



PennState

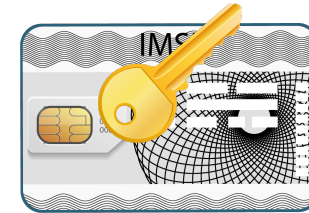
CMPSC 443: Introduction to Computer Security

Module: Cellular Network Security

Imtiaz Karim
Ph.D. Candidate
Department of Computer Science
Purdue University

Cellular Device or User Equipment

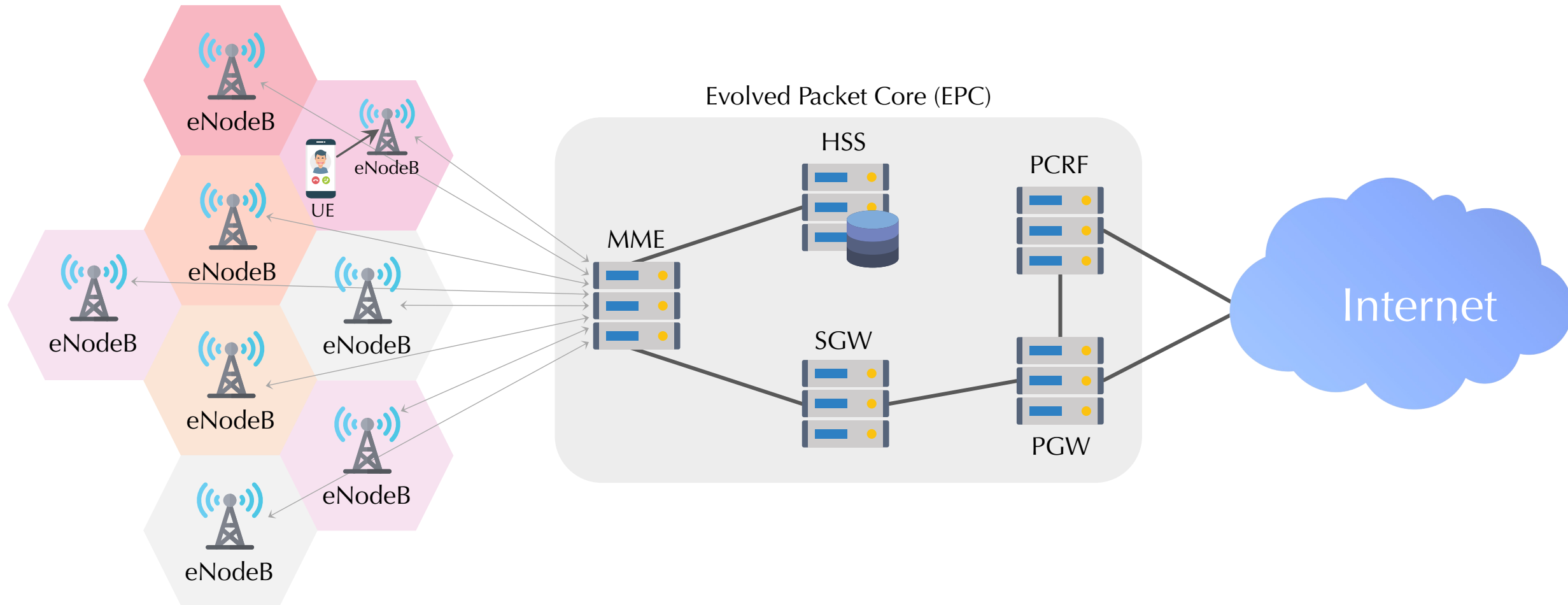
UE



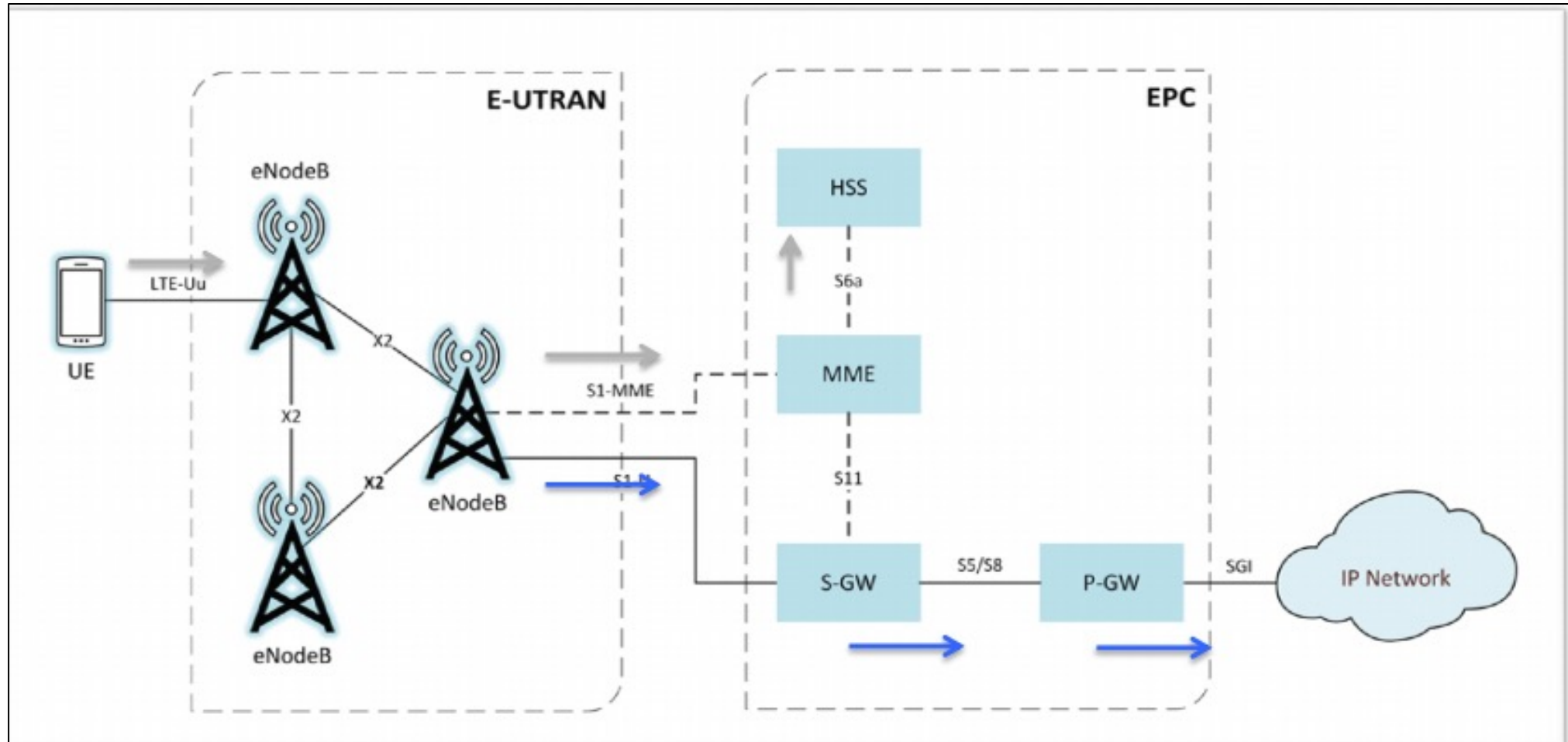
IMSI = International Mobile Subscriber Identity

IMEI = International Mobile Equipment Identity

Background: LTE Architecture

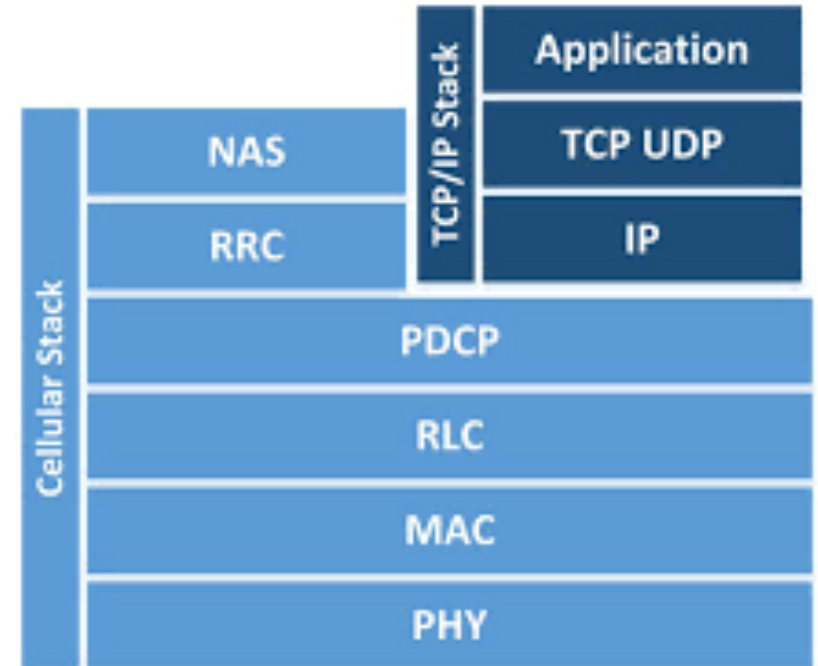


LTE Network

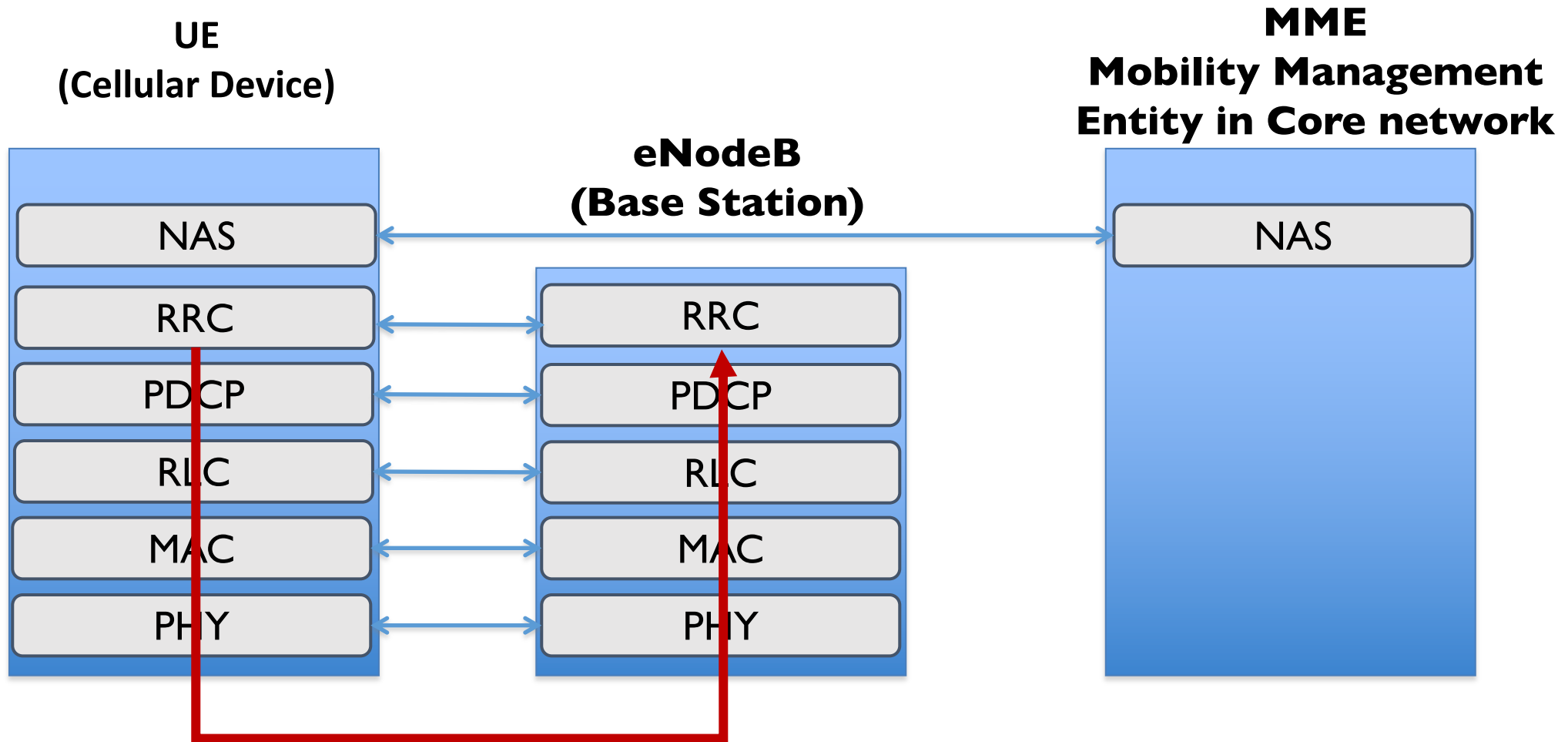


Protocol Stack

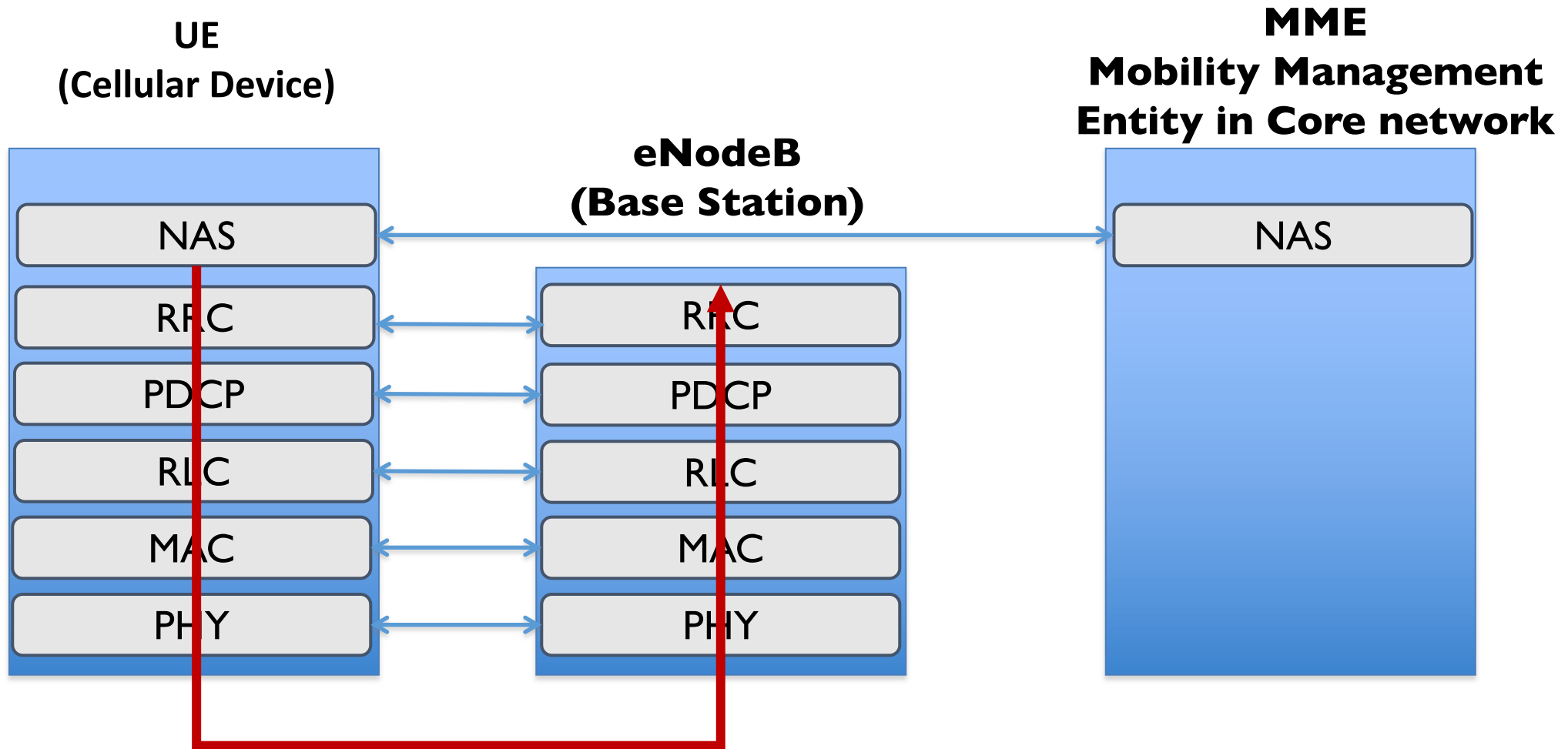
- TCP/IP sits on top of the cellular protocol stack:
- **Non-Access Stratum (NAS)**: Communicates between UE and core-network
- **Radio Resource Control (RRC)**: Transfers NAS messages, AS information may be included, signaling, and ECM
- **Packet Data Convergence Protocol (PDCP)**: header compression,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



