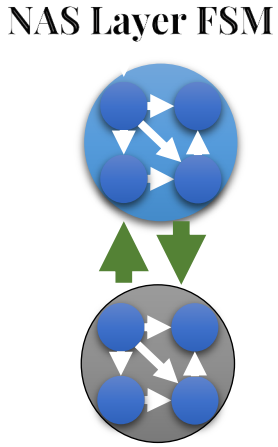
Multiple Protocol Layers

System Data and Packet Payload
E.g., Timer and Message Authentication Code



State Space Explosion

Behavior-Aware Predicate Abstraction
E.g., Validity, Presence, Grouping Predicates, etc.



Validity of MAC
(isValid_MAC)

Validity Predicate

Findings

5G 11 new attacks

Authentication Bypass

Location tracking

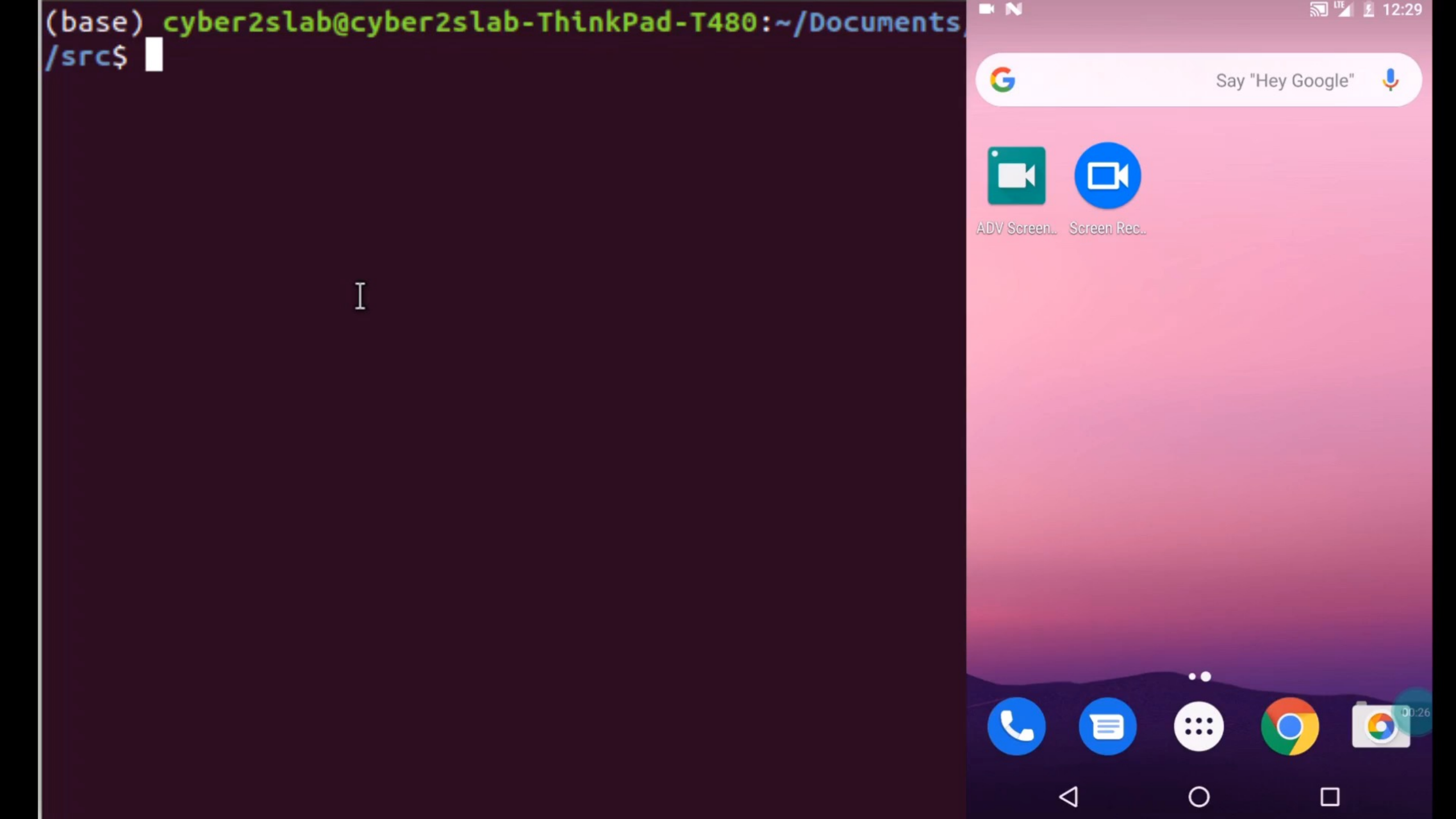
Service Profiling

4G LTE 10 new attacks

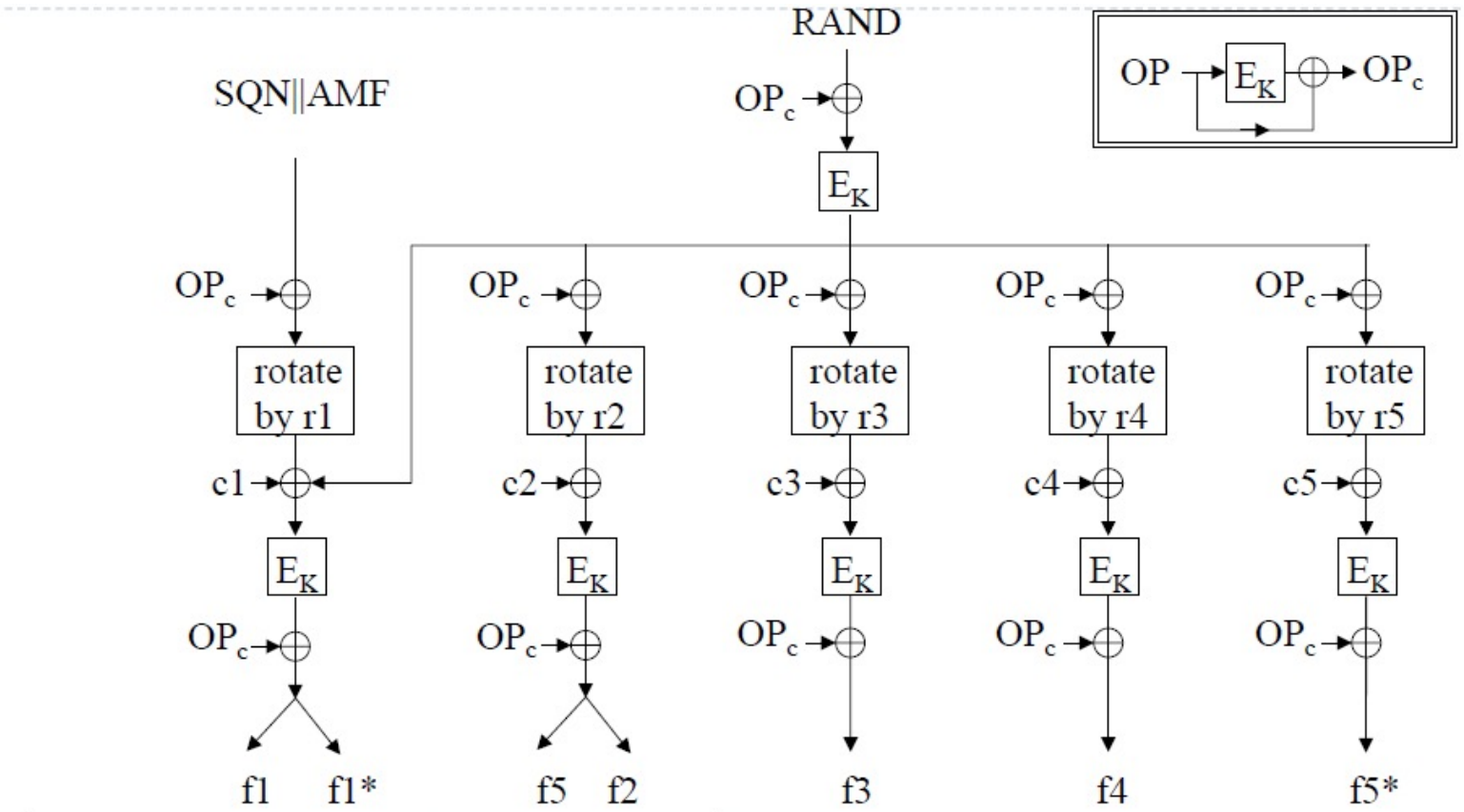
TMSI exposure

Overbilling

Artificial Chaos


(base) cyber2slab@cyber2slab-ThinkPad-T480:~/Documents
/src$
12:29
Say "Hey Google"
ADV Screen..
Screen Rec..

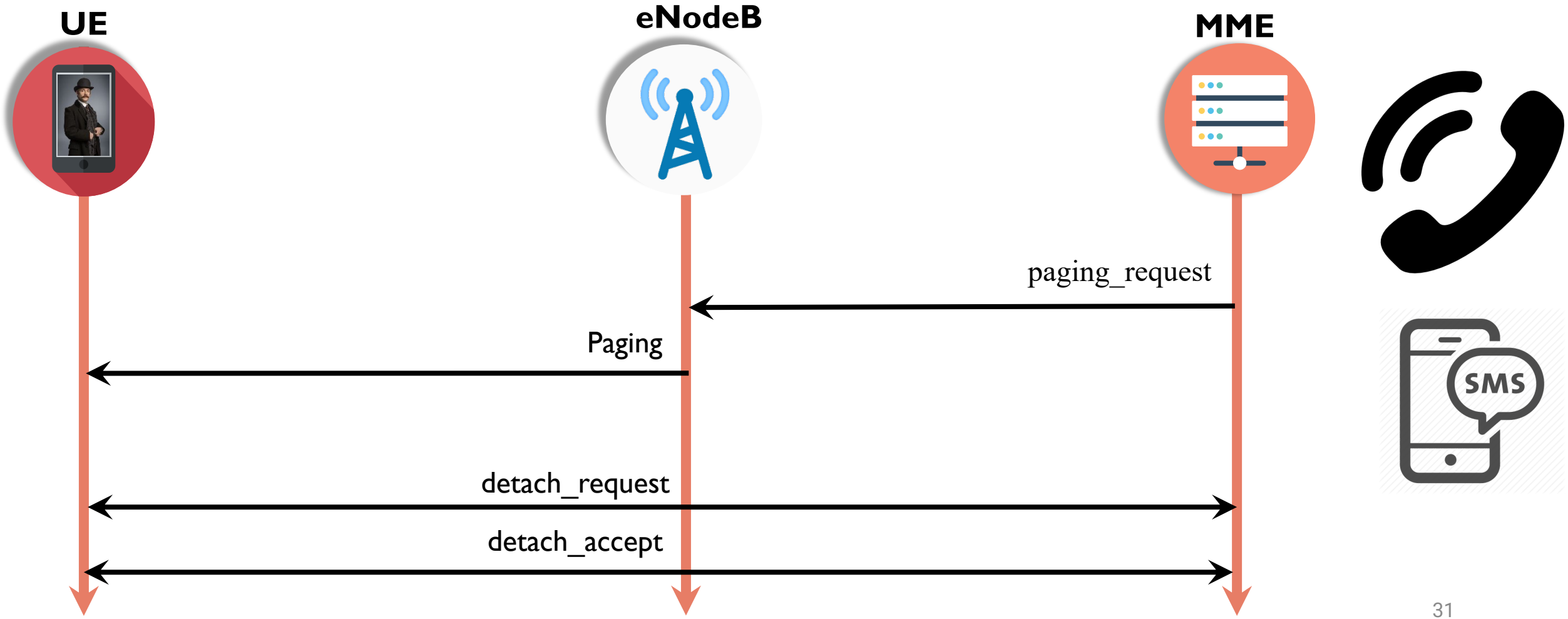
Generation of f1-f5, f1*, and f5* using Kernel Function E_K



