



فصل سوم: بررسی یک روپه در شیله

ابوالفضل دیانت

آخرین ویرایش: ۲۲ آبان ۱۴۰۱ در ساعت ۱۶ و ۴ دقیقه - نسخه ۰.۱

فهرست مطالب

۱	برقراری یک تماس
۲۰	رویه انتخاب سلول و بازانتخاب سلول
۵۱	رویه بروزرسانی منطقه مکانی
۵۷	رویه دسترسی تصادفی
۶۵	رویه شناسایی
۶۹	امنیت در شبکه‌های تلفن همراه
۷۴	ASN.1

۹۶	پشته پروتکلی در RAN
۱۱۴	مراجع
۱۱۶	فهرست اختصارات
۱۳۱	واژه نامه انگلیسی به فارسی
۱۴۰	واژه نامه فارسی به انگلیسی

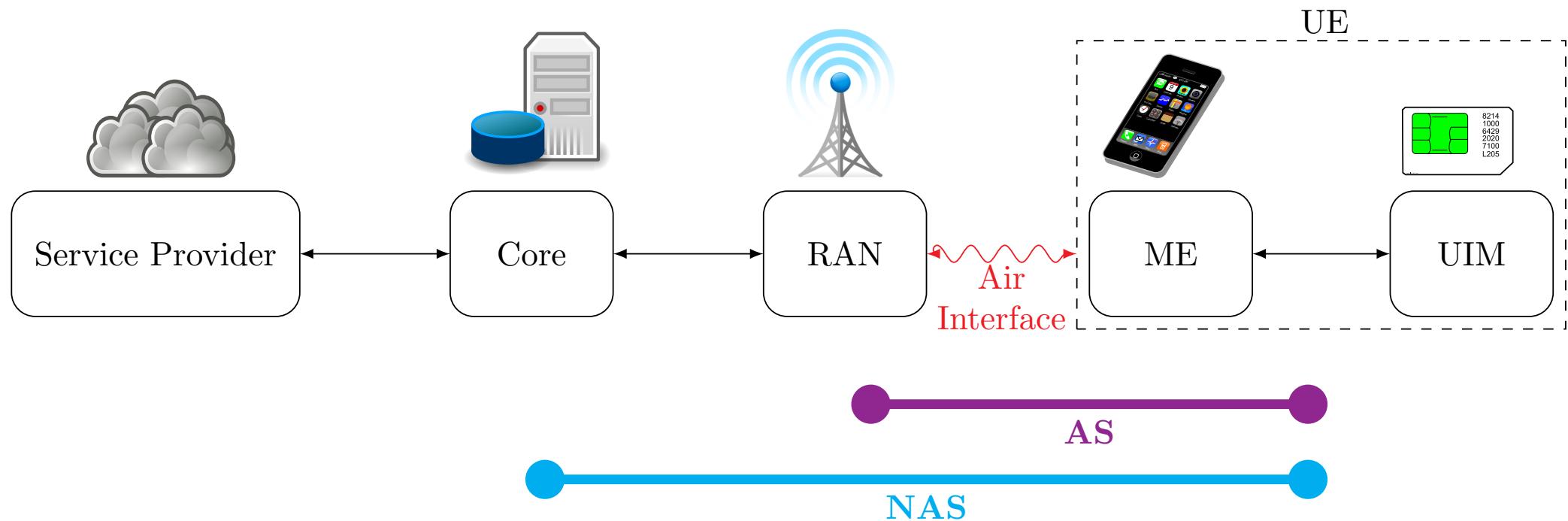
پُر قراری پک نماس