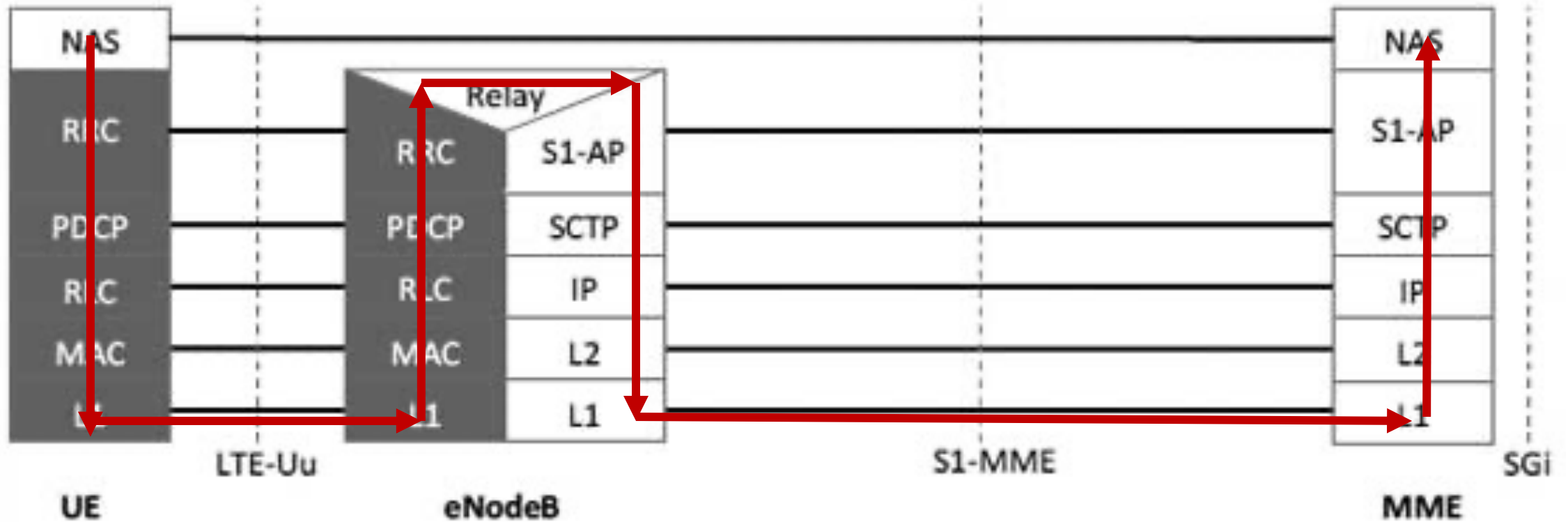
4G Control Plane Protocol Stack



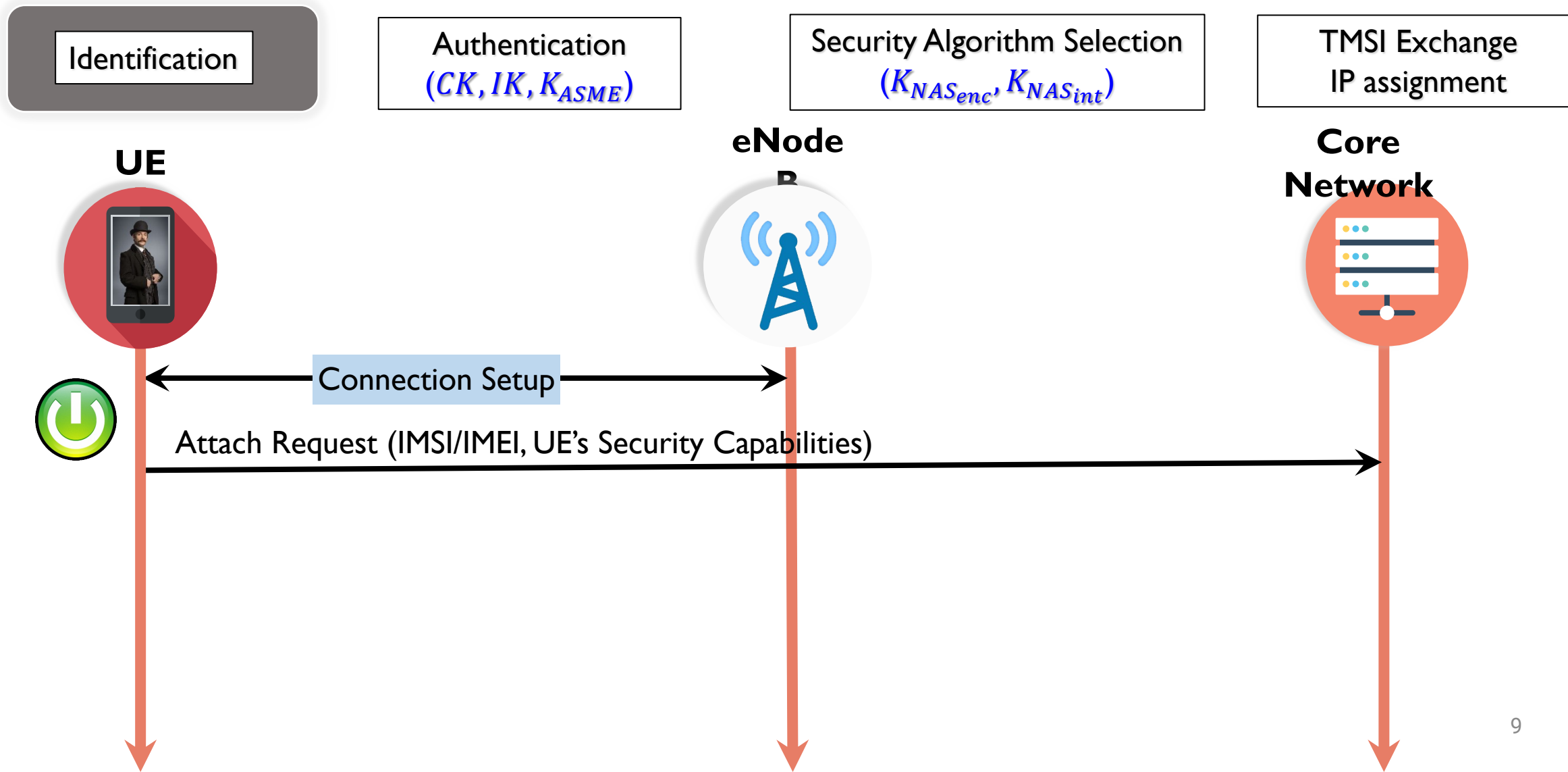
4G Control Plane Protocol Stack



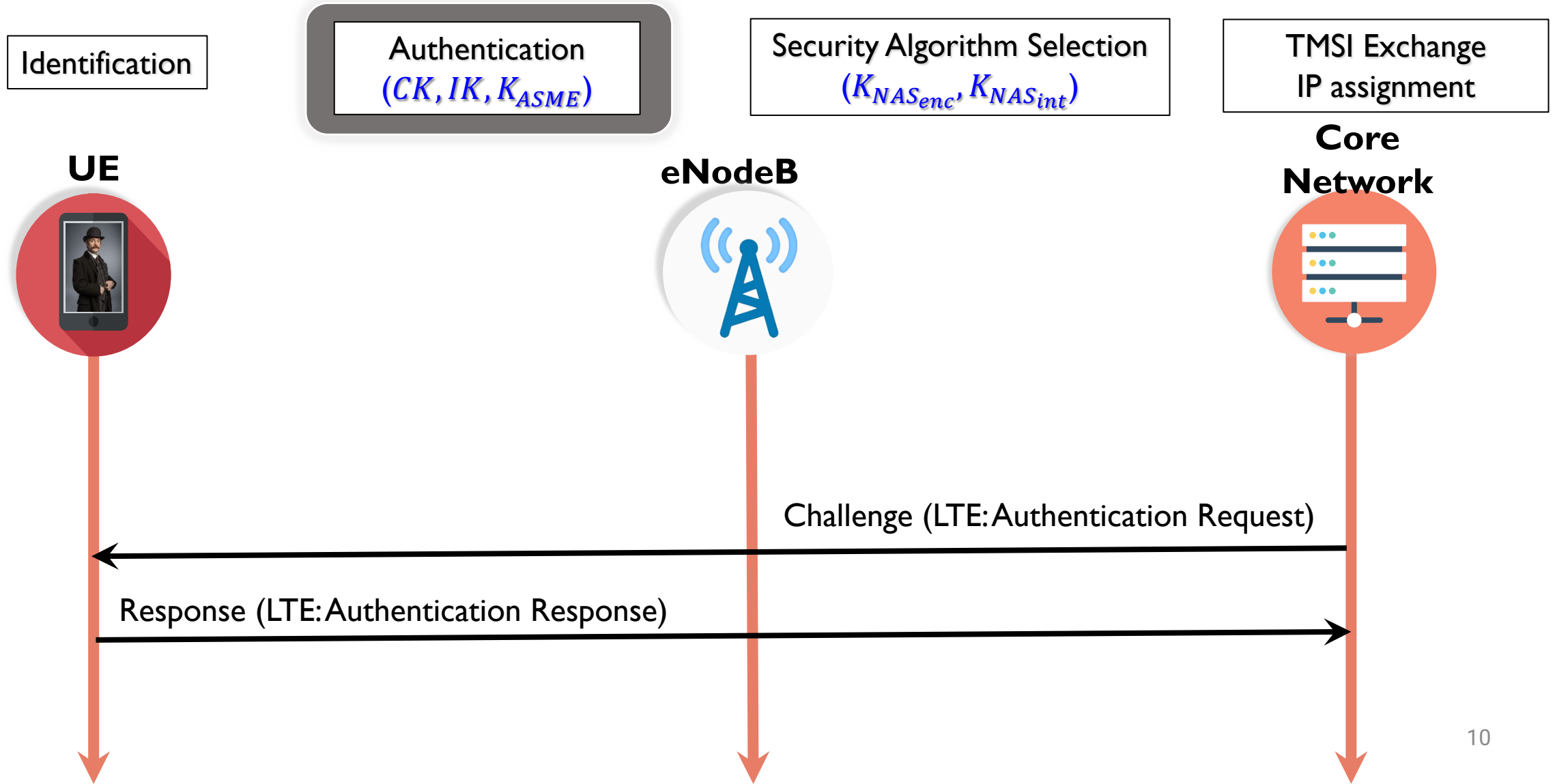
4G Control Plane Protocol Stack



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

UE



eNodeB



Core Network



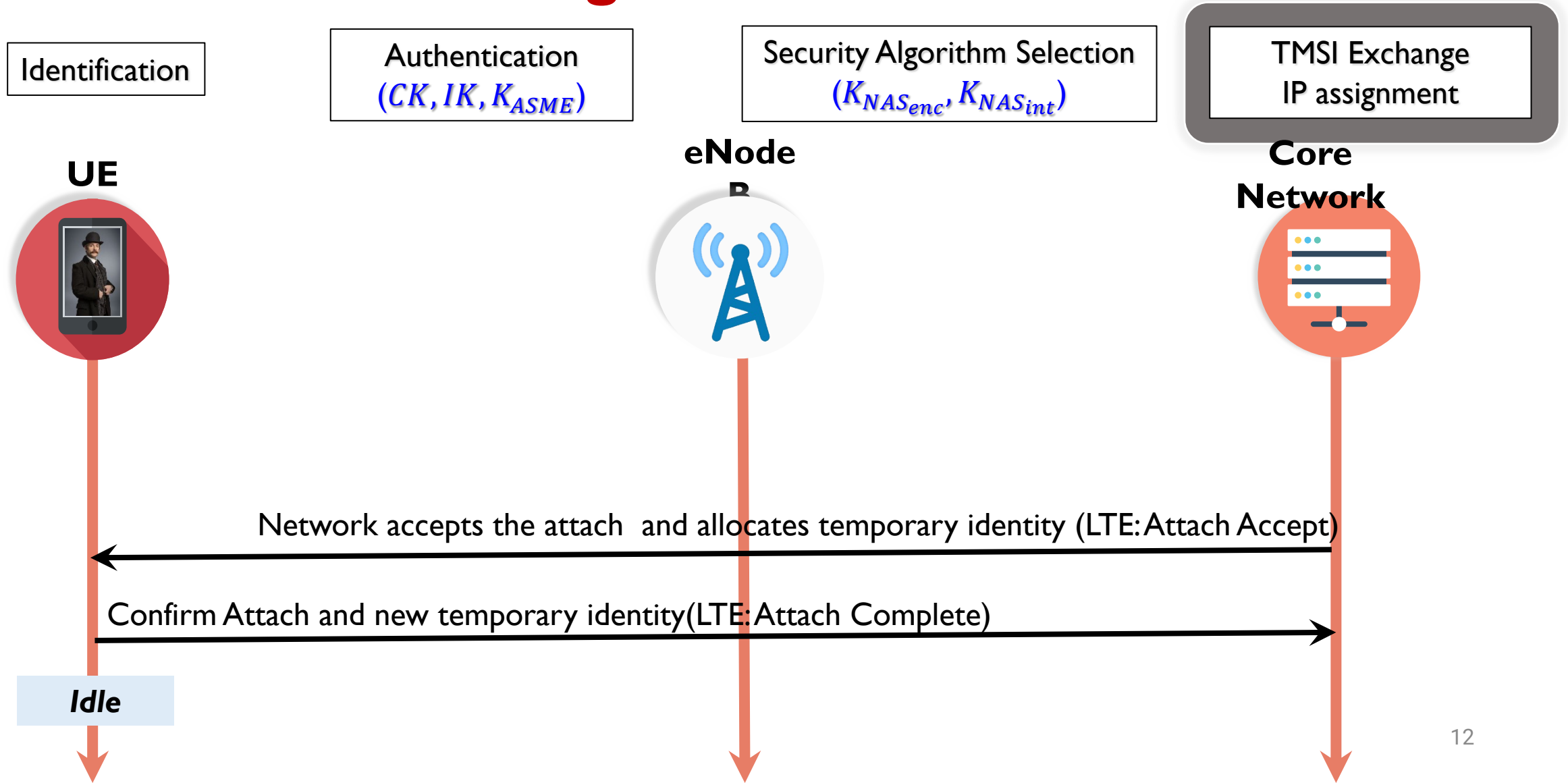
Select Security Algorithm (LTE: Security Mode Command)



