Sherlock on Specs: Building LTE Conformance Tests through Automated Reasoning

Yi Chen, Di Tang, Yepeng Yao, Mingming Zha, XiaoFeng Wang,
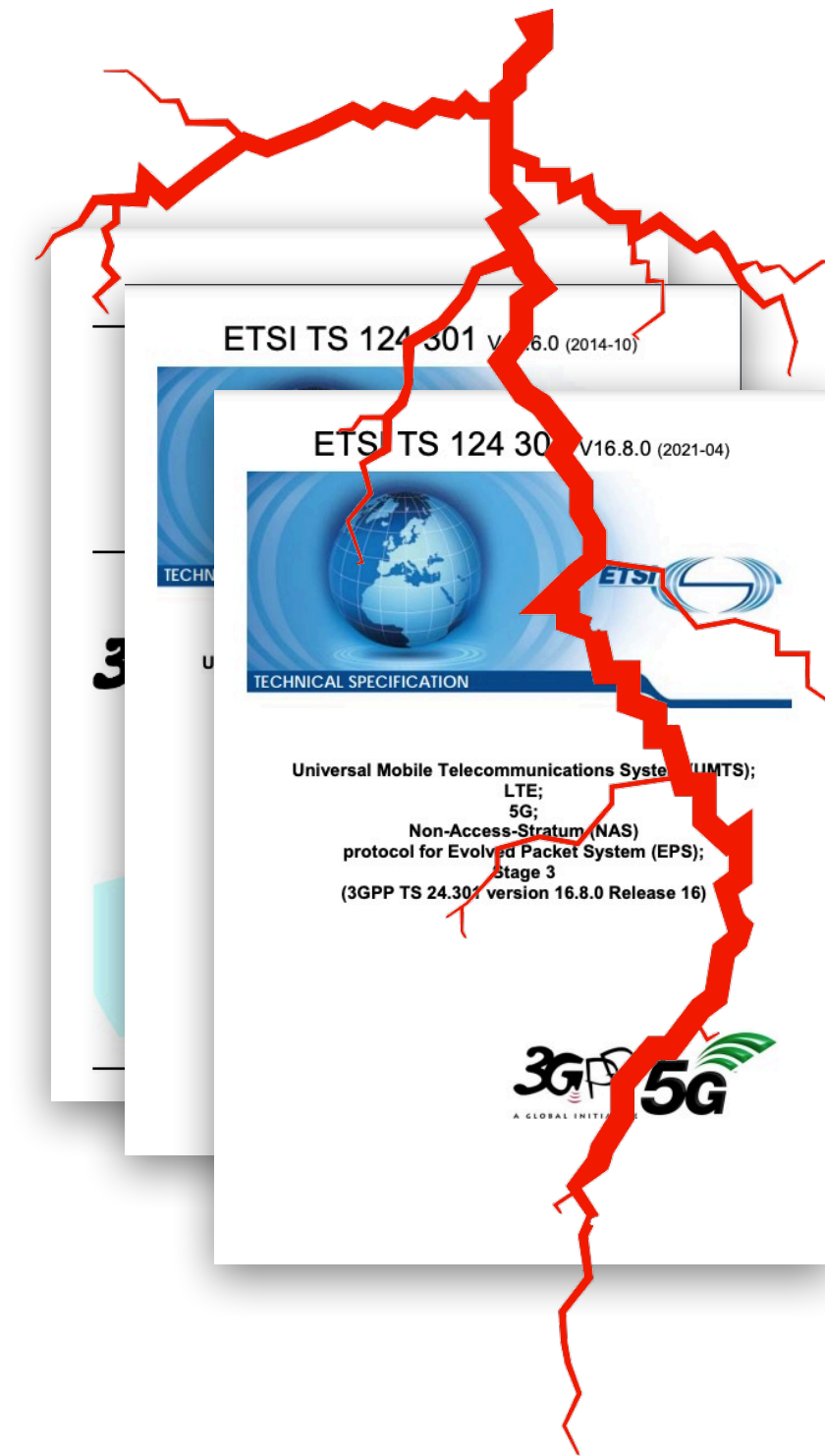Xiaozhong Liu, Haixu Tang, Baoxu Liu

INDIANA UNIVERSITY
BLOOMINGTON

中国科学院 信息工程研究所
INSTITUTE OF INFORMATION ENGINEERING, CAS

WPI

ETSI TS 124 301 V...6.0 (2014-10)

ETSI TS 124 30... V16.8.0 (2021-04)