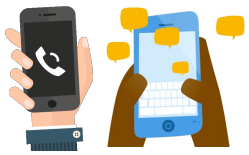
OP: operator-specific parameter
r1,…, r5: fixed rotation constants
c1,…, c5: fixed addition constants

E_K : Rijndael block cipher with 128 bits text input and 128 bits key

Background (Paging & Detach)



Paging Procedure



CONNECTED

Base Station

Core Network

MUTUAL AUTHENTICATION

Paging Procedure

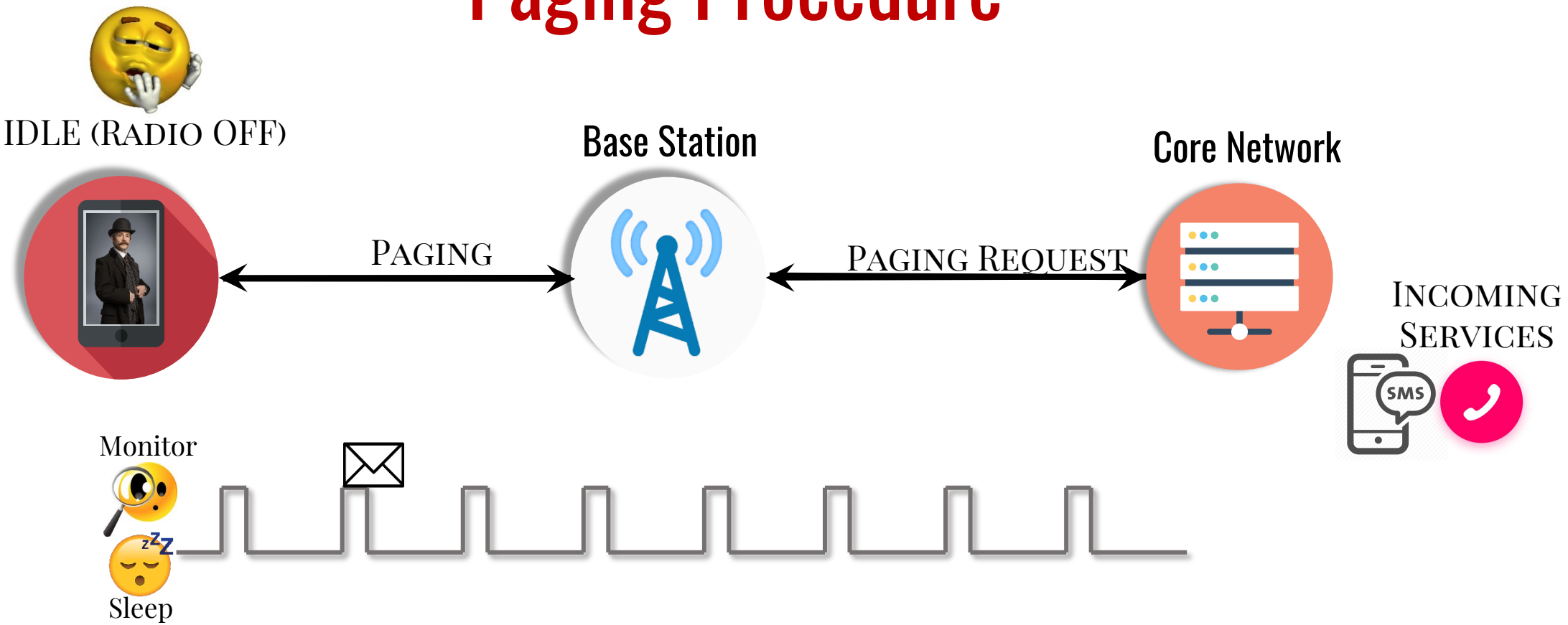
IDLE (RADIO OFF)