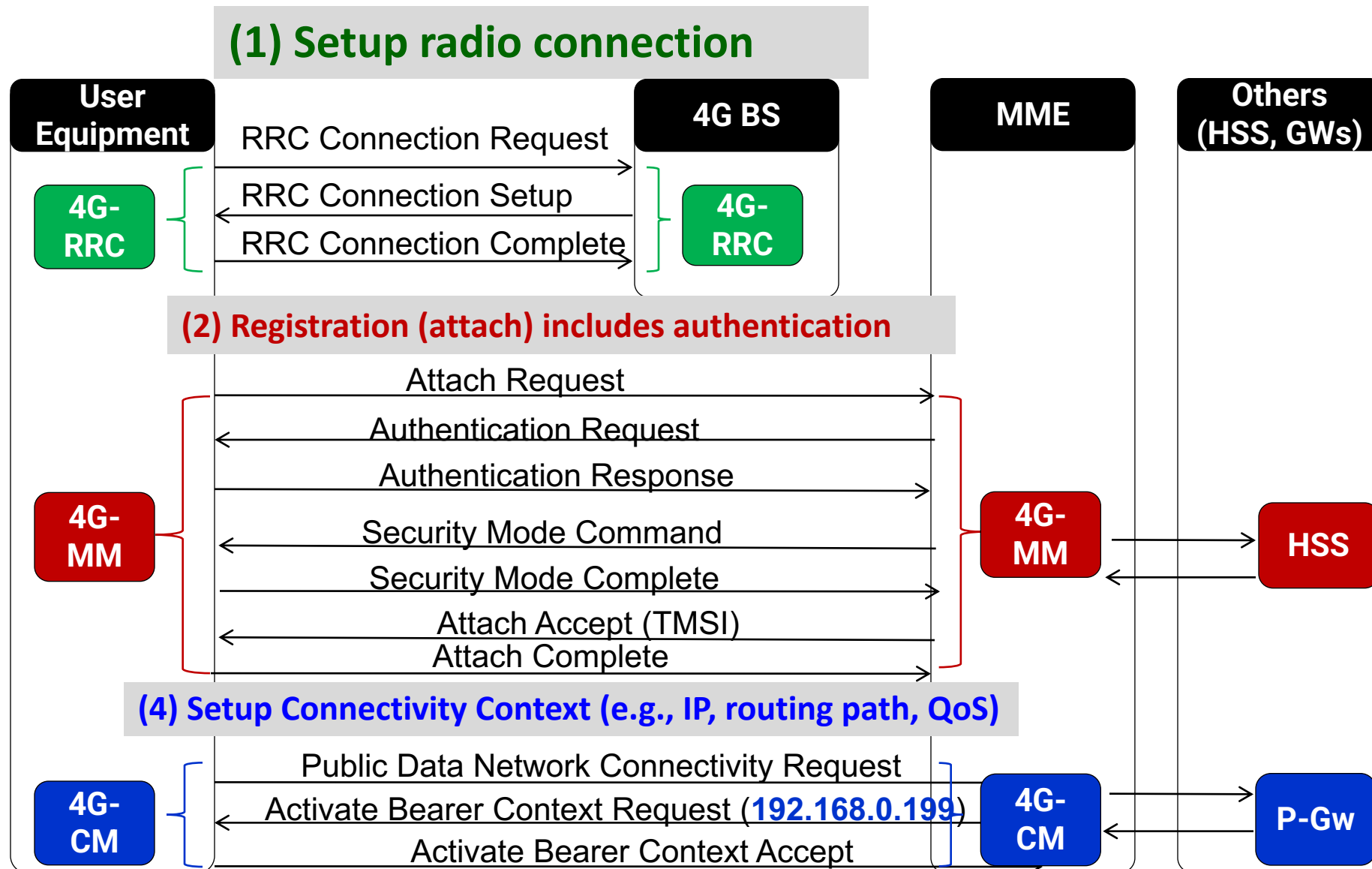
Confirm Security Algorithm (LTE: Security Mode Complete)