TECHNICAL SPECIFICATION

Universal Mobile Telecommunications System (UMTS);
LTE;
5G;
Non-Access-Stratum (NAS)
protocol for Evolved Packet System (EPS);
Stage 3
(3GPP TS 24.301 version 16.8.0 Release 16)

3GPP 5G

Conformance Testing

❖ **2020 3GPP conformance testing: 37% of the goal**

❖ **LTE NAS conformance testing: 9 security-related in 665**

Automated Assistance

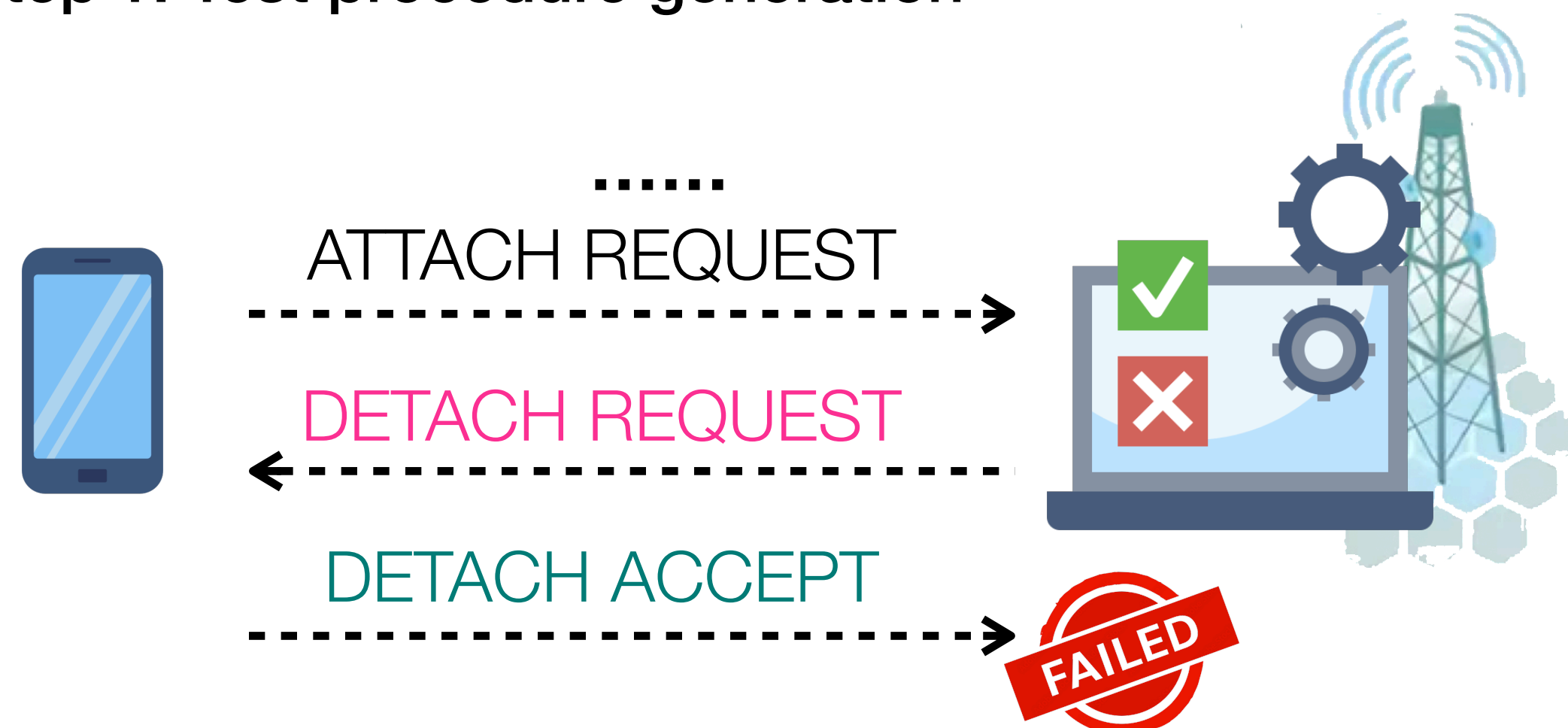## Conformance Testing
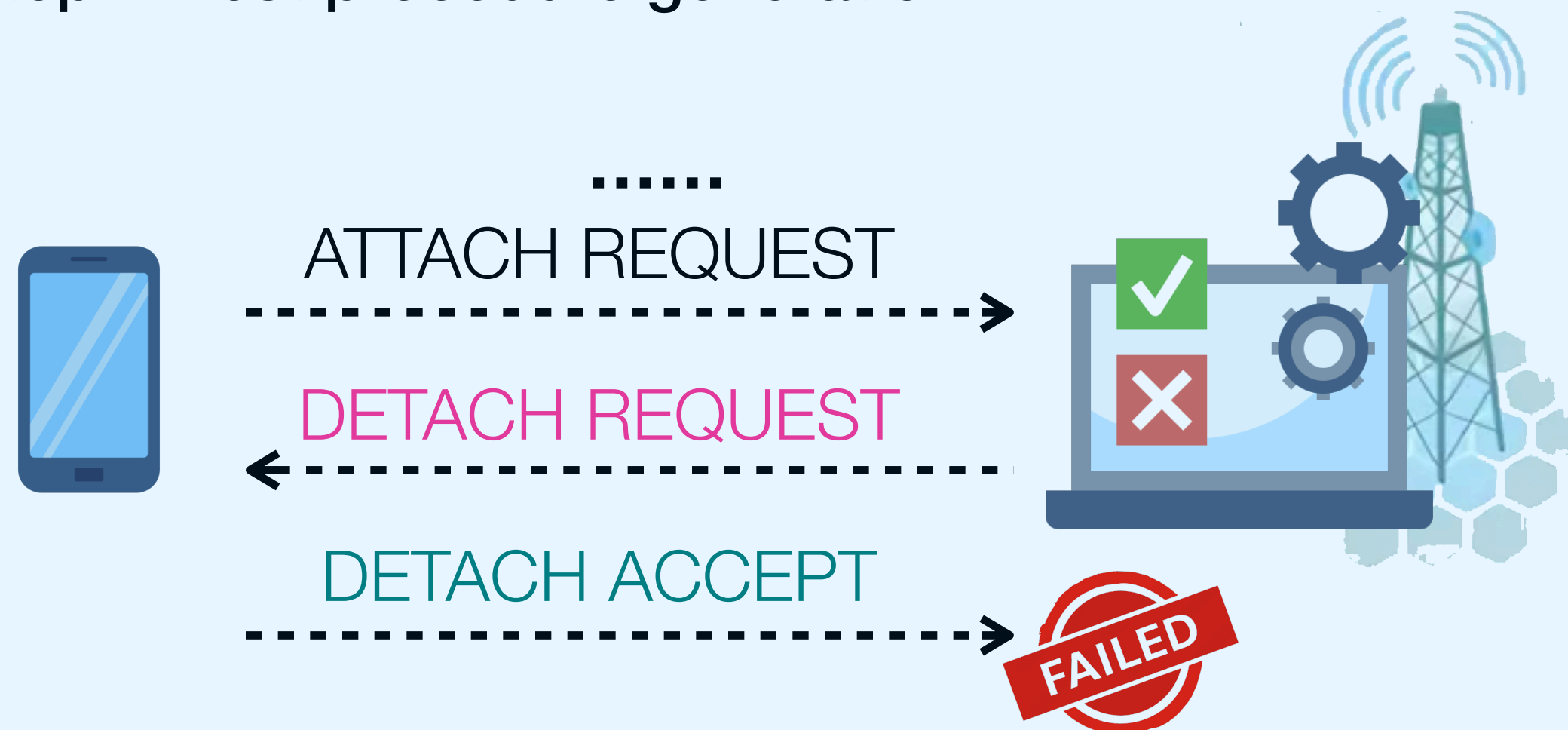
Input: Test purpose