©Elephants on the Wall

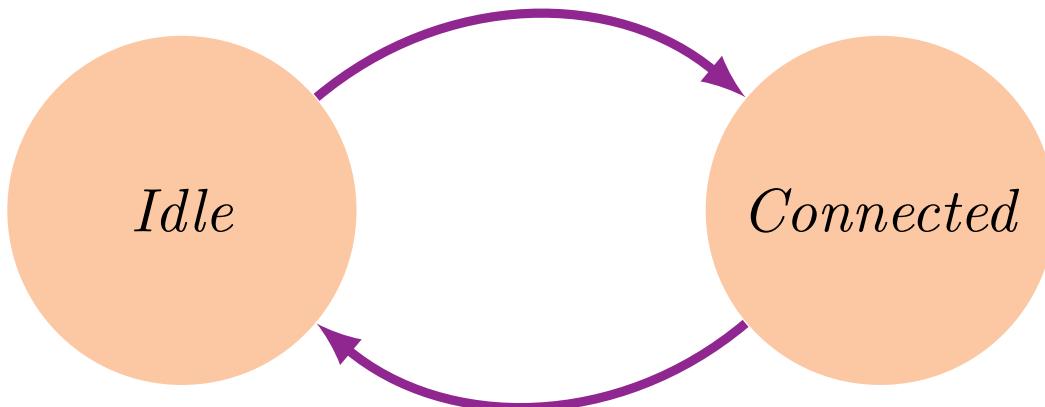
من می خواهم یک تماس تلفنی از طریق یک شبکه تلفن همراه برقرار کنم؟!

NAS (Non Access Stratum) و AS (Access Stratum)



AS: داده‌های این سطح به Radio Access Network (RAN) ختم می‌شود.
NAS (Non Access Stratum) نسبت به داده‌های این سطح شفاف (Transparent) است.

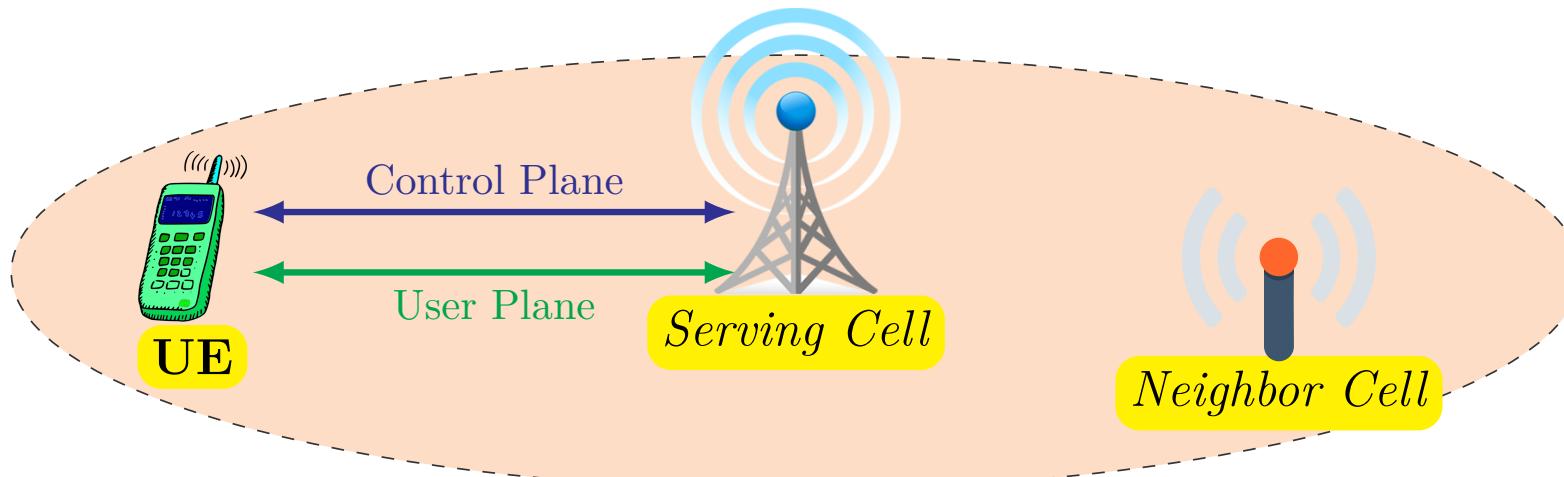
ماشین حالت (State Machine) برای UE



همواره بین مُد بیکار (Connected Mode) و مُد متصل (Idle Mode) در حال گذار است.