Base Station

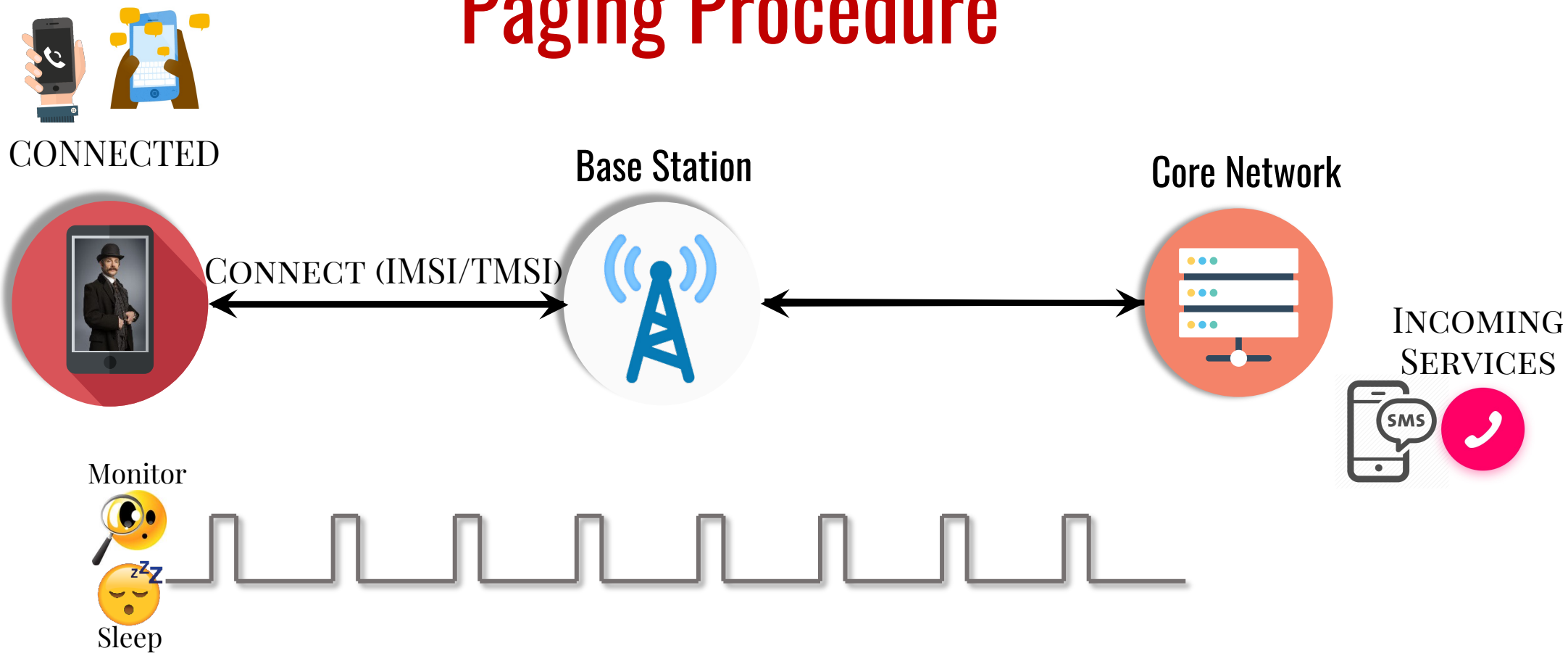
Core Network

INCOMING SERVICES

Paging Procedure

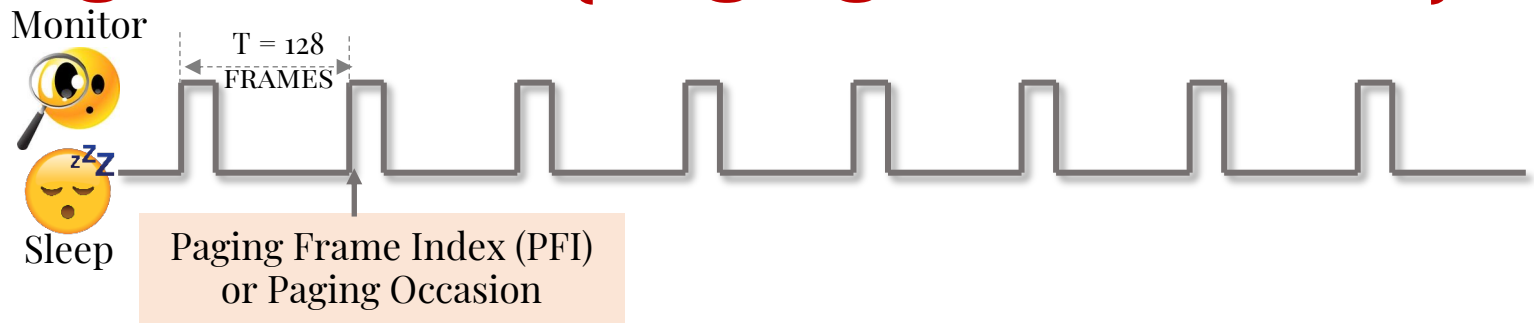


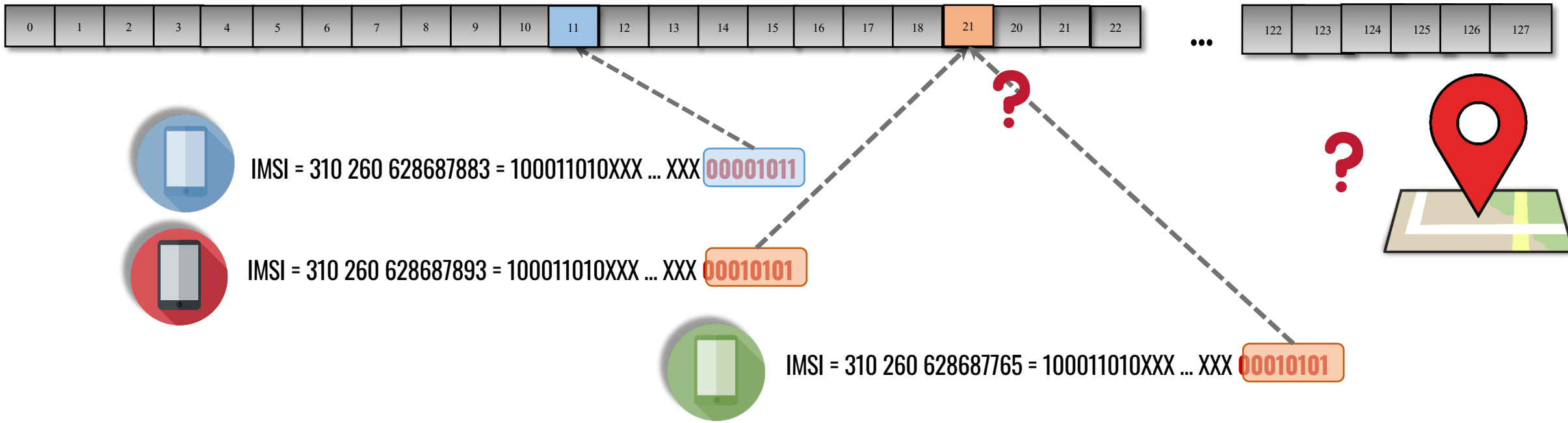
Paging Procedure



If I make a phone call to your number, your device will receive a paging message from the base station your device is connected.