Attach/Registration Procedure



Setting Up Data Service in 4G

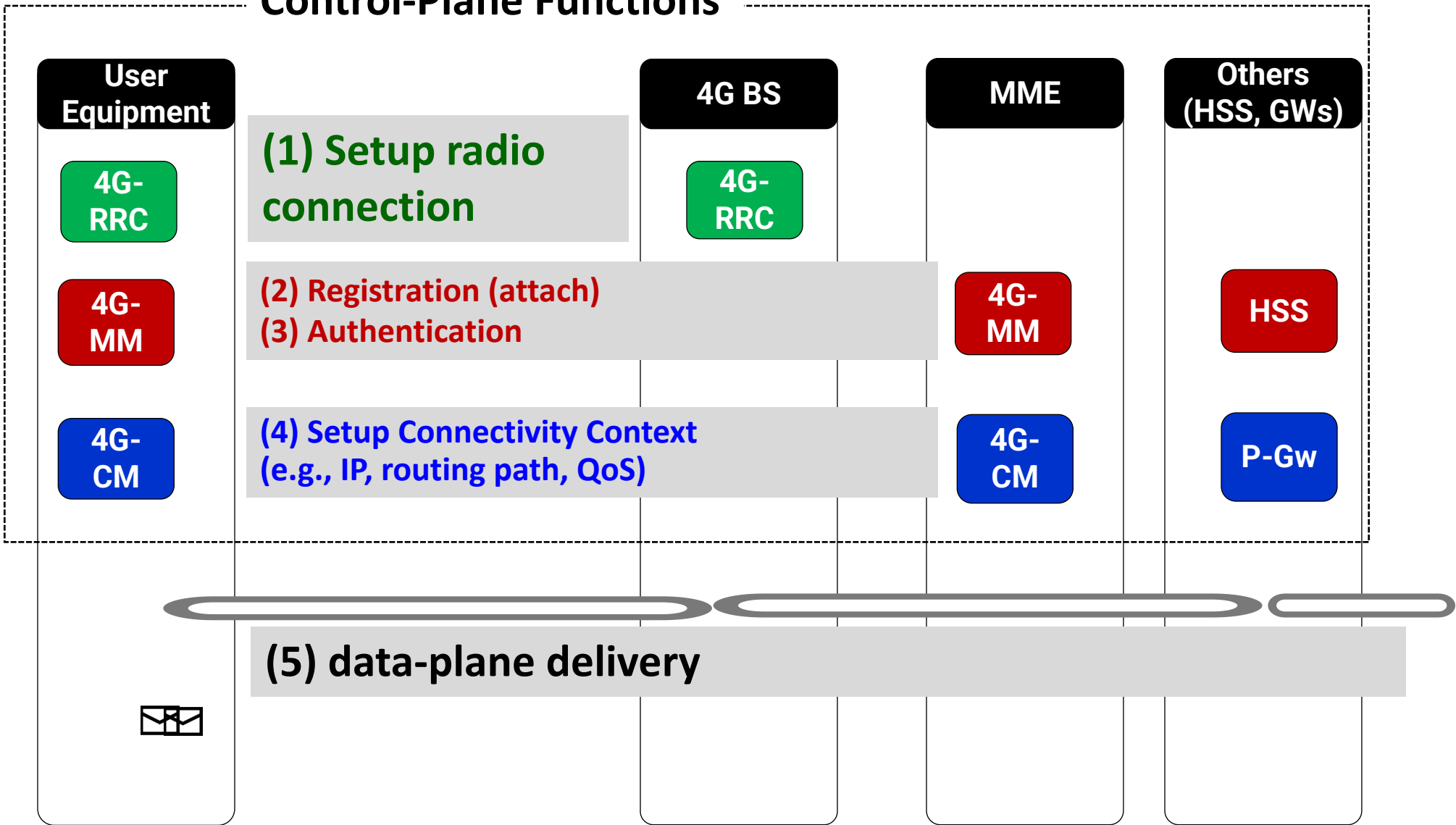


PDN: Public Data Network

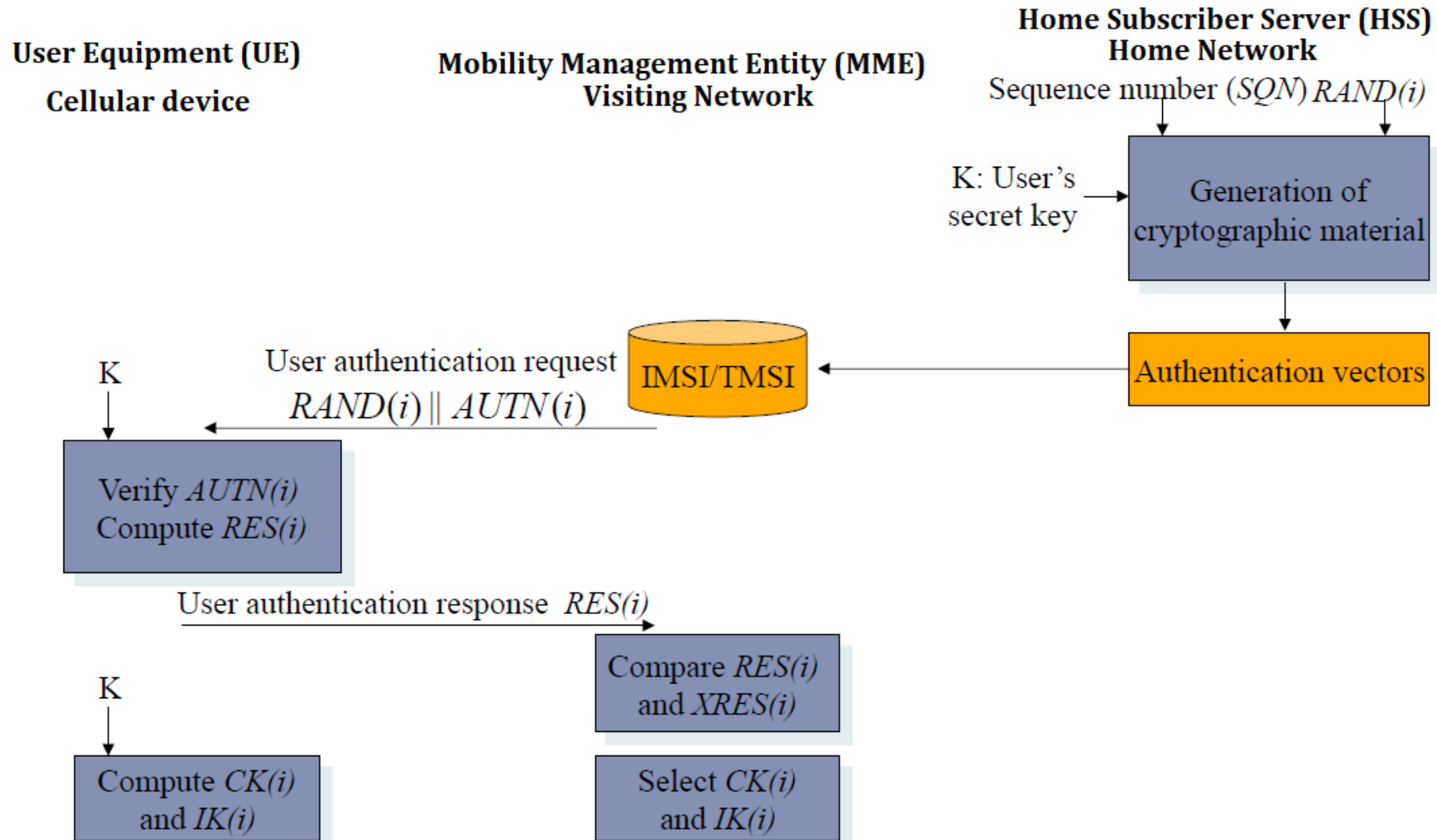
EPS: Evolved Packet System

Setting Up Data Service in 4G

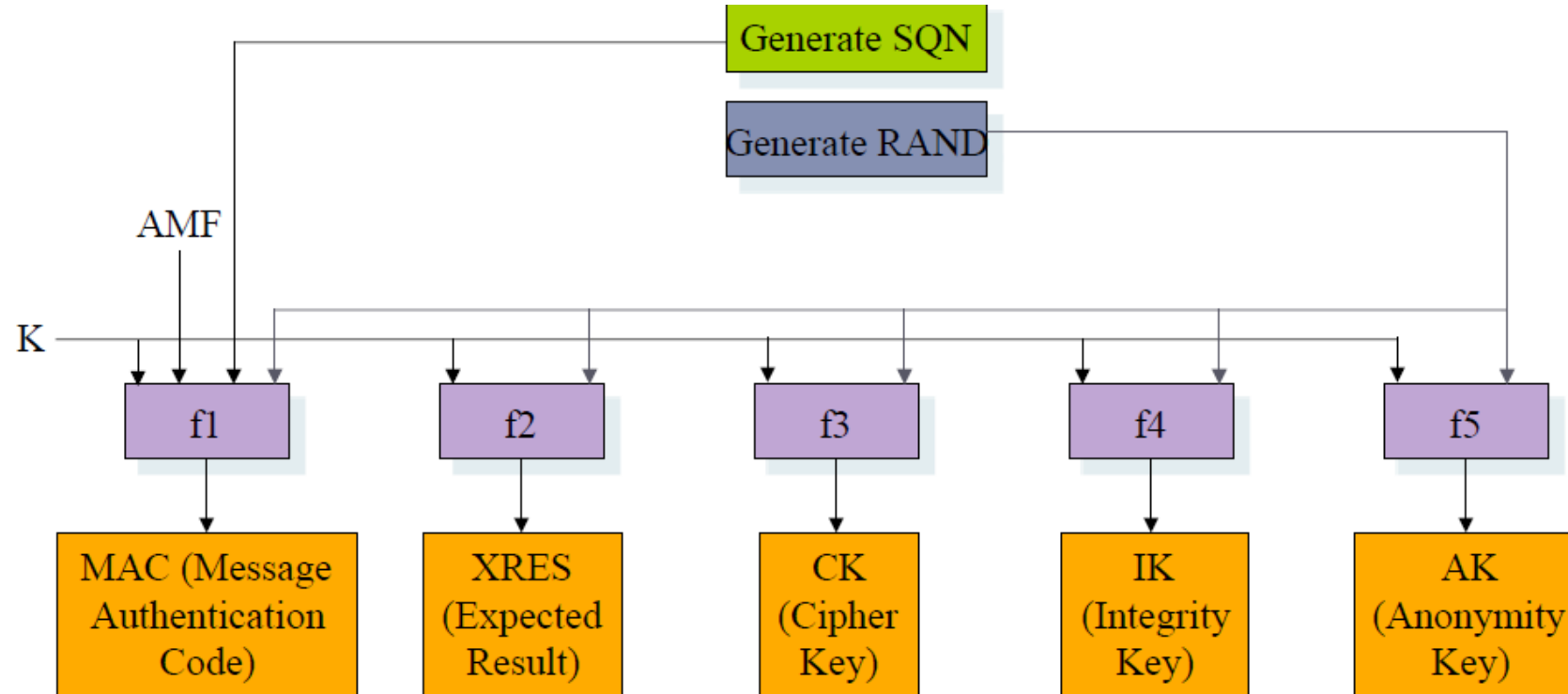
Control-Plane Functions



4G Authentication



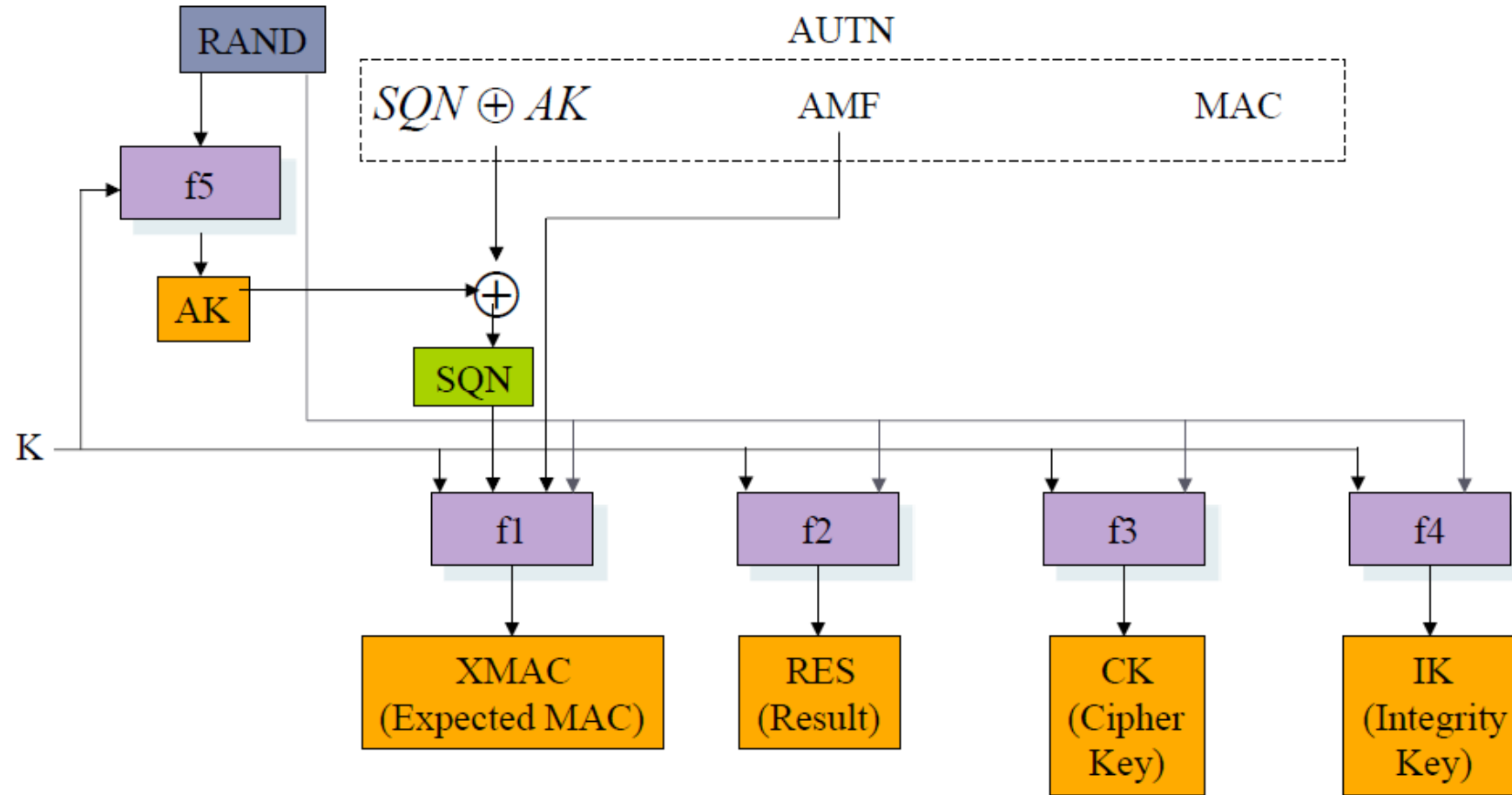
Generation of Authentication Vector or Challenge



$$AUTN := (SQN \oplus ACK) \parallel AMF \parallel MAC$$
$$AV := RAND \parallel XRES \parallel CK \parallel IK \parallel AUTN$$

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

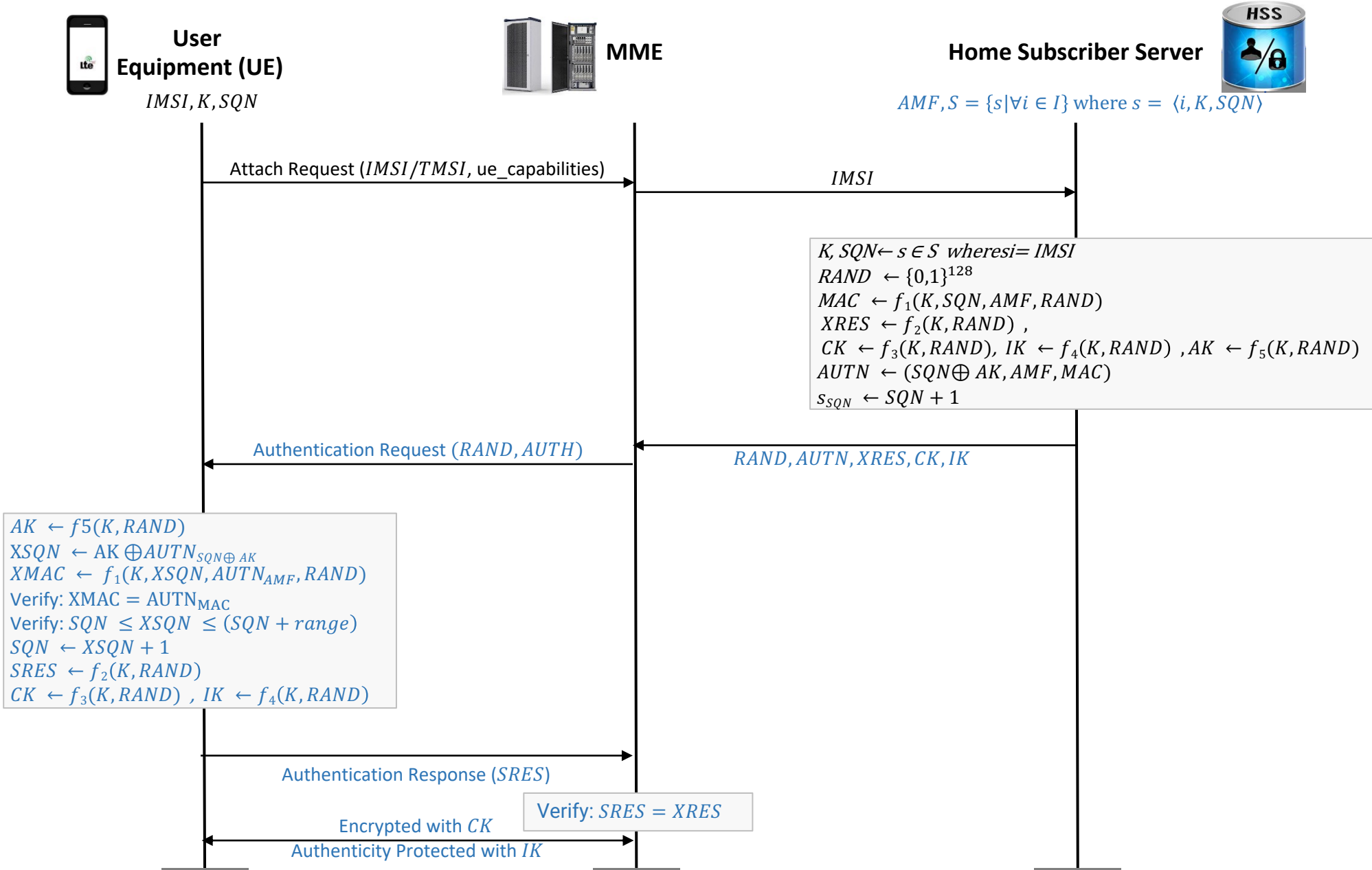
User Authentication Function in USIM



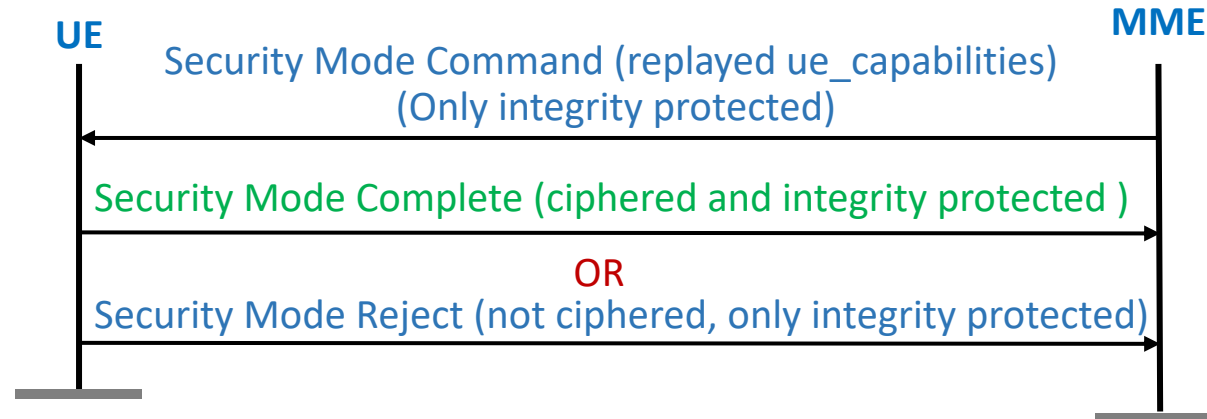
- Verify $MAC = XMAC$
- Verify that SQN is in the correct range

USIM: User Services Identity Module

Authentication in 4G



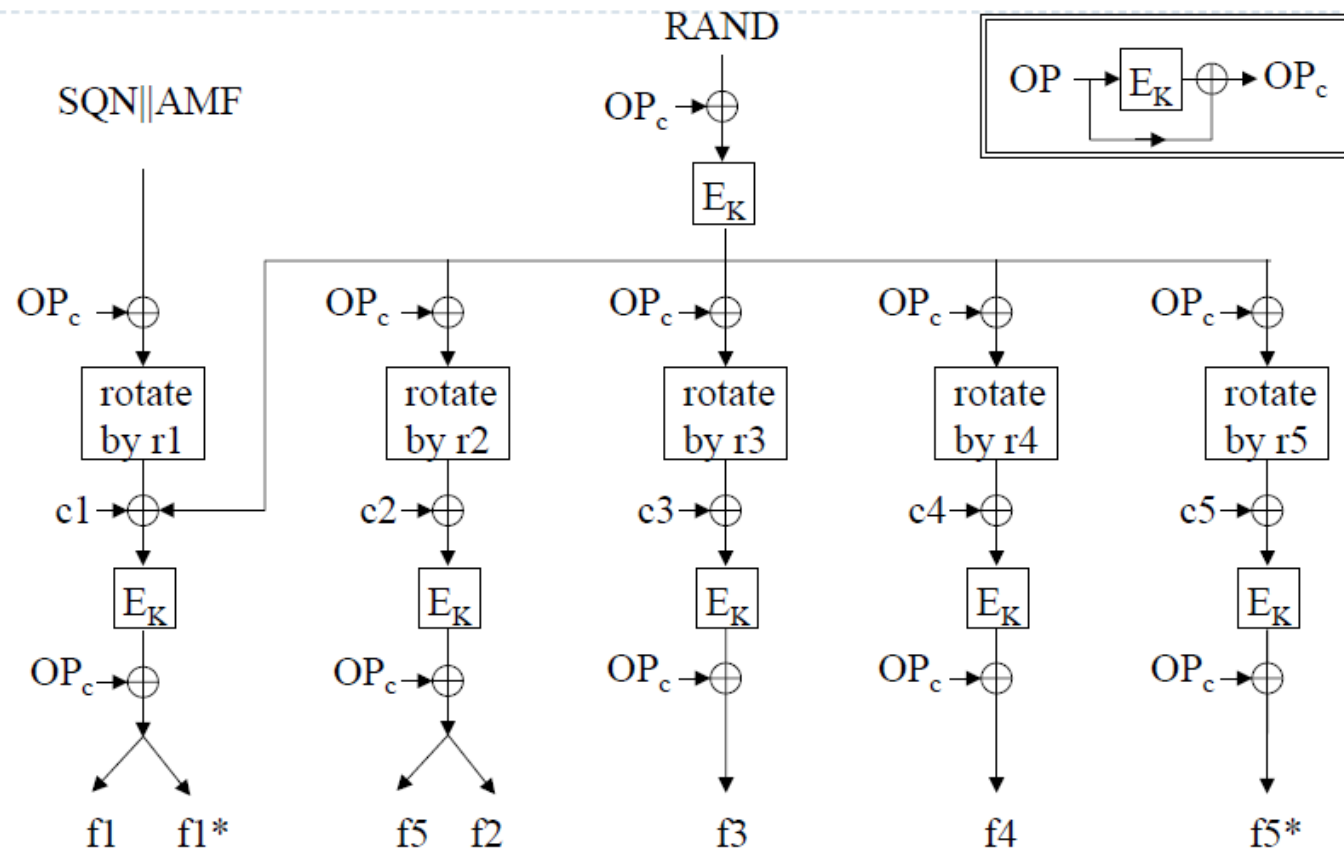
Security Mode Command Procedure



Authentication and Key Generation (AKA)

- In addition to f_1 , f_2 , f_3 , f_4 and f_5 , two more functions are defined: f_1^* and f_5^* , used in case the authentication procedure gets desynchronized (detected by the range of SQN).
- f_1 , f_1^* , f_2 , f_3 , f_4 , f_5 and f_5^* 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 $f_1 \dots f_5^*$ is based on the Rijndael algorithm

Generation of f_1 - f_5 , f_1^* , and f_5^* using Kernel Function E_K



OP : operator-specific parameter
 r_1, \dots, r_5 : fixed rotation constants
 c_1, \dots, c_5 : fixed addition constants