در هر حالت UE رویه‌های خاصی را انجام می‌دهد. اما در مُد بیکار چرا؟

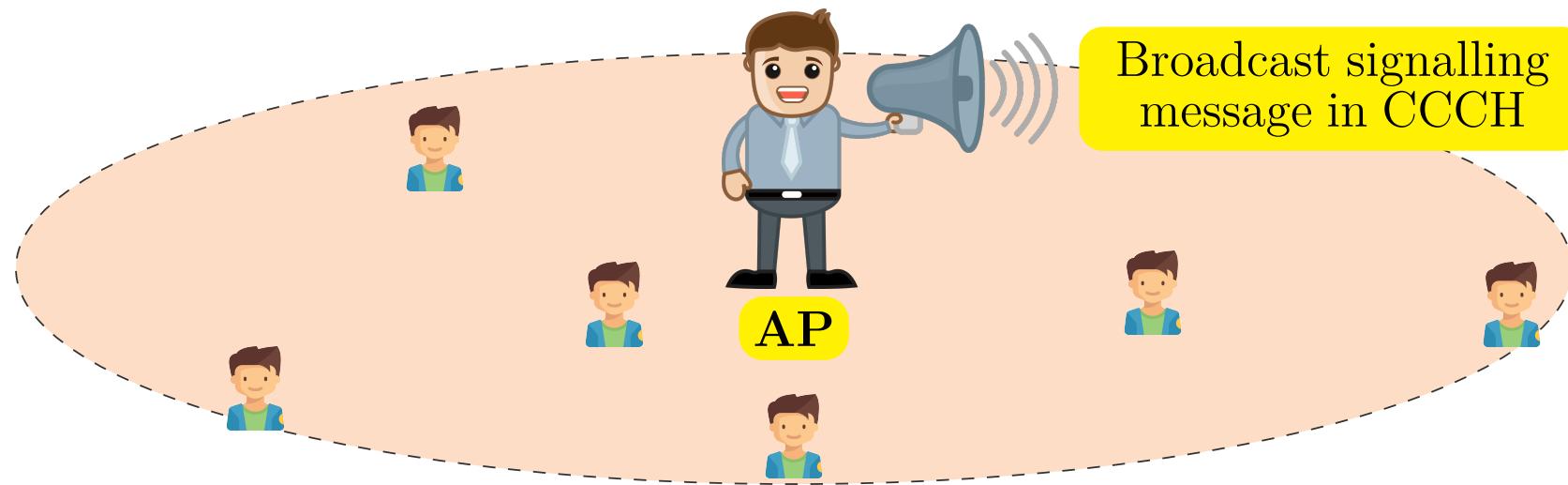
سطح کنترلی (User Plane) و سطح کاربر (Control Plane)



سطح کاربر یا همان ترافیک کاربر : جلوگیری از داده های کاربر به مانند انتقال صوت، کاربردهای چند رسانه ای، خدمات اینترنت.

سطح کنترلی یا سیگنال دهنده : فرایند کنترل ارتباطات (مشتمل بر برقراری تماس، نگهداری تماس و آزادسازی تماس)، کنترل امنیتی، کیفیت خدمت، محاسبه هزینه ها، مدیریت حرکت پذیری (Mobility Management) کاربران و کنترل منابع رادیویی.

کانال‌های کنترلی - کانال‌های کنترلی عمومی (Common Control Channel)



کانال‌های کنترلی عمومی، کانال‌هایی هستند که بین همه کاربران به اشتراک گذاشته می‌شوند.

CCCH (Common Control Channel) به مانند:

- کanal (BCCH - Broadcast Control Channel)

- کanal (PCCH - Paging Control Channel)