Paging Occasion (Paging Frame Index)





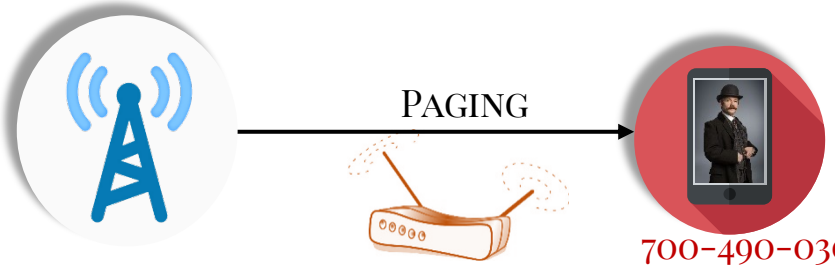
Paging Occasion (Paging Frame Index)

Can a passive adversary knowing victim's phone number/Twitter handle
(1) Identify victim's PFI?
(2) Identify/track the victim's presence in a target area?

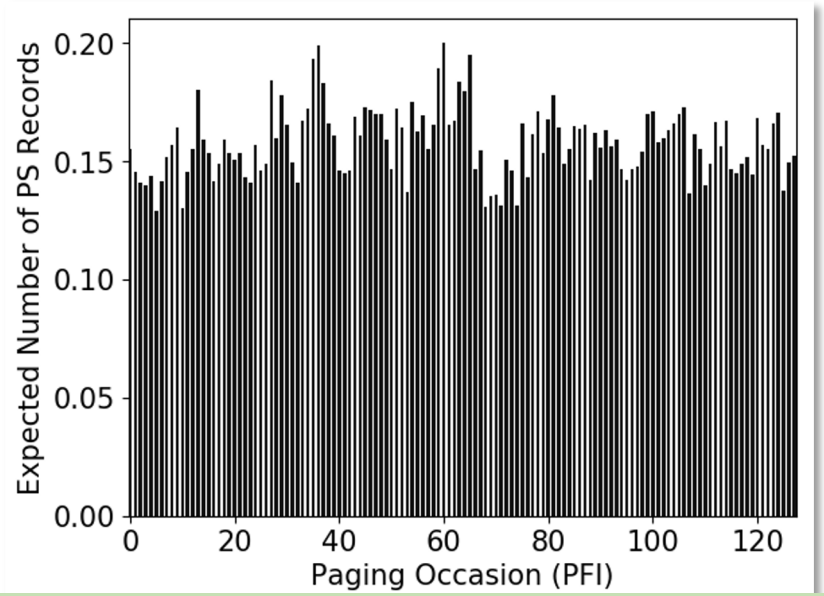
IMSI = 310 260 628687893 = 100011010XXX ... XXX 00010101

IMSI = 310 260 628687765 = 100011010XXX ... XXX 00010101

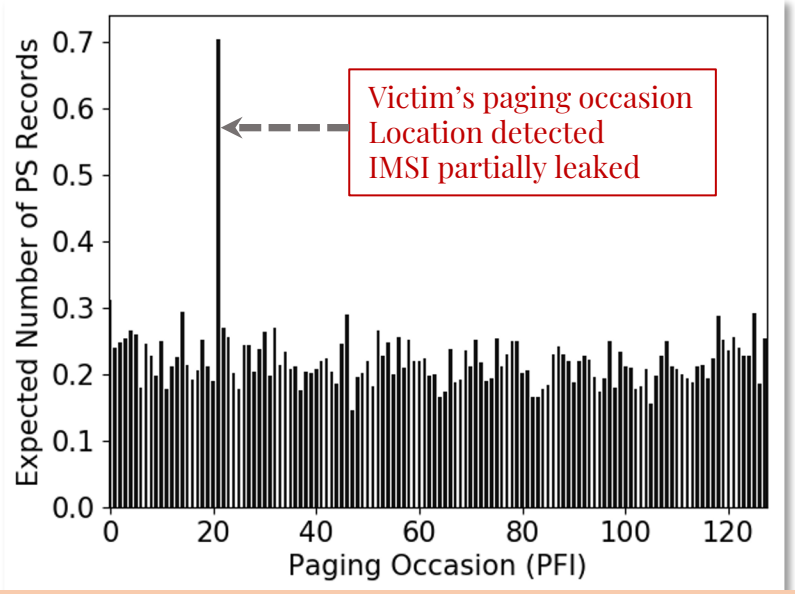
ToRPEDO
TRacking via Paging mEssage DistributiOn



700-490-0301
https://twitter.com/victim



Distribution of paging messages (PS records) when attacker makes no phone call



Distribution of paging messages (PS records) when attacker makes silent phone calls