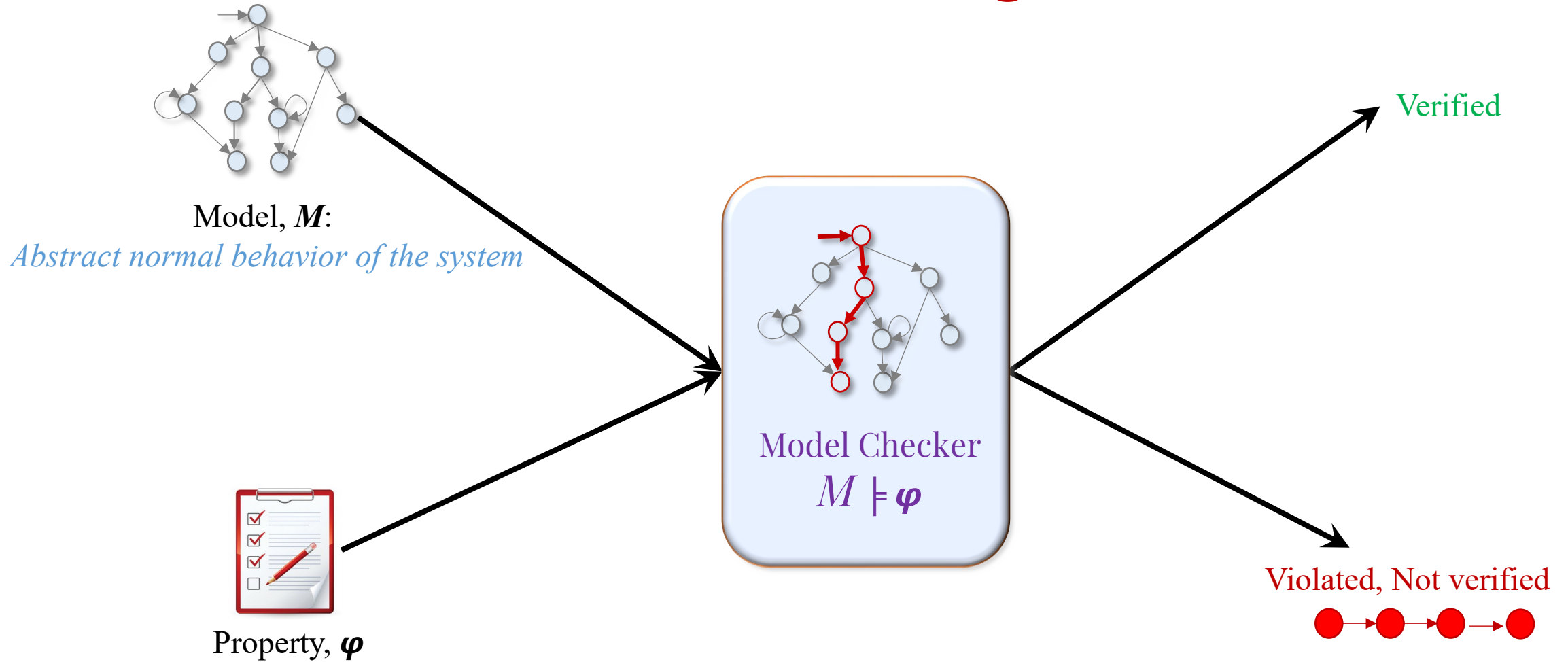
E_K : Rijndael block cipher with
 128 bits text input and 128 bits key



PennState

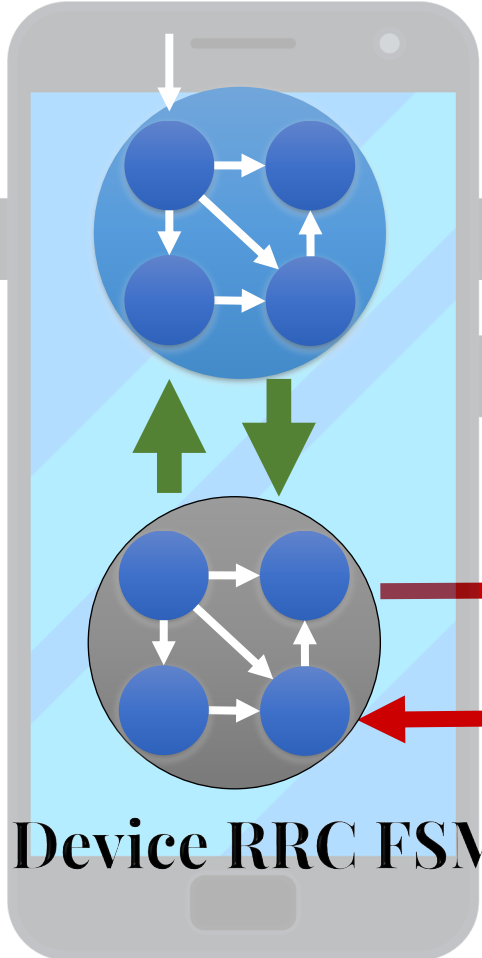
5GReasoner: A Property-Directed Security and Privacy Analysis Framework for 5G Cellular Network Protocol

Model Checking

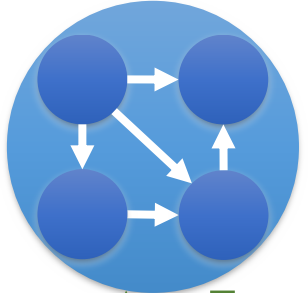


Dolev-Yao Adversary Model

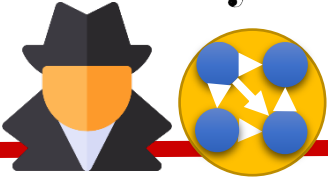
Device NAS FSM



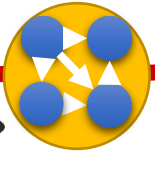
Core Network NAS FSM



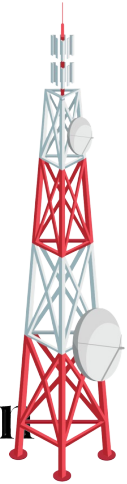
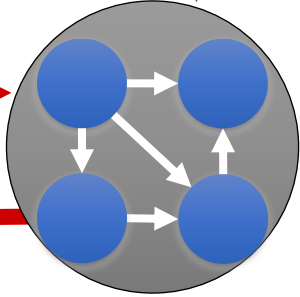
Adversary FSM



Adversary FSM



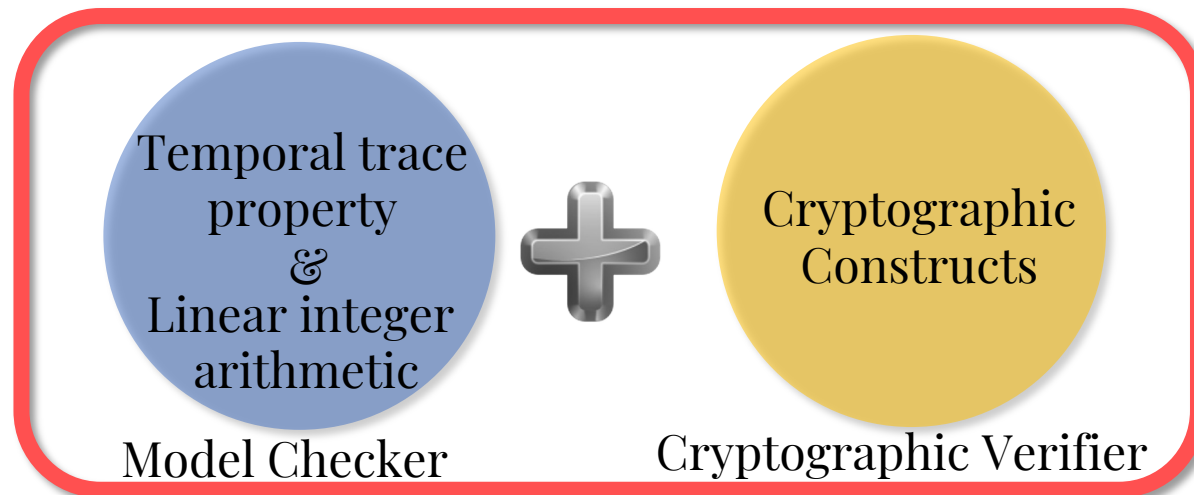
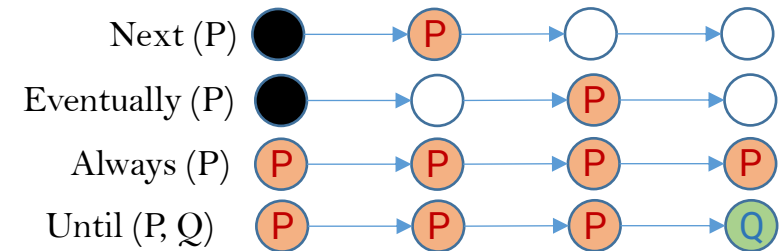
Base Station RRC FSM



Key Insight of Our Adversarial Testing Framework

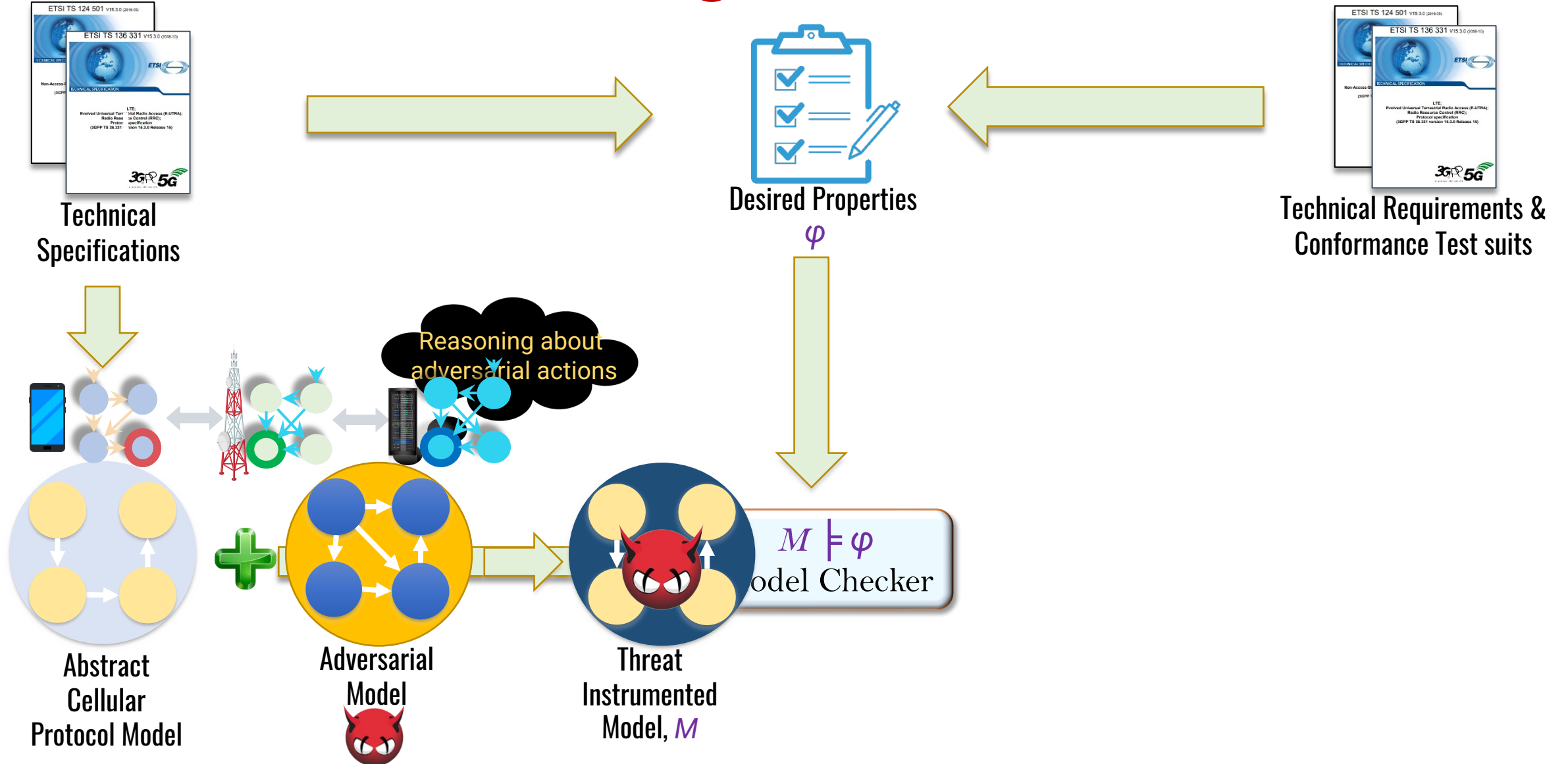
□ Property characteristics

- ✓ Temporal ordering of events
- ✓ Cryptographic constructs
- ✓ Linear integer arithmetic and other predicates
 - $SQN++$ and verify $SQN \leq XSN \leq (SQN + range)$

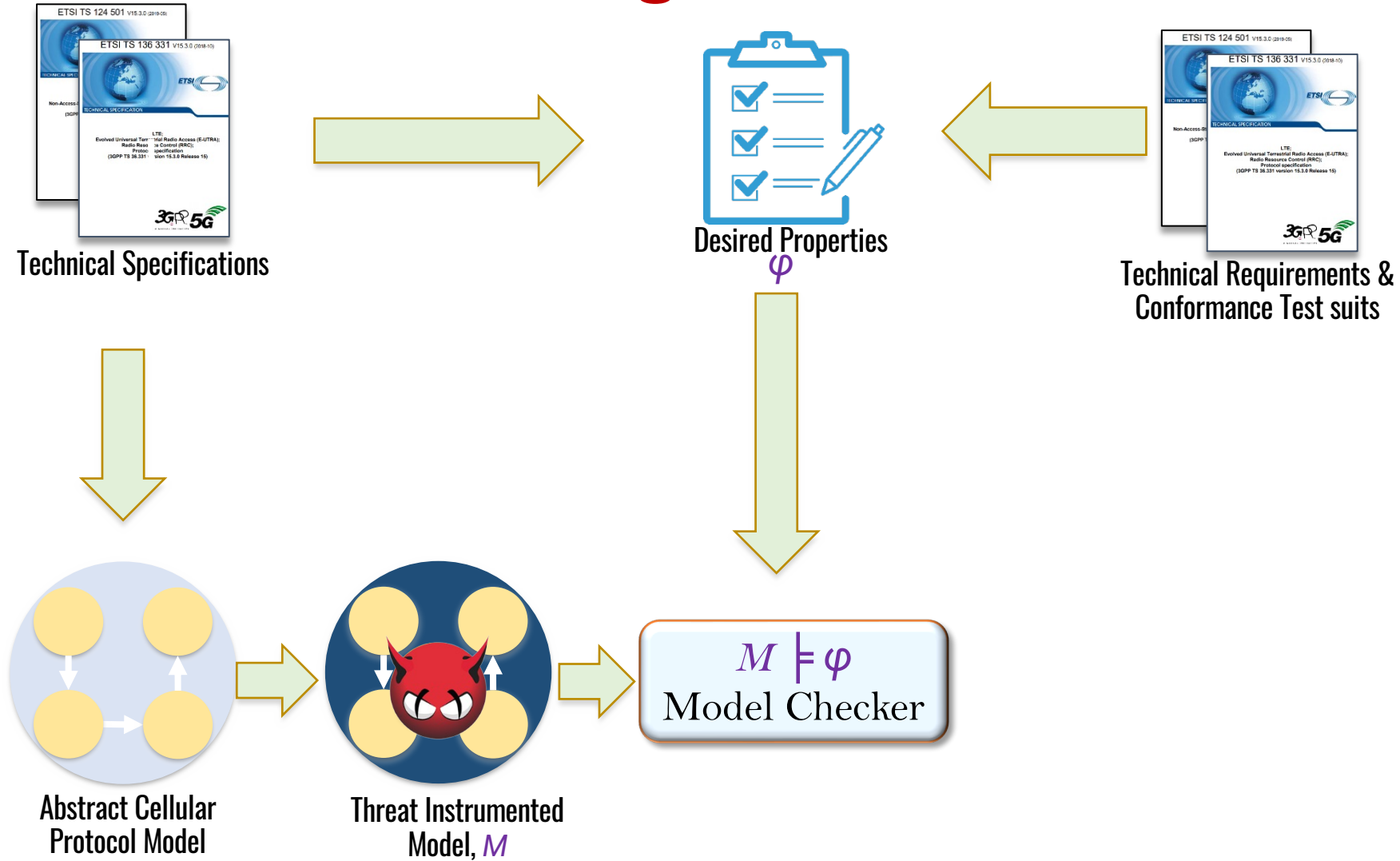


How can we leverage reasoning power of these two?