کانال (Broadcast Control Channel) BCCH

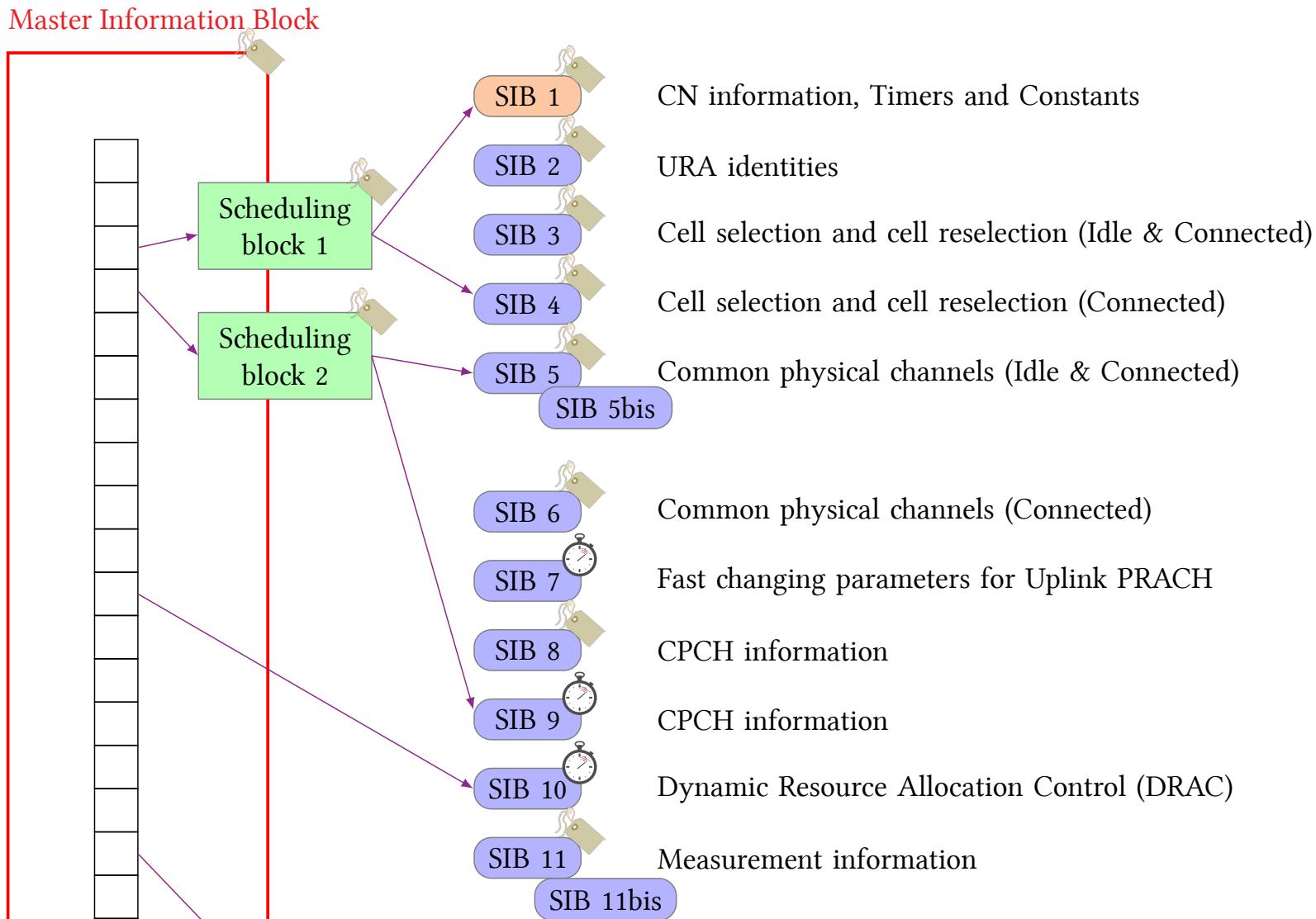
کانال (BCCH) یک کانال کنترلی عمومی برای پیوند فروسو است که توسط آن اطلاعات سامانه (System Information) ارسال می‌گردد.

(Transmitted به مانند: شناسه Public Land Mobile Network (PLMN)، شناسه سلول، توان ارسالی و اطلاعات لازم برای کمک به UE برای اتصال به شبکه.)

اطلاعات سامانه تحت قالب‌هایی به نام SIB (System Information Block) ارسال می‌گردد.

MIB	SIB1	SIB2	SIB3	SIB4	SIB5	SIB6	SIB7	SIB8
SIB9	SIB10	SIB11	SIB12	SIB13	SIB14	SIB15	SIB16	SIB17
SIB18	SB1	SB2						

کانال BCCH (Broadcast Control Channel) (ادامه)



کانال BCCH (Broadcast Control Channel) (ادامه)