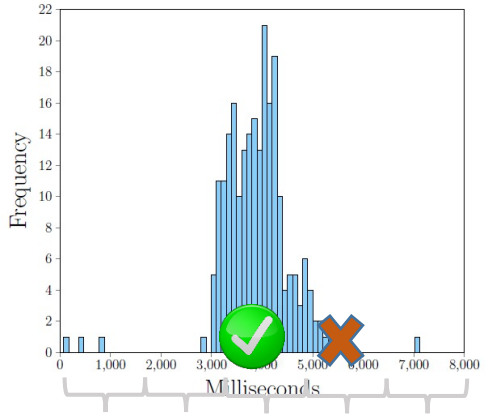
Privacy Attacks to the 4G and 5G Cellular Paging Protocols Using Side Channel Information

Syed Rafiul Hussain, Mitziu Echeverria[†], Omar Chowdhury[†], Ninghui Li[*], Elisa Bertino[*]

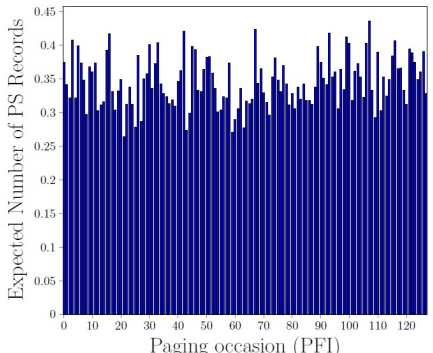
PURDUE UNIVERSITY, UNIVERSITY OF IOWA

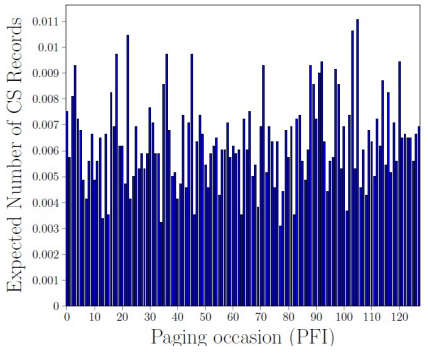
Likelihood Analysis – ToRPEDO Attack

- 16 paging records with PS and CS indication
- Timing information



- Base rate of PS, and CS records





Likelihood Analysis – ToRPEDO Attack

Compute the likelihood L_i of i to be the victim's PFI

$$L_i = \prod_{n\ trials} l_i \prod_{m=0, m\neq i}^{T-1} l'_m$$

$$l_i = (1-\varphi)\prod_{j=1}^{c} Pr\left[P(\lambda_b) = v_{i,j}\right] + \varphi \sum_{j=1}^{c} \Big(F\big(time(i,j)\big) - F\big(time(i,j-1)\big)\Big) * Pr[P(\lambda_b) = v_{i,j-1}] \prod_{k=1,k\neq j}^{c} Pr\left[P(\lambda_b) = v_{i,k}\right]$$

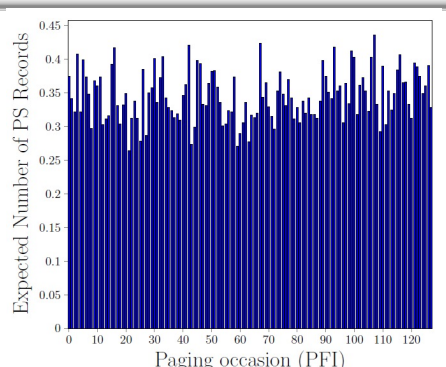
Compute the likelihood L_{-1}

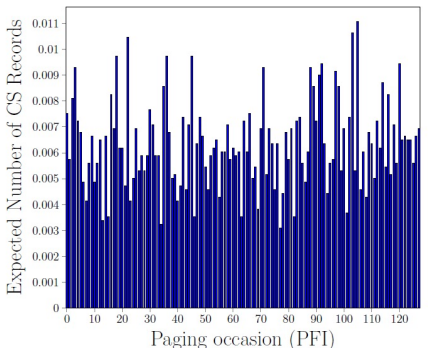
$$L_{-1} = \prod_{n\ trials} \prod_{m=0}^{T-1} l'_m$$