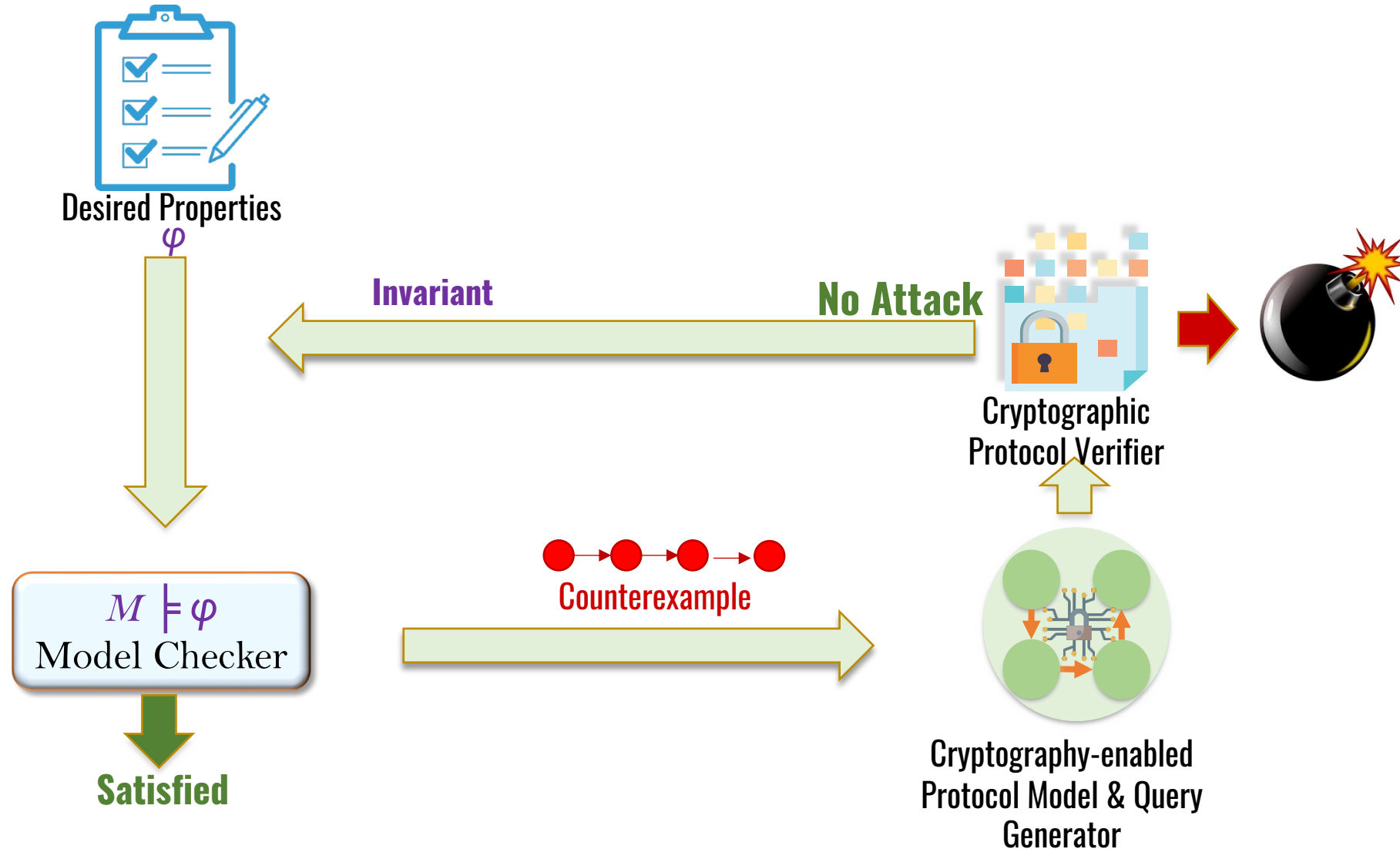
Adversarial Testing Framework: 5GReasoner



Adversarial Testing Framework: 5GReasoner



Adversarial Testing Framework: 5GReasoner

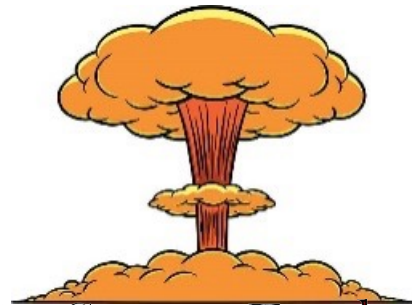


Addressing State Space Explosion

Multiple Protocol Layers

System Data and Packet Payload

E.g., Timer and Message Authentication Code



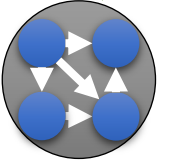
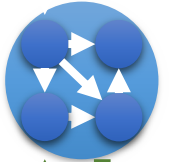
State Space Explosion

Behavior-Aware Predicate Abstraction

E.g., **Validity**, Presence, Grouping Predicates, etc.



NAS Layer FSM



RRC Layer FSM

Validity of MAC
(isValid_MAC)

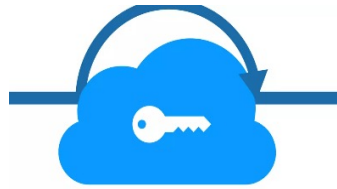


Validity Predicate

Findings

5G 11 new attacks

4G^{LTE} 10 new attacks



Authentication Bypass



Location tracking



TMSI exposure

Overbilling



Service Profiling



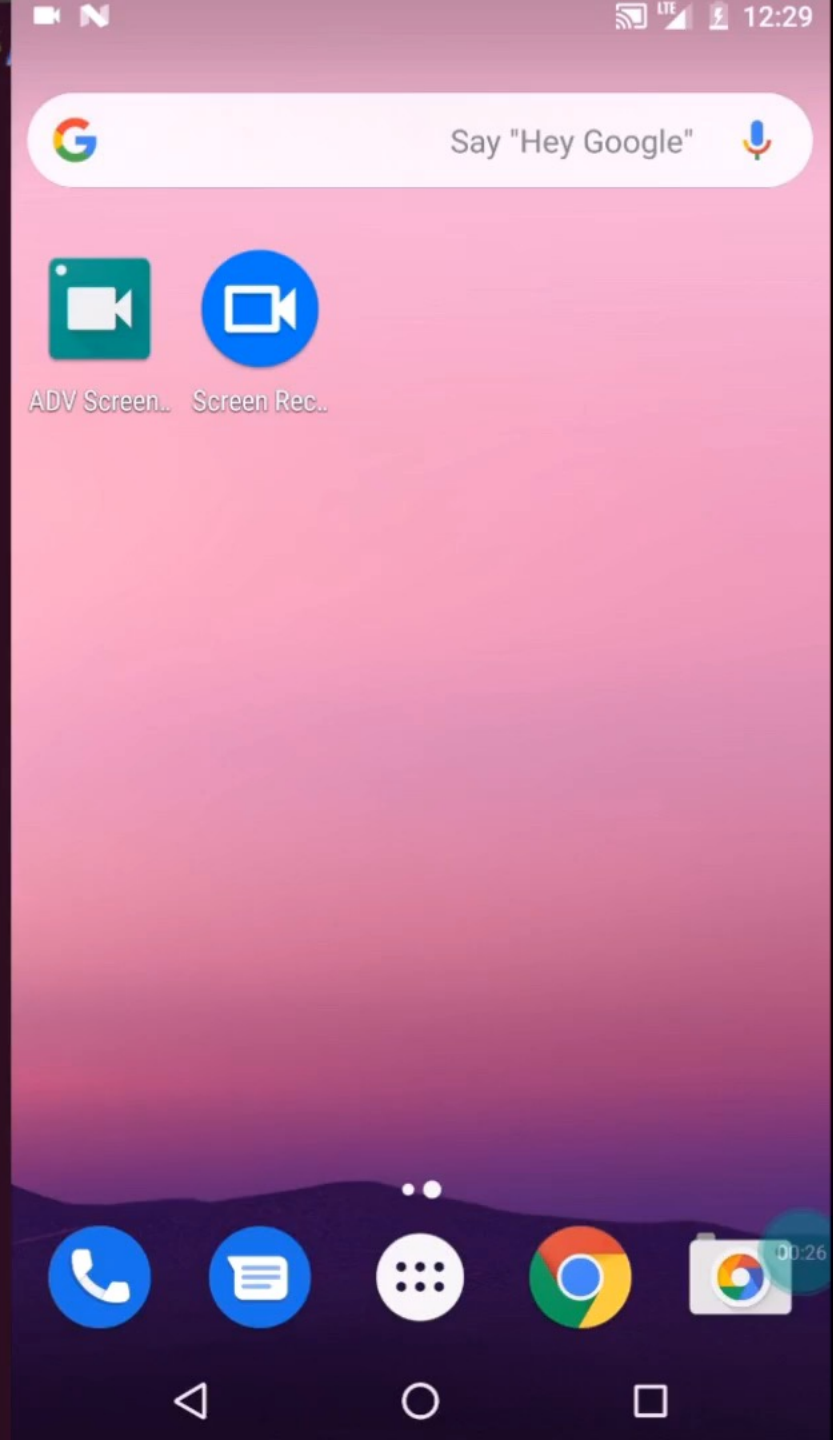
Battery depletion



Artificial Chaos

```
(base) cyber2slab@cyber2slab-ThinkPad-T480:~/Documents  
/src$
```

I

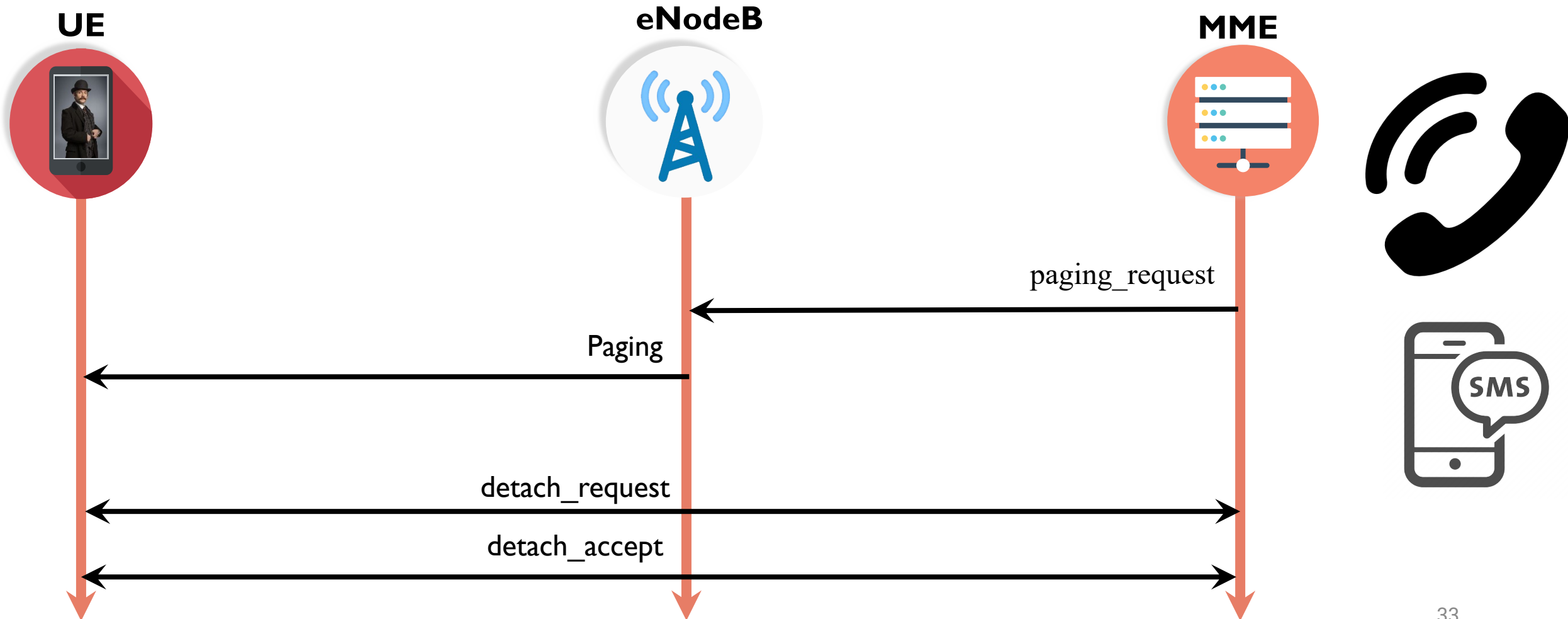




PennState

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

Background (Paging & Detach)



Paging Procedure



Paging Procedure



IDLE (RADIO OFF)



Base Station

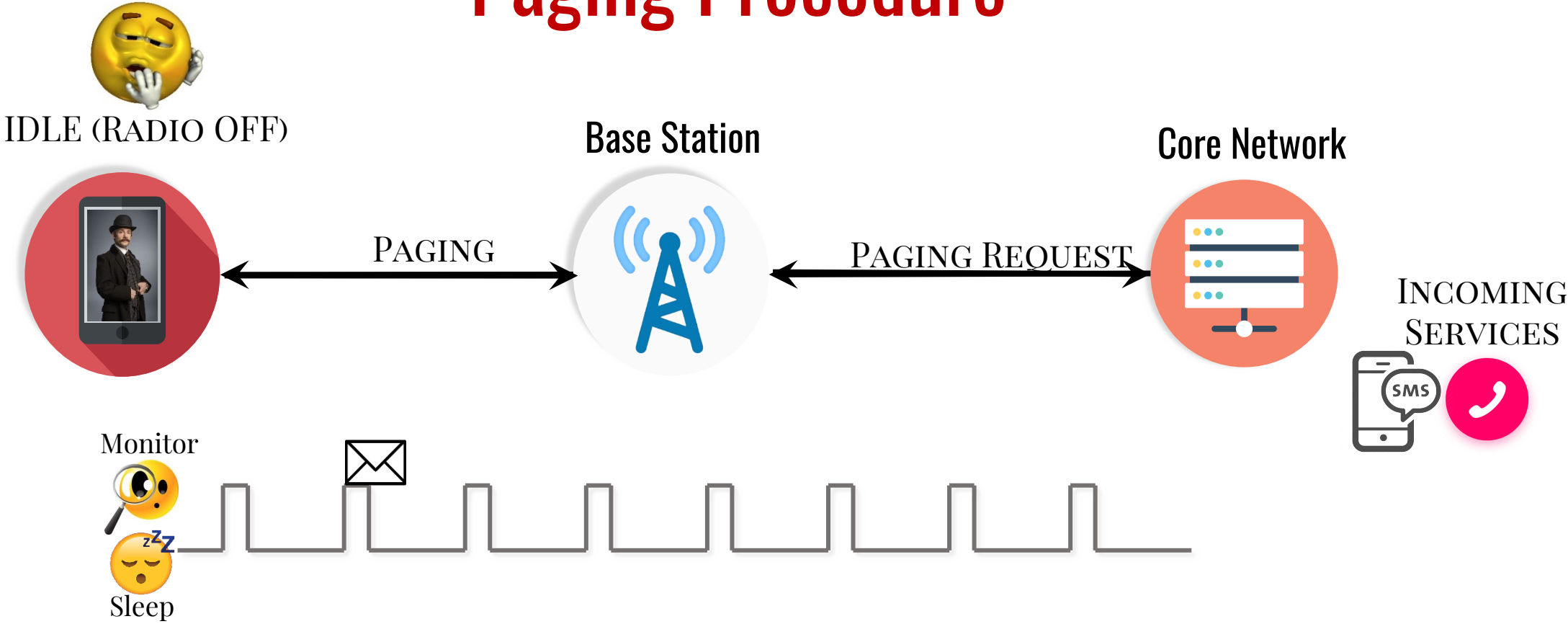


Core Network

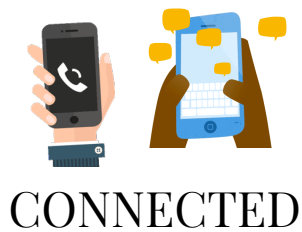


INCOMING SERVICES

Paging Procedure



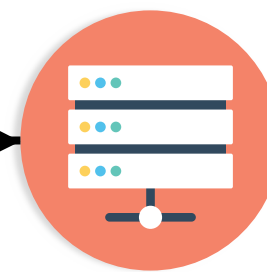
Paging Procedure



Base Station



Core Network



INCOMING SERVICES



CONNECT (IMSI/TMSI)