condition event

initiate test status

[TS 24.301]: *If the **UE receives a DETACH REQUEST message** from the network **in state EMM-REGISTERED-INITIATED** and ..., the attach procedure shall be processed and the **DETACH REQUEST message shall be ignored***.
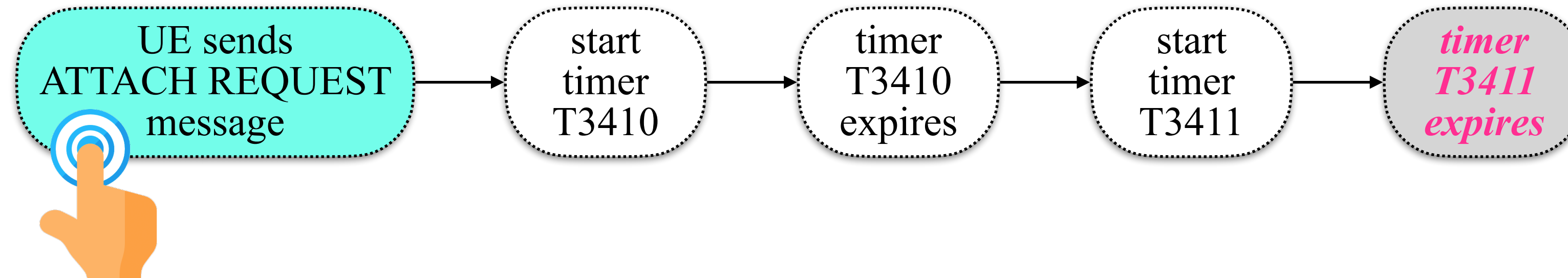
expected operation
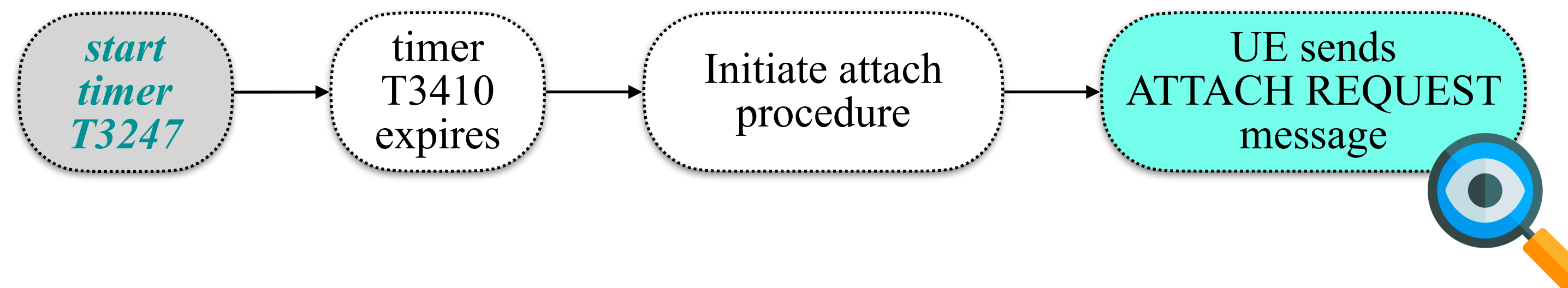
Step 1: Test procedure generation

ATTACH REQUEST

DETACH REQUEST

DETACH ACCEPT

FAILED

Test purpose 1

[TS 24.301]: *The UE shall initiate tracking area updating procedure **on the expiry of timer T3411**.*

?

```
UE sends          start         timer          start          timer
ATTACH REQUEST →  timer    →    T3410    →     timer    →     T3411
message           T3410         expires        T3411          expires
```

Test purpose 2

[TS 24.301]: *Upon receipt of an AUTHENTICATION REJECT message, if the message is received without integrity protection, the **UE shall start timer T3247** with a random value uniformly drawn from the range between 30 minutes and 60 minutes.*

?

```
start           timer                             UE sends
timer    →      T3410    →  Initiate attach  →   ATTACH REQUEST
T3247           expires     procedure             message
```

Test purpose 1

[TS 24.301]: *The UE shall initiate tracking area updating procedure **on the expiry of timer T3411**.*

...(13) ... ... (25) ...

UE sends ATTACH REQUEST message → start timer T3410 → timer T3410 expires → start timer T3411 → *timer T3411 expires*
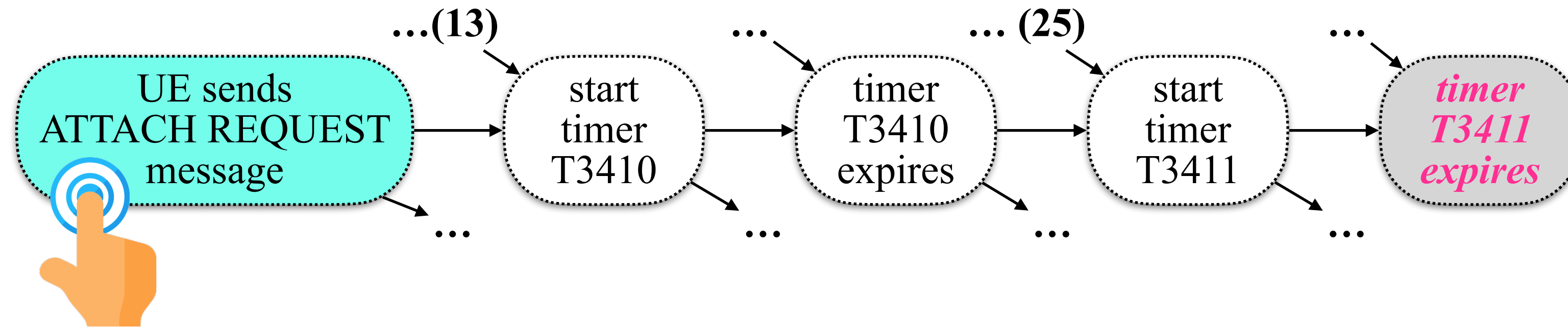
Test purpose 2