The adversary identifies i as the victim's PFI when

$$\frac{L_i}{L_j} > 10^{\mathcal{T}}$$

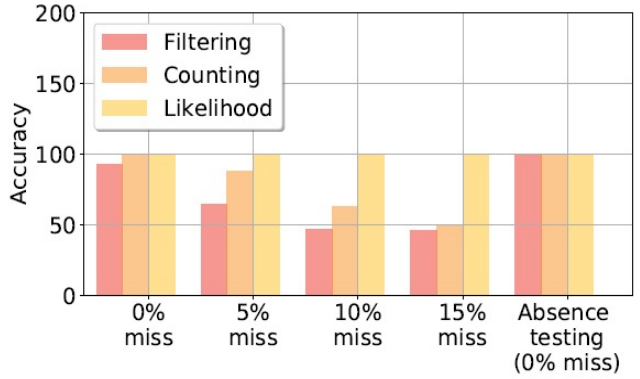
Base rate of PS, and CS records

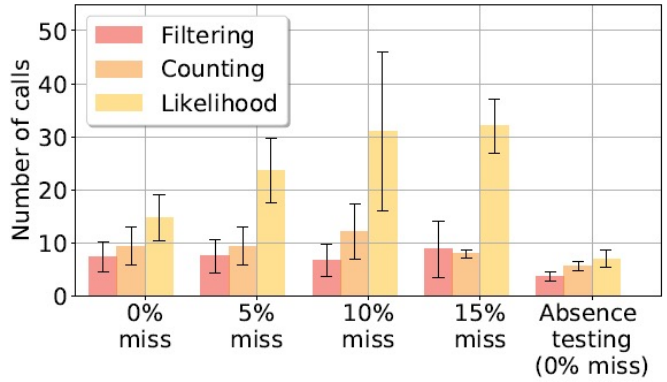




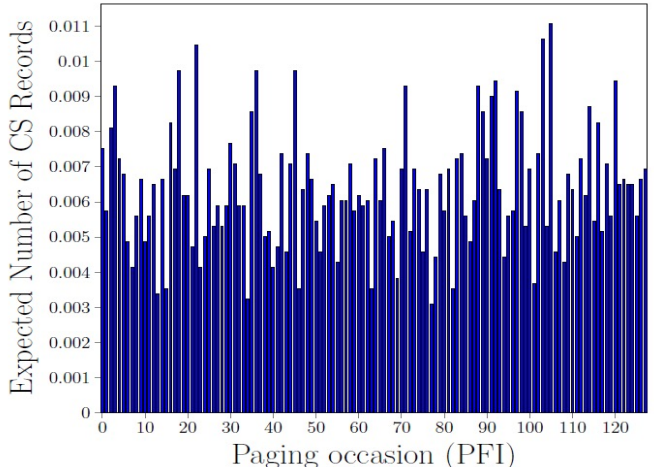
Evaluation and Mitigation

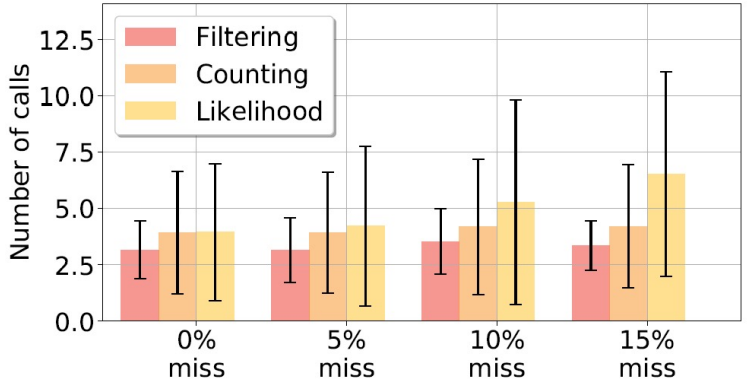
VoLTE calls (peak-time)





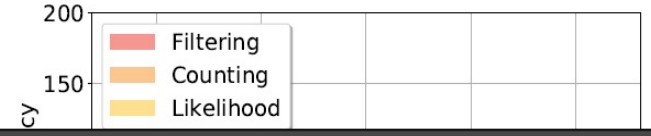
CSFB calls (peak-time)





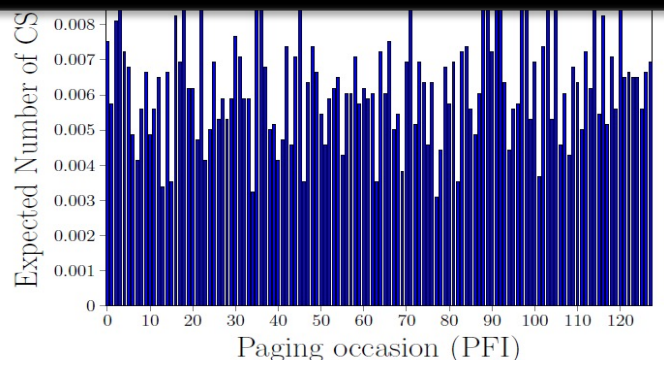
Evaluation and Mitigation

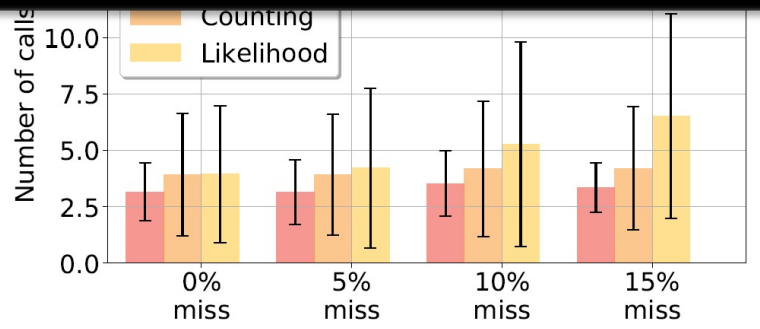
VoLTE calls (peak-time)



The adversary requires 4-10 phone calls/SMS/tweets/comments to identify PFI (last 7 bits of victim's IMSI)

Variable paging occasion based on TMSI instead of IMSI





IMSI-Cracking

IMSI is not exposed in plaintext in 5G

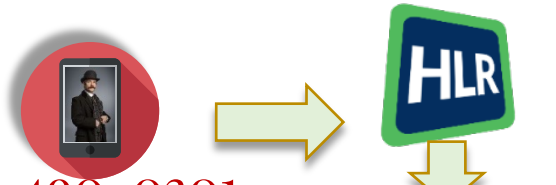
IMSI-Cracking

Exploit Registration Procedure

Legitimate Base Station + Core Network

IMSI	Key
IMSI_1	Key_1
IMSI_2	Key_2
IMSI_victim	Key_victim

IMSI-Cracking



IMSI = **310 260** 628687893 = **100011010XXX** … XXXXXXX**00010101**

MCC	MNC	MSIN	49 bits		
USA	T-Mobile		18 bits	24 bits unknown	7 bits

Exploit Registration Procedure

Victim

MitM Relay

Legitimate Base Station + Core Network

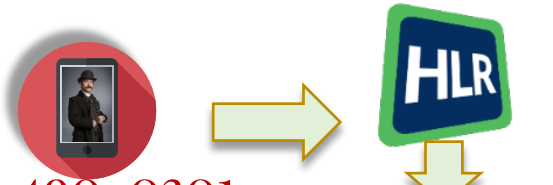
Registration Request
$E_{PK}(IMSI_{guess})$