Monitor

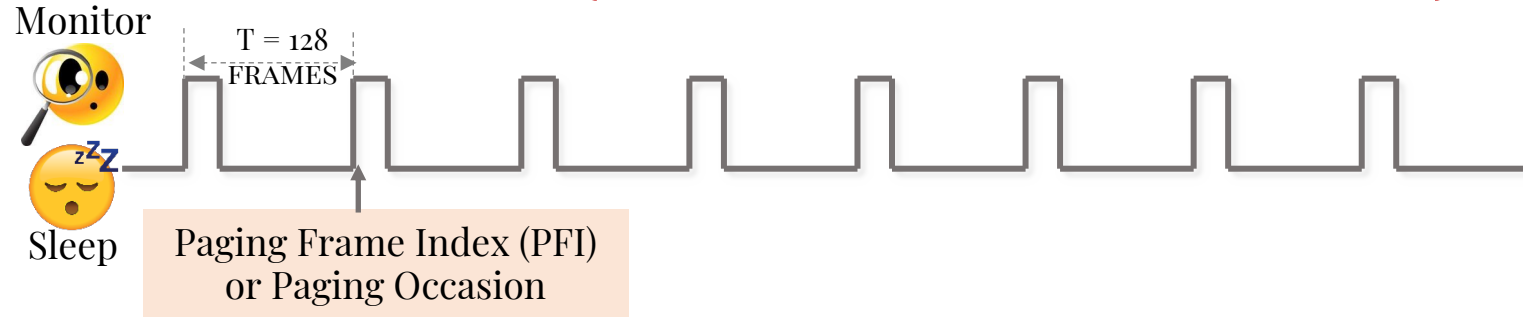


Sleep



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)



IMSI = 310 260 628687883 = 100011010XXX ... XXX **00001011**



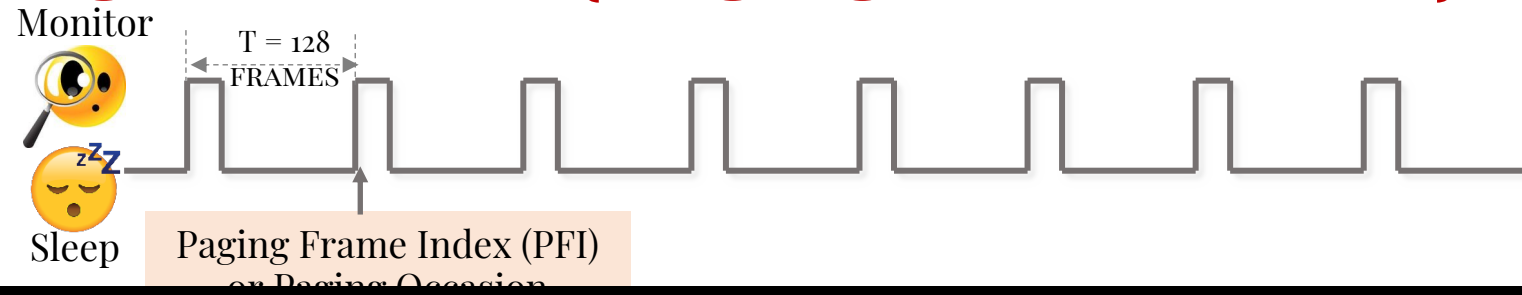
IMSI = 310 260 628687893 = 100011010XXX ... XXX **00010101**



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



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

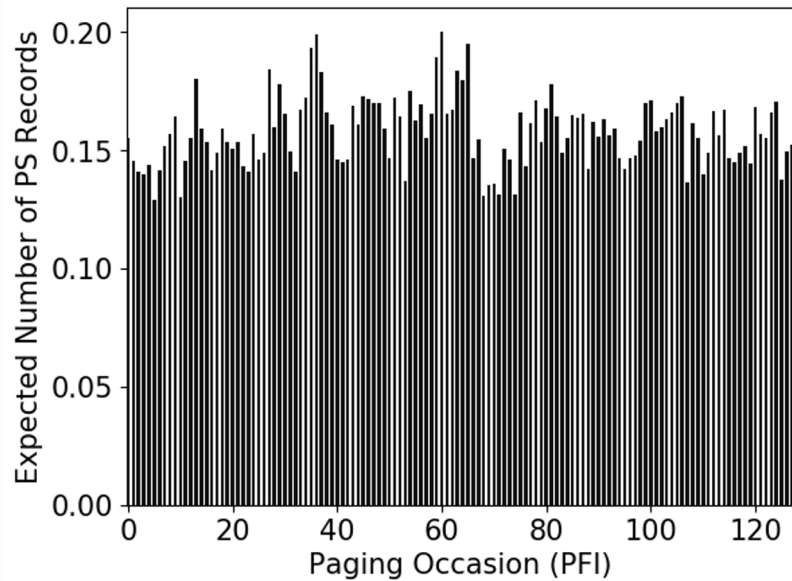


PAGING

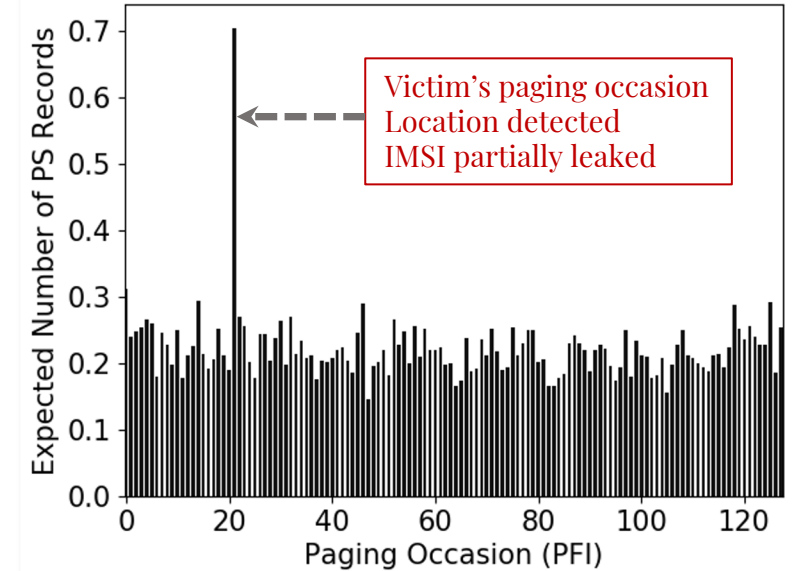


700-490-0301

<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



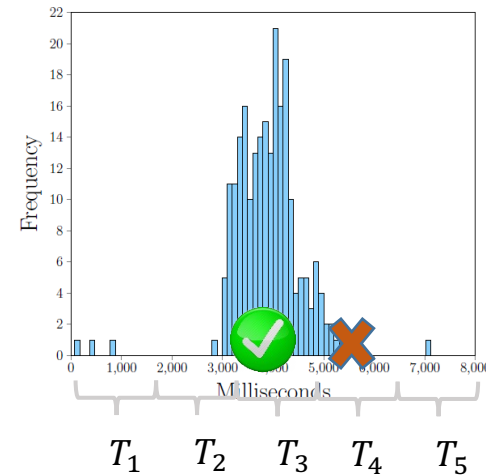
Likelihood Analysis – ToRPEDO Attack



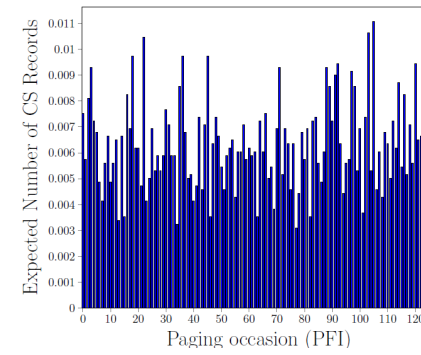
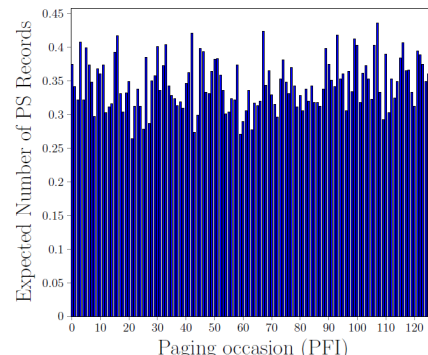
16 paging records with PS and CS indication



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

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

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



Compute the likelihood L_{-1}

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

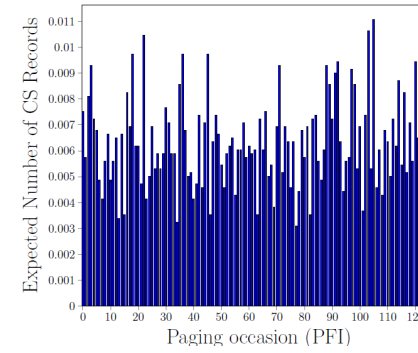
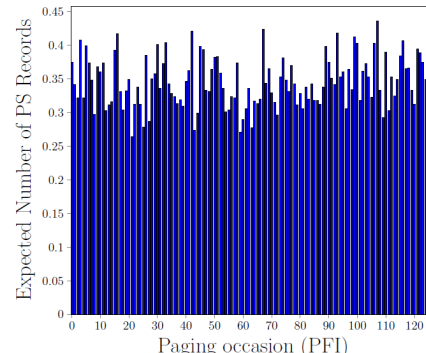


The adversary identifies i as the victim's PFI when

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

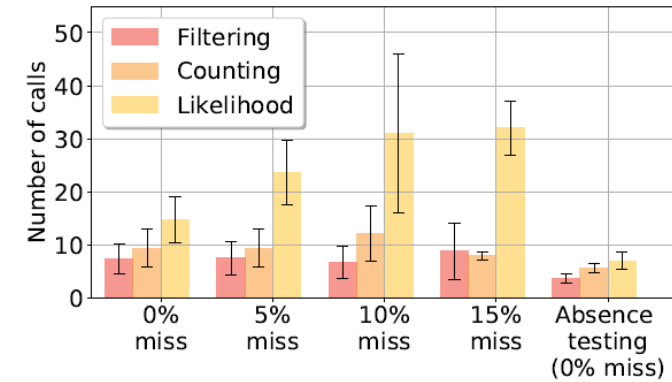
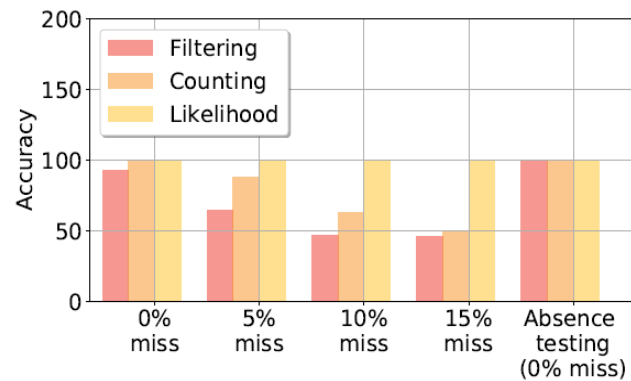


Base rate of PS, and CS records

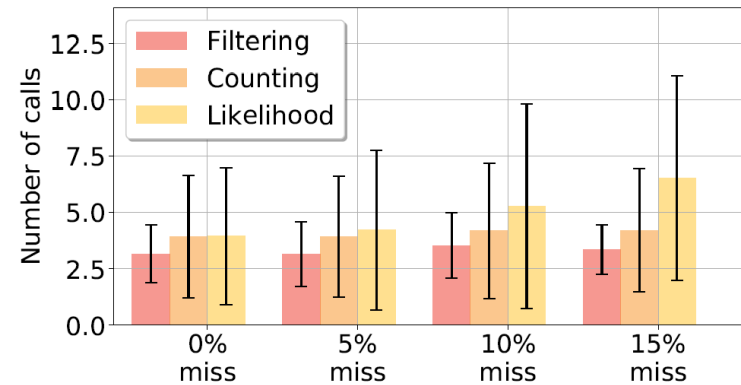
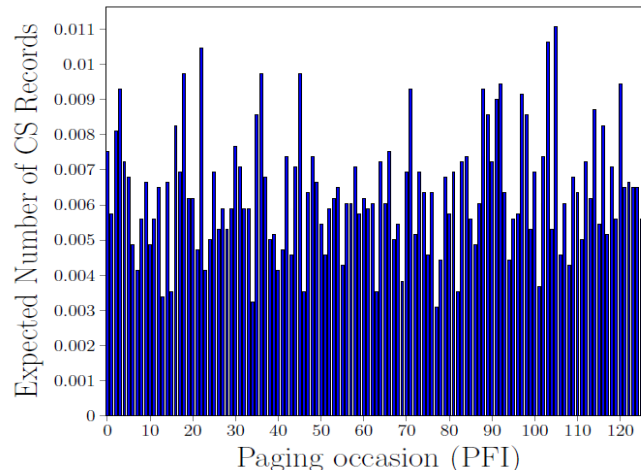


Evaluation and Mitigation

VoLTE calls (peak-time)

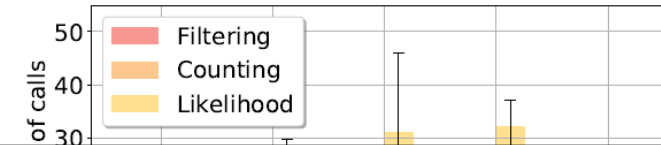


CSFB calls (peak-time)



Evaluation and Mitigation

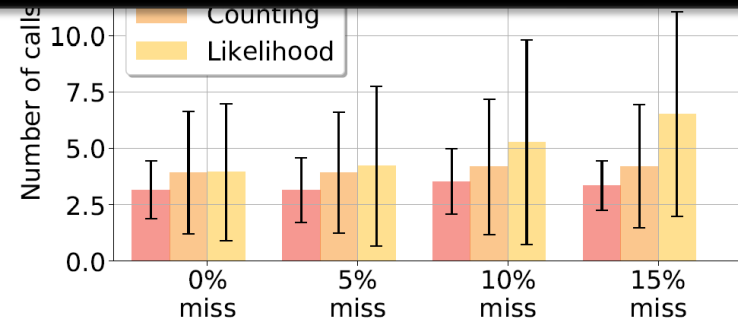
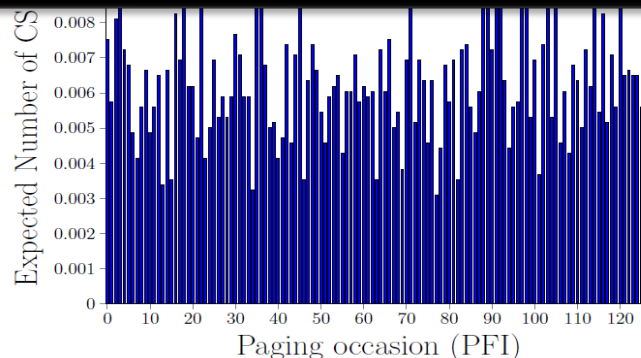
VoLTE calls (peak-time)