[TS 24.301]: *Upon receipt of an AUTHENTICATION REJECT message, if the message is received without integrity protection, the **UE shall start timer T3247** with a random value uniformly drawn from the range between 30 minutes and 60 minutes.*
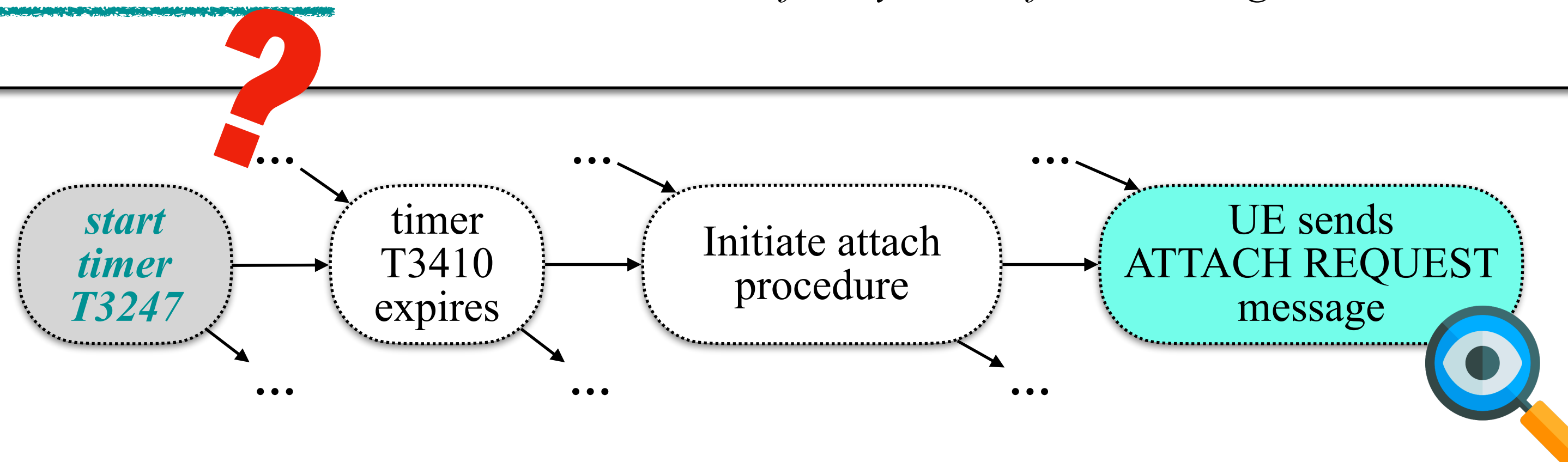
... ...

start timer T3247 → timer T3410 expires → Initiate attach procedure → UE sends ATTACH REQUEST message

Test purpose 1

[TS 24.301]: *The UE shall initiate tracking area updating procedure **on the expiry of timer T3411**.*

Step 2: recover the chain

Step 3: construct test procedure

Step 1: build the event dependency graph (EDG)

Test purpose 2

[TS 24.301]: *Upon receipt of an AUTHENTICATION REJECT message, if the message is received without integrity protection, the **UE shall start timer T3247** with a random value uniformly drawn from the range between 30 minutes and 60 minutes.*

[TS 24.301]: *Upon* *expiry of timer T3247,* *the UE shall initiate an EPS attach procedure.*

Upon expiry of timer T3247	,	*the UE*	*shall*
ARGM-TMP		ARG0	ARGM-MOD

initiate	*an EPS attach procedure*	.
V	ARG1	

expiry of timer T3247

the UE shall initiate an EPS attach procedure

[TS 24.301]: *the UE initiates the attach procedure* *by sending an ATTACH REQUEST message to the MME.*