2022-04-02 16:51:29.917	2329	3G	▲	RRC	UL DCCH	Physical Channel Reconfiguration Complete	1078
2022-04-02 16:51:28.885	2329	3G	▲	RRC	UL DCCH	Physical Channel Reconfiguration	1078
2022-04-02 16:51:28.881	2329	3G	▲	RRC	UL DCCH	Radio Bearer Reconfiguration Complete	1078
2022-04-02 16:51:28.878	2329	3G	▼	RRC	DL DCCH	UTRAN Mobility Information Confirm	1078
2022-04-02 16:51:28.878	2329	3G	▼	RRC	DL DCCH	Cell Update Confirm	1078
2022-04-02 16:51:28.672	2329	3G	▲	RRC	UL CCCH	Cell Update	1078
2022-04-02 16:51:28.662	2329	3G	▼	RRC	COMPLETE SIB	SIB ExtensionType	1078
2022-04-02 16:51:28.660	2329	3G	▼	RRC	COMPLETE SIB	SIB 12	1078
2022-04-02 16:51:28.657	2329	3G	▼	RRC	COMPLETE SIB	SIB 11	1078
2022-04-02 16:51:28.655	2329	3G	▼	RRC	COMPLETE SIB	SIB 5	1078
2022-04-02 16:51:28.652	2329	3G	▼	RRC	COMPLETE SIB	SIB 3	1078
2022-04-02 16:51:28.650	2329	3G	▼	RRC	COMPLETE SIB	SIB 1	1078
2022-04-02 16:51:28.647	2329	3G	▼	RRC	COMPLETE SIB	SB 2	1078
2022-04-02 16:51:28.644	2329	3G	▼	RRC	COMPLETE SIB	MIB	1078
2022-04-02 16:51:28.229	2329	3G	▼	RRC	DL DCCH	Radio Bearer Reconfiguration	1078
2022-04-02 16:51:24.438	2329	3G	▲	RRC	UL DCCH	Uplink Direct Transfer	1078
2022-04-02 16:51:24.422	2329	3G	▲	NAS	GPRS SM	Modify PDP Context Accept M2N	1078
2022-04-02 16:51:24.418	2329	3G	▼	NAS	GPRS SM	Modify PDP Context Request N2M	1078
2022-04-02 16:51:24.415	2329	3G	▼	RRC	DL DCCH	Downlink Direct Transfer	1078
2022-04-02 16:51:24.413	2329	3G	▲	RRC	UL DCCH	Radio Bearer Reconfiguration Complete	1078
2022-04-02 16:51:24.406	2329	3G	▼	RRC	DL DCCH	Radio Bearer Reconfiguration	1078
2022-04-02 16:51:23.979	2329	3G	▲	RRC	UL DCCH	Radio Bearer Setup Complete	1078
2022-04-02 16:51:03.250	2329	3G	▲	RRC	UL DCCH	Measurement Report	1078

MasterInformationBlock
 mib-ValueTag: 8
 plmn-Type: gsm-MAP (0)
 gsm-MAP
 plmn-Identity
 mcc: 3 items
 Item 0
 Digit: 4
 Item 1
 Digit: 3
 Item 2
 Digit: 2
 mnc: 2 items
 Item 0
 Digit: 1
 Item 1
 Digit: 1
 Mobile Country Code (MCC): Iran (Islamic Republic of) (432)
 Mobile Network Code (MNC): Telecommunication Company of Iran (TCI) (11)
sibSb-ReferenceList: 5 items
 Item 0
 SchedulingInformationSIBSb
 sibSb-Type: sysInfoTypeSB1 (21)
 sysInfoTypeSB1: 1
 scheduling
 scheduling
 sib-Pos: rep128 (5)
 rep128: 63
 Item 1
 SchedulingInformationSIBSb
 sibSb-Type: sysInfoType1 (0)
 sysInfoType1: 14
 scheduling
 scheduling
 sib-Pos: rep32 (3)
 rep32: 2
 Item 2
 SchedulingInformationSIBSb
 sibSb-Type: sysInfoType3 (2)
 sysInfoType3: 3
 scheduling
 scheduling
 sib-Pos: rep16 (2)
 rep16: 1

کانال BCCH (Broadcast Control Channel) (ادامه)