Registration Reject

IMSI	Key
IMSI_1	Key_1
IMSI_2	Key_2
IMSI_victim	Key_victim

IMSI_guess

IMSI-Cracking

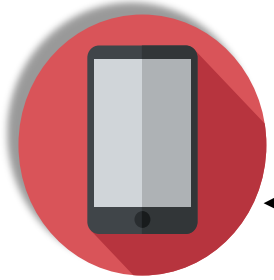


IMSI = **310 260** 628687893 = **100011010XXX** … XXXXXXX**00010101**

49 bits

MCC USA — MNC T-Mobile — MSIN — 18 bits — 24 bits unknown — 7 bits

Exploit Registration Procedure



Registration Request
$E_{PK}(IMSI_{guess})$

$C, MAC = f(MasterKey_{IMSI_{guess}})$

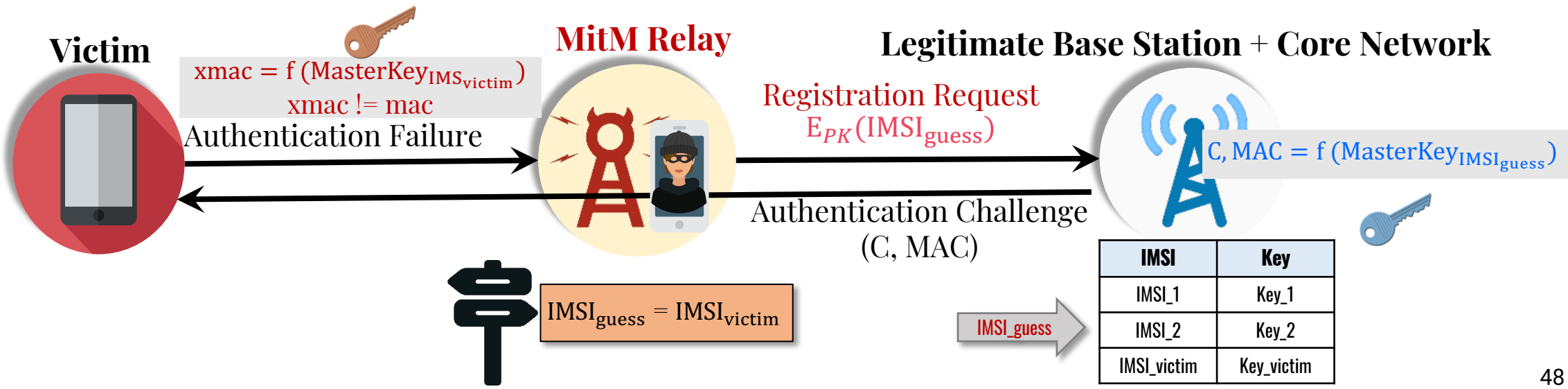
Authentication Challenge
(C, MAC)

IMSI_guess

IMSI	Key
IMSI_1	Key_1
IMSI_2	Key_2
IMSI_victim	Key_victim

IMSI-Cracking

Exploit Registration Procedure



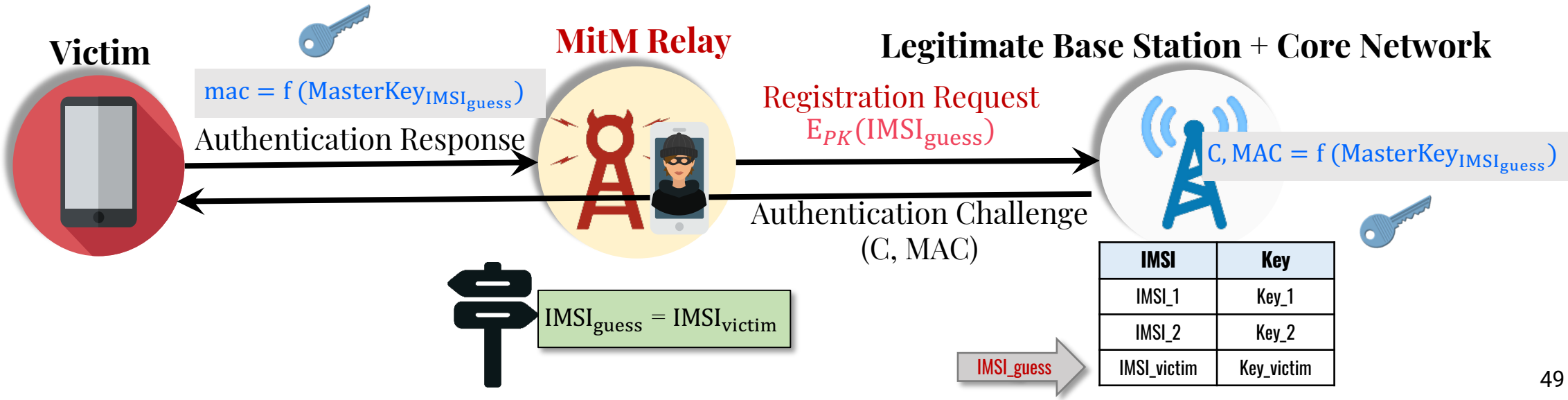
IMSI-Cracking

814-490-0301

IMSI = 310 260 628687893 = 100011010XXX ... XXXXXXX00010101

MCC (USA) MNC (T-Mobile) MSIN — 49 bits: 18 bits, 24 bits unknown, 7 bits

Exploit Registration Procedure



Summary and Discussion

- Primer on mobile network: architecture, protocols, operations
  - And its evolution
  - And its complexity

- ToRPEDO and IMSI-Cracking attack