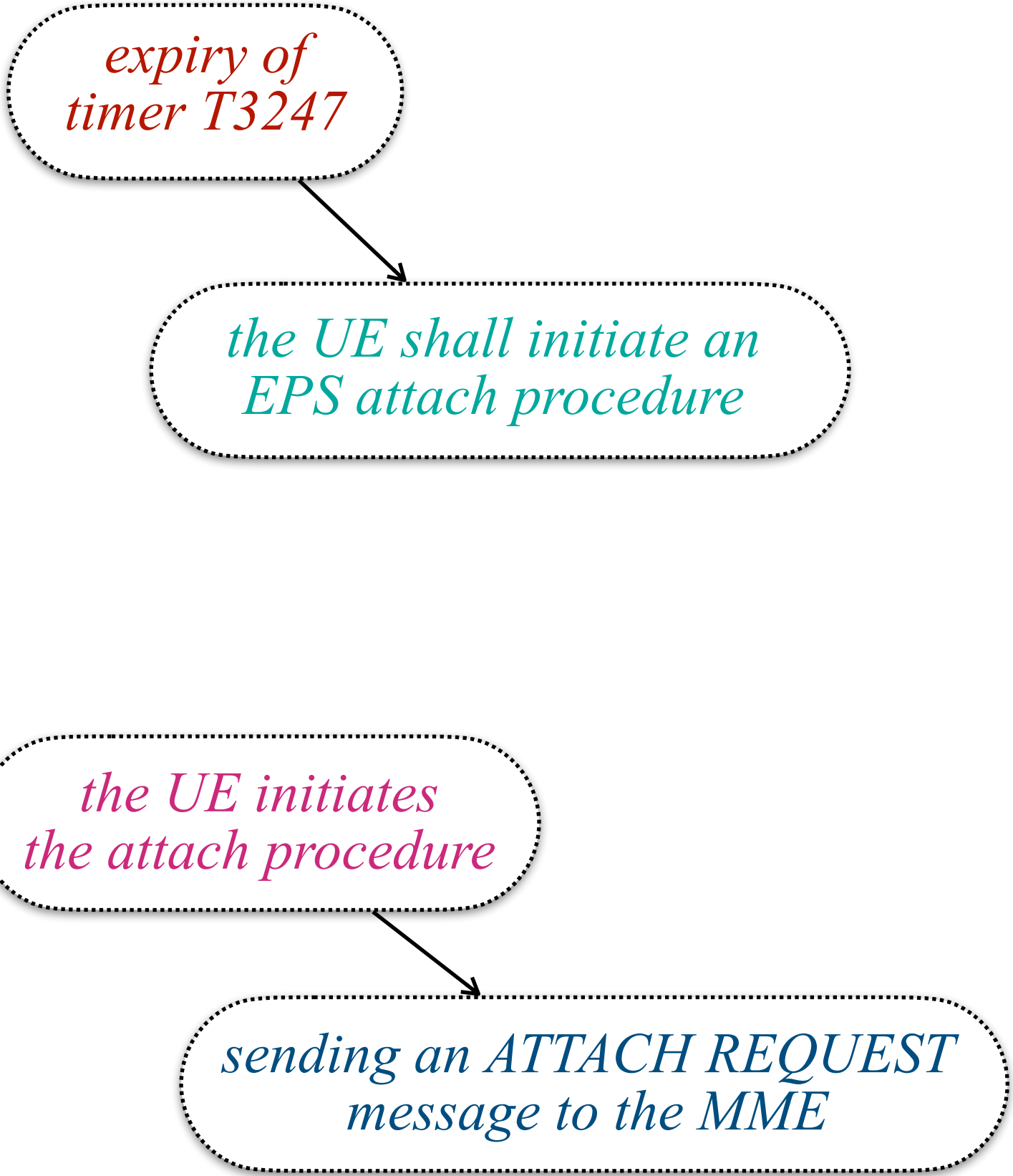*the UE initiates the attach procedure*

sending an ATTACH REQUEST message to the MME

[TS 24.301]: *Upon expiry of timer T3247, the UE shall initiate an EPS attach procedure.*