Timestamp	N	T	D	C	Type	Name	A
2022-03-04 22:18:03.227	2320	4G	▲	RRC	UL DCCH	Measurement Report	33
2022-03-04 22:18:03.227	2320	4G	▲	RRC	UL DCCH	Measurement Report	33
2022-03-04 22:18:03.221	2320	4G	▲	RRC	UL DCCH	RRC Connection Reconfiguration Complete	33
2022-03-04 22:18:03.219	2320	4G	▼	RRC	DL DCCH	RRC Connection Reconfiguration	33
2022-03-04 22:18:03.179	2320	4G	▲	RRC	UL DCCH	RRC Connection Reconfiguration Complete	33
2022-03-04 22:18:03.175	2320	4G	▼	RRC	DL DCCH	RRC Connection Reconfiguration	33
2022-03-04 22:18:03.162	2320	4G	▼	RRC	BCCH_SCH	System Information	33
2022-03-04 22:18:03.139	2320	4G	▲	RRC	UL DCCH	RRC Connection Reconfiguration Complete	33
2022-03-04 22:18:03.134	2320	4G	▼	RRC	DL DCCH	RRC Connection Reconfiguration	33
2022-03-04 22:18:03.122	2320	4G	▼	RRC	BCCH_SCH	System Information	33
2022-03-04 22:18:03.102	2320	4G	▲	RRC	UL DCCH	RRC Connection Reconfiguration Complete	33
2022-03-04 22:18:03.099	2320	4G	▼	RRC	DL DCCH	RRC Connection Reconfiguration	33
2022-03-04 22:18:03.086	2320	4G	▼	RRC	BCCH_BCH	MIB	33
2022-03-04 22:18:03.085	2320	4G	▼	RRC	BCCH_SCH	SIB 1	33
2022-03-04 22:18:03.050	2320	4G	▲	RRC	UL DCCH	RRC Connection Reconfiguration Complete	33
2022-03-04 22:18:03.023	2320	4G	▼	RRC	DL DCCH	RRC Connection Reconfiguration	33
2022-03-04 22:18:02.990	2320	4G	▲	RRC	UL DCCH	Measurement Report	33
2022-03-04 22:18:01.230	2320	4G	▲	RRC	UL DCCH	Measurement Report	33
2022-03-04 22:18:00.910	2320	4G	▲	RRC	UL DCCH	Measurement Report	33
2022-03-04 22:18:00.470	2320	4G	▲	RRC	UL DCCH	Measurement Report	33
2022-03-04 22:17:59.910	2320	4G	▲	RRC	UL DCCH	Measurement Report	33
2022-03-04 22:17:57.630	2320	4G	▲	RRC	UL DCCH	Measurement Report	33
2022-03-04 22:17:57.230	2320	4G	▲	RRC	UL DCCH	Measurement Report	33
2022-03-04 22:17:56.990	2320	4G	▲	RRC	UL DCCH	Measurement Report	33
2022-03-04 22:17:56.670	2320	4G	▲	RRC	UL DCCH	Measurement Report	33
2022-03-04 22:17:56.510	2320	4G	▲	RRC	UL DCCH	Measurement Report	33

Text Find

```
6050C823A0FE1612D018235184420411310C9B400000
DLT: 148, Payload: aww (Automator Wireshark Wrapper)
Automator Wireshark Wrapper
Protocol: 103
Data length: 22
BCCH-DL-SCH-Message
message: c1 (0)
  c1: systemInformationBlockType1 (1)
    systemInformationBlockType1
    cellAccessRelatedInfo
    plmn-IdentityList: 1 item
      Item 0
        PLMN-IdentityInfo
        plmn-Identity
        mcc: 3 items
          Item 0
            MCC-MNC-Digit: 4
          Item 1
            MCC-MNC-Digit: 3
          Item 2
            MCC-MNC-Digit: 2
        mnc: 2 items
          Item 0
            MCC-MNC-Digit: 1
          Item 1
            MCC-MNC-Digit: 1
        cellReservedForOperatorUse: notReserved (1)
        trackingAreaCode: a0fe [bit length 16, 1010 0000 1111 1110 decimal value 41214]
        cellIdentity: 1612d010 [bit length 28, 4 LSB pad bits, 0001 0110 0001 0010 1101 0000 0001 ....
decimal value 23145729]
        cellBarred: notBarred (1)
        intraFreqReselection: allowed (0)
        ... .0. csq-Indication: False
        cellSelectionInfo
        q-RxLevMin: -124dBm (-62)
        p-Max: 23 dBm
        freqBandIndicator: 7
        schedulingInfoList: 3 items
          Item 0
            SchedulingInfo
            si-Periodicity: rf16 (1)
            sib-MappingInfo: 1 item
              Item 0
                SIB-Type: sibType3 (0)
          Item 1
            SchedulingInfo
            si-Periodicity: rf32 (2)
            sib-MappingInfo: 1 item
              Item 0
                SIB-Type: sibType5 (2)
```