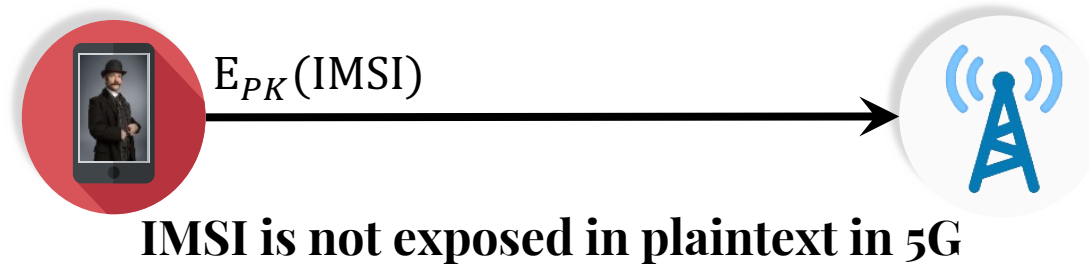
The adversary requires 4-10 phone calls/SMS/tweets/comments to identify PFI (last 7 bits of victim's IMSI)



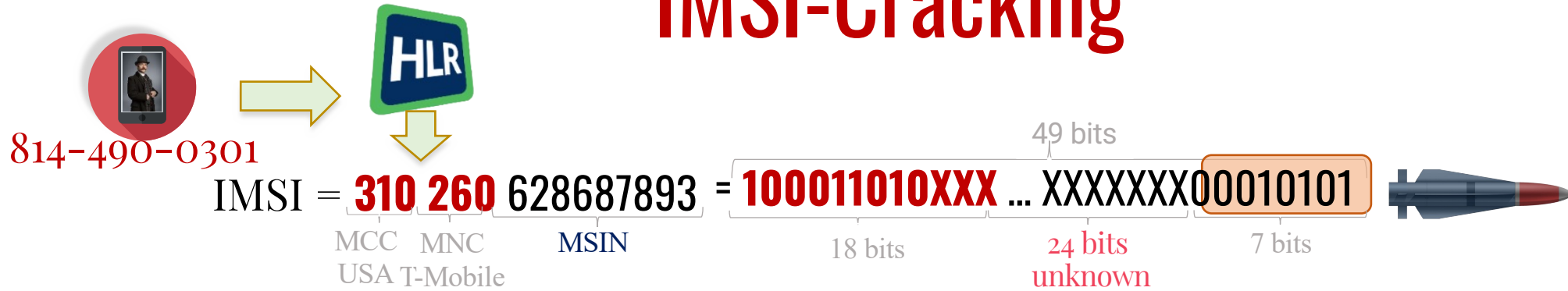
Variable paging occasion based on TMSI instead of IMSI



IMSI-Cracking



IMSI-Cracking



Exploit Registration Procedure

Victim



MitM Relay



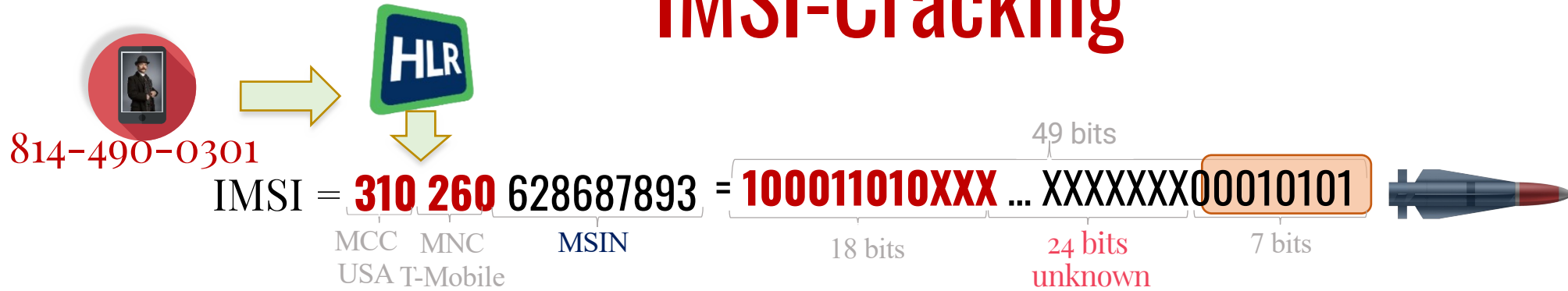
Legitimate Base Station + Core Network



Initial Connection Setup
(insecure)

IMSI	Key
IMSI_1	Key_1
IMSI_2	Key_2
IMSI_victim	Key_victim

IMSI-Cracking



Exploit Registration Procedure

Victim



MitM Relay



Legitimate Base Station + Core Network



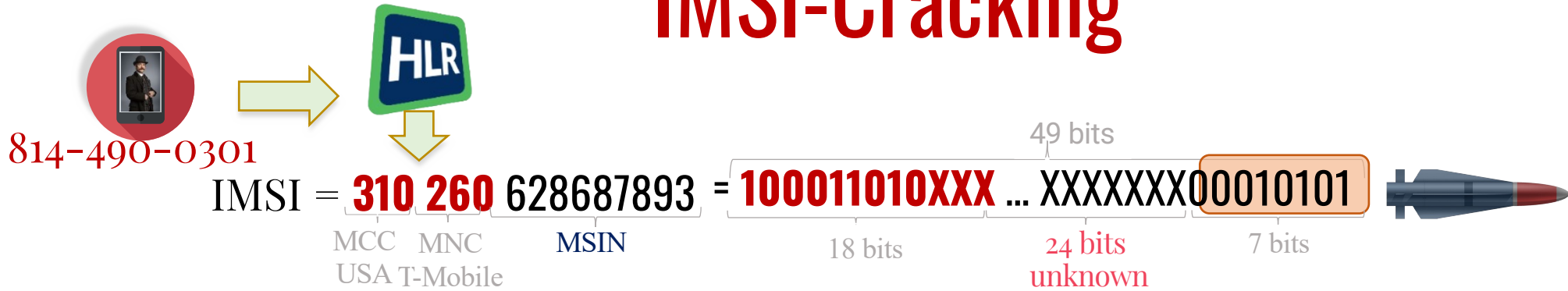
Registration Request
 $E_{PK}(IMSI_{guess})$

Registration Reject

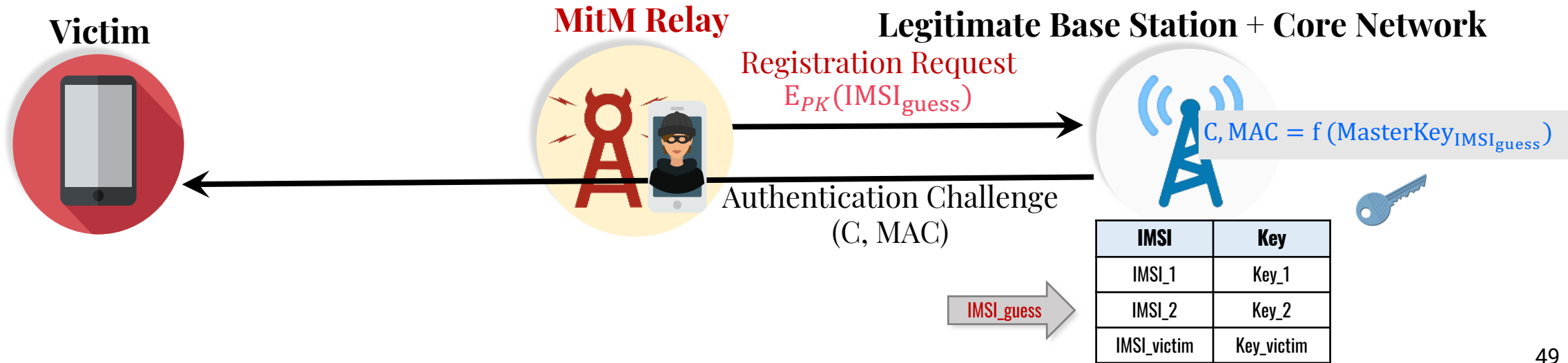
IMSI	Key
IMSI_1	Key_1
IMSI_2	Key_2
IMSI_victim	Key_victim

IMSI_guess

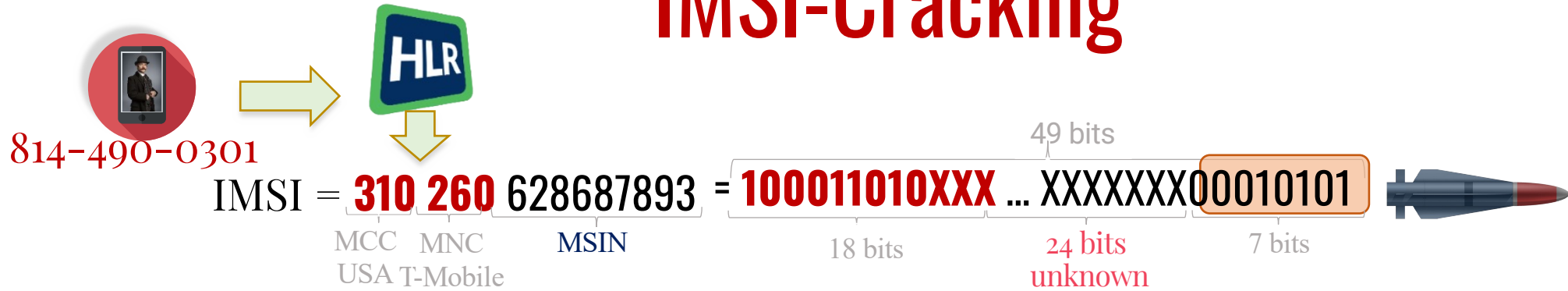
IMSI-Cracking



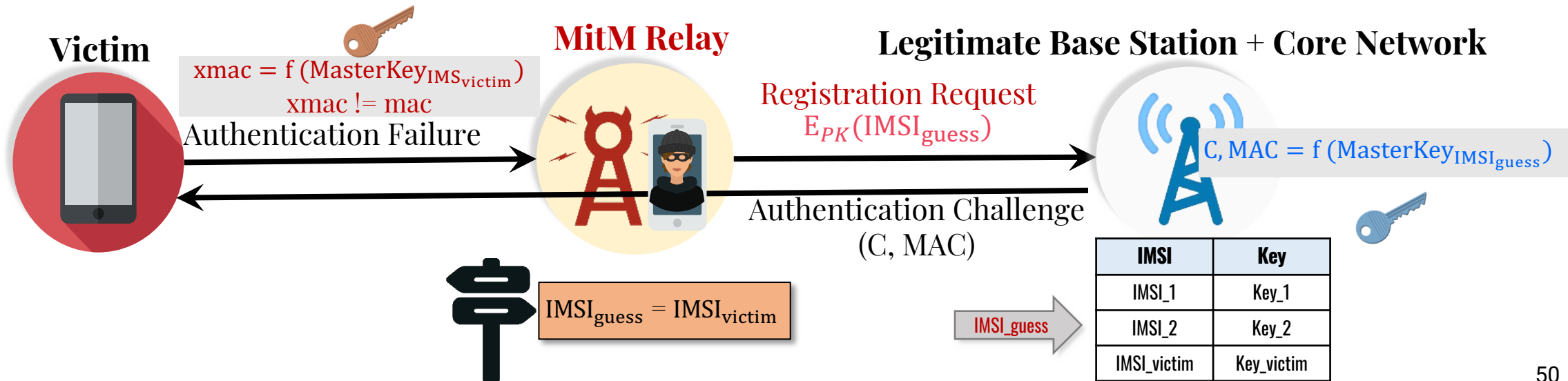
 **Exploit Registration Procedure**



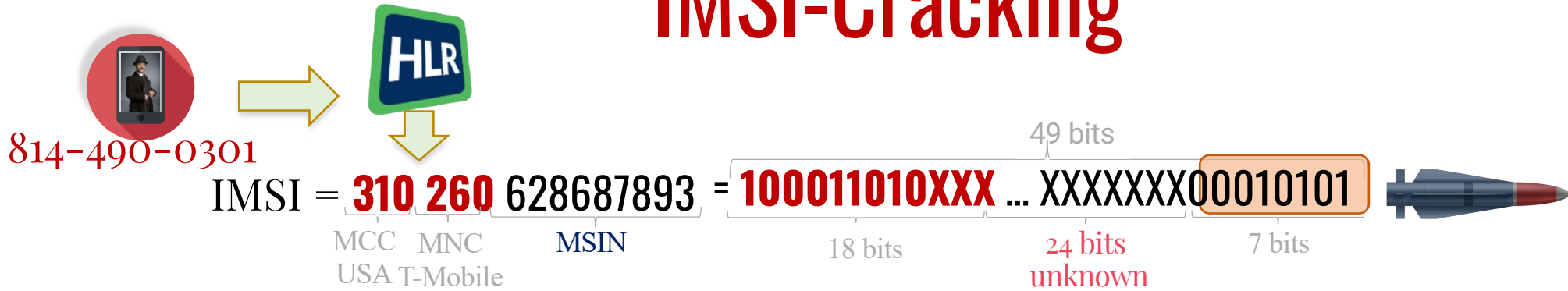
IMSI-Cracking



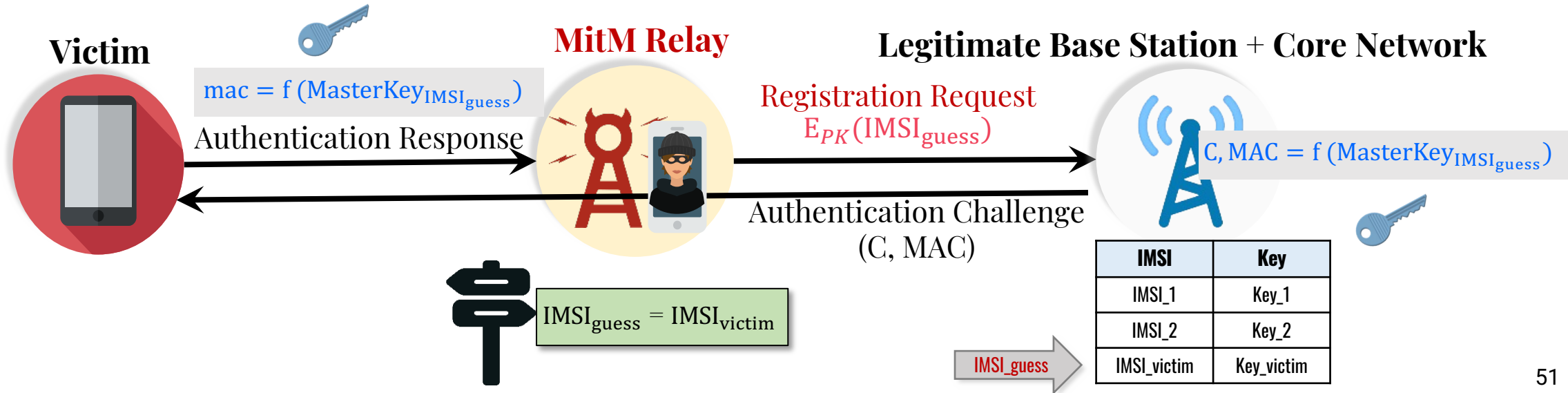
 Exploit Registration Procedure



IMSI-Cracking



 Exploit Registration Procedure



Summary and Discussion

- Primer on mobile network: architecture, protocols, operations
 - And its evolution
 - And its complexity
- 5GReasoner, ToRPEDO and IMSI-Cracking attack