Upon expiry of timer T3247	,	*the UE*	*shall*
ARGM-TMP		ARG0	ARGM-MOD

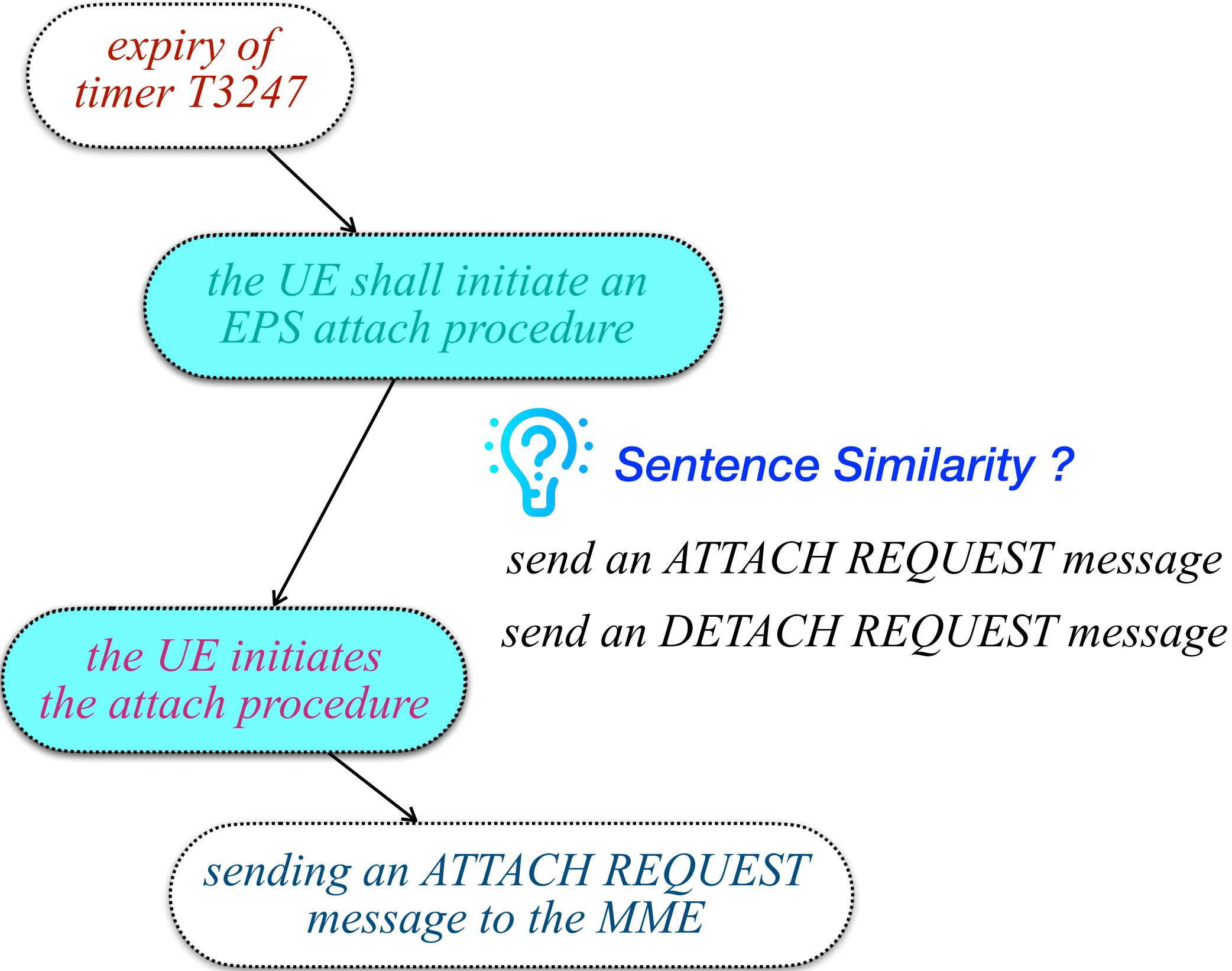| *initiate*	*an EPS attach procedure*	.
V	ARG1	

[TS 24.301]: *the UE initiates the attach procedure by sending an ATTACH REQUEST message to the MME.*