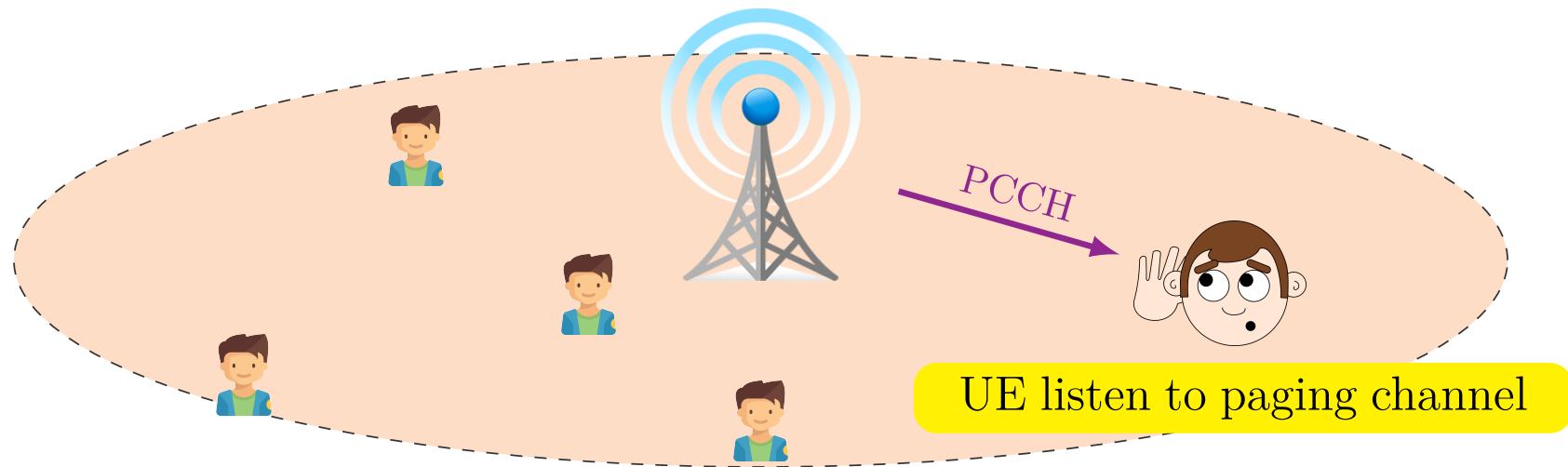
اطلاعات سامانه (System Information)، داده‌های کنترلی هستند که توسط هسته شبکه و یا RAN تولید گشته و در هر سلوول به صورت همه‌پخشی (Broadcast) ارسال می‌گردد. این اطلاعات به UE کمک می‌کند، تا بتواند پارامترهای لازم به منظور اتصال به RAN و هسته شبکه را بدست آورد. اطلاعات سامانه در واقع مجموعه‌ای از عناصر اطلاعات (Information Element) هستند. عناصر اطلاعات از یک نوع معمولاً در کنار هم‌دیگر، در قالب‌هایی به نام System Information Block (SIB) منتشر می‌گردند.

مثال ۱ به عنوان نمونه UE از SIB3، پارامترهای مورد نیاز برای اجرای رویه‌های انتخاب سلوول (Cell Selection) و بازانتخاب سلوول (Cell Reselection) در مُد بیکار را استخراج می‌نماید.

در Long Term Evolution (LTE) و Universal Mobile Telecommunications System (UMTS) قالبی به نام Master Information Block (MIB)، نحوه زمان‌بندی SIB‌ها را معین می‌سازد و همچنین وظیفه اطلاع‌رسانی از تغییر آن‌ها را نیز بر عهده دارد. قالب‌هایی به نام بلوک زمان‌بندی به صورت اختیاری می‌تواند ارسال گردد تا

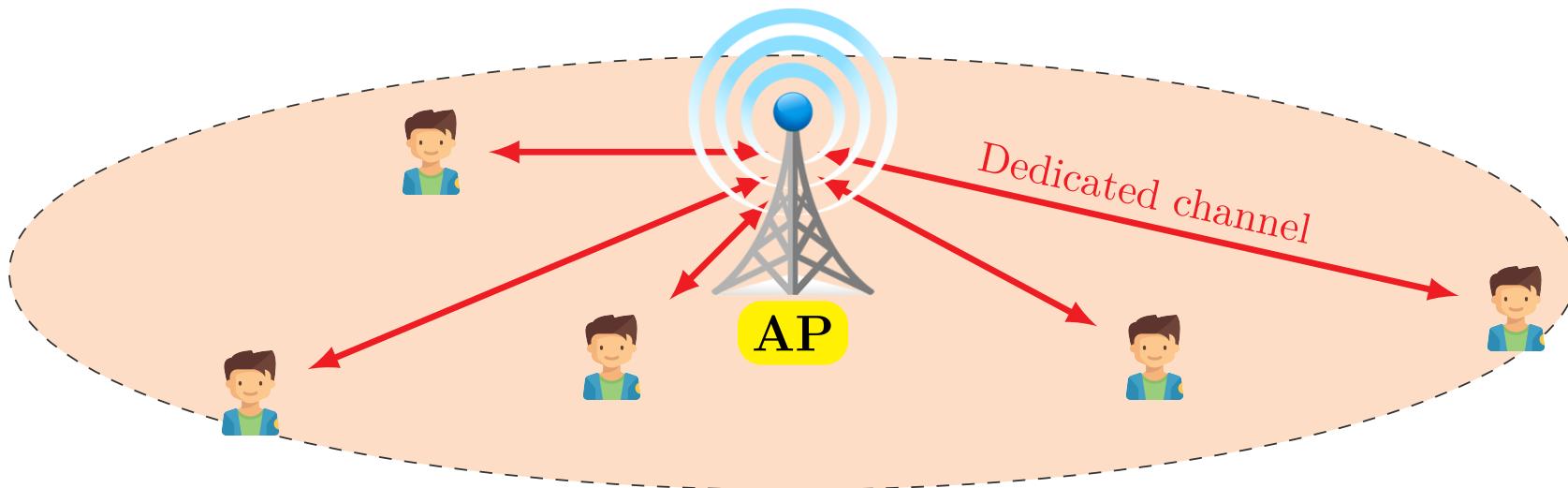
کمک کار MIB در زمان بندی SIB ها باشد.

کانال PCCH (Paging Control Channel)

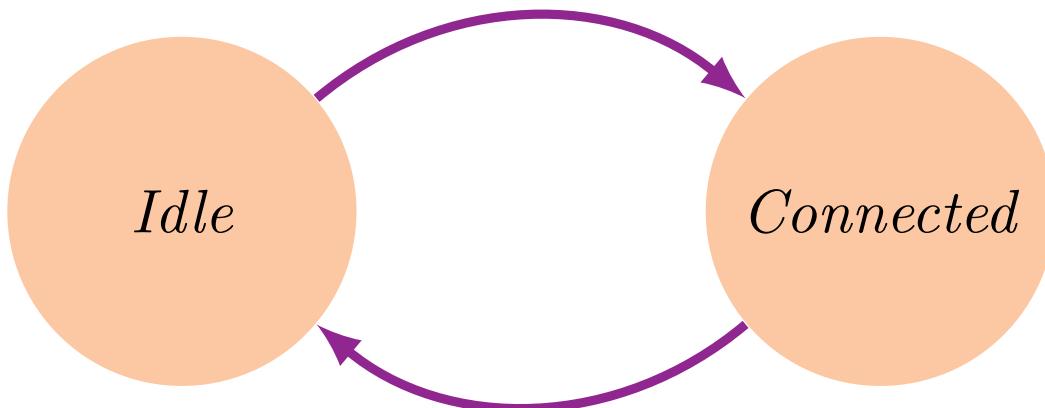


- UE نقش مشتری (Client) را برای شبکه ایفا می‌کند. پس او باید شروع کننده ارتباط باشد.
- UE می‌بایست به طور مداوم به کانال Paging Control Channel (PCCH