expiry of timer T3247

the UE shall initiate an EPS attach procedure

Sentence Similarity ?
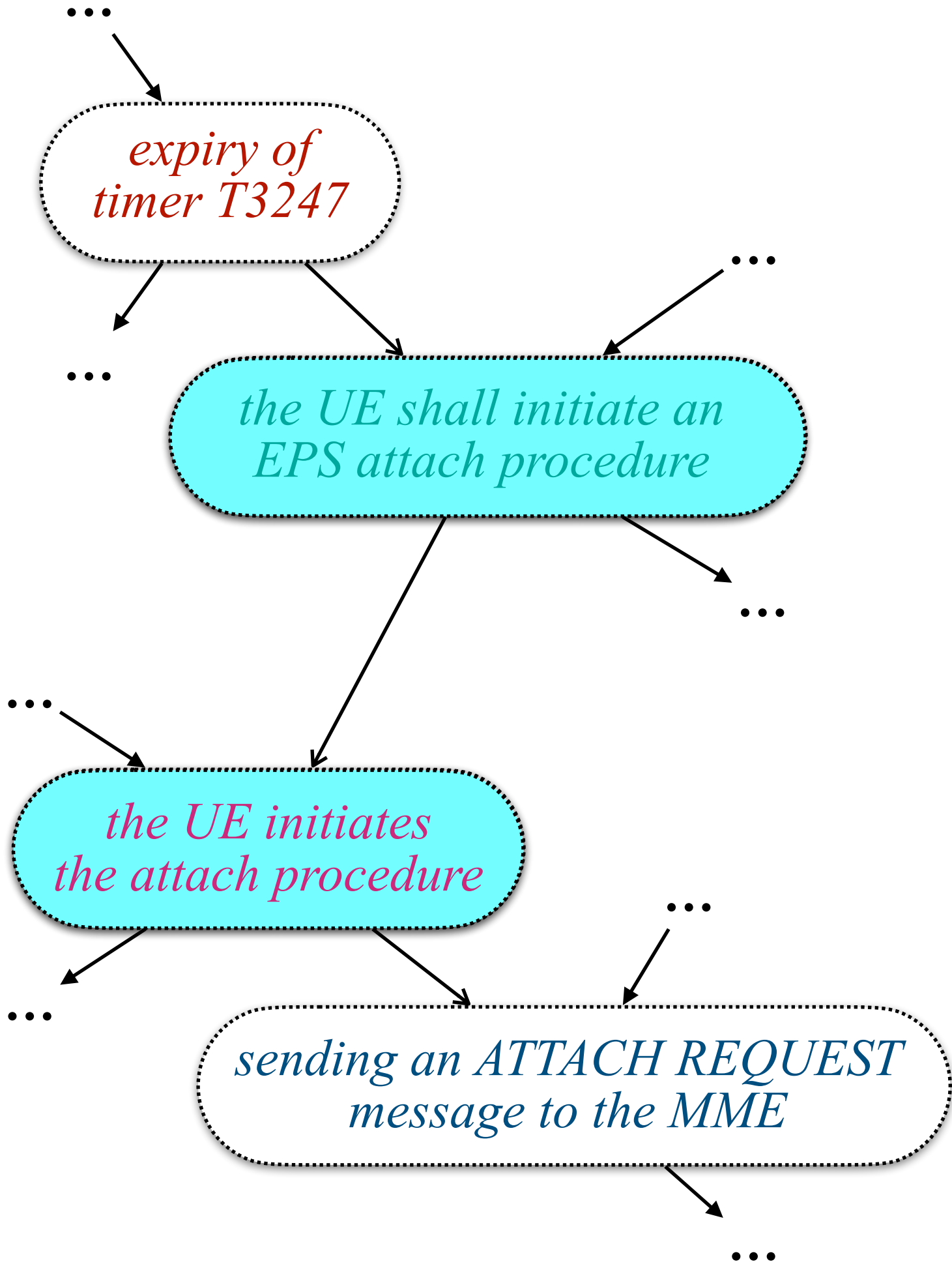
send an ATTACH REQUEST message

send an DETACH REQUEST message

the UE initiates the attach procedure
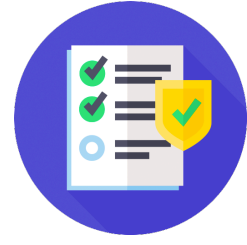
sending an ATTACH REQUEST message to the MME

[TS 24.301]: *Upon expiry of timer T3247, the UE shall initiate an EPS attach procedure.*

Upon expiry of timer T3247	,	*the UE*	*shall*
ARGM-TMP		ARG0	ARGM-MOD

initiate	*an EPS attach procedure*	.
V	ARG1	

[TS 24.301]: *the UE initiates the attach procedure by sending an ATTACH REQUEST message to the MME.*

...

expiry of timer T3247

...

...

the UE shall initiate an EPS attach procedure

...

...

the UE initiates the attach procedure

...

...

sending an ATTACH REQUEST message to the MME

...

22 security requirements

20 mobile phones + 2 IoT devices

iPhone 13 Pro Max, iPhone 13, iPhone 12 Pro, iPhone 11, iPhone 6

Pixel 5a, Pixel 3, Pixel 2, Nexus 6P, Nexus 6, Nexus 4

Honor 30S, Honor 6X, Honor Play20

Redmi K30i, Redmi Note2, Xiaomi MIX 2S

Galaxy A71 5G, Galaxy S10
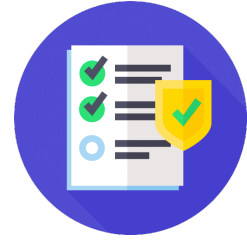
Realme GT

Huawei E3276 USB Dongle

SINELINK MF782 USB Dongle

197 Security Violations
(190 New)

22 security requirements

20 mobile phones + 2 IoT devices

iPhone 13 Pro Max, iPhone 13, iPhone 12 Pro, iPhone 11, iPhone 6

Pixel 5a, Pixel 3, Pixel 2, Nexus 6P, Nexus 6, Nexus 4

Honor 30S, Honor 6X, Honor Play20

Redmi K30i, Redmi Note2, Xiaomi MIX 2S

Galaxy A71 5G, Galaxy S10

Realme GT

Huawei E3276 USB Dongle

SINELINK MF782 USB Dongle

https://sites.google.com/view/contester

197 Security Violations
(190 New)

3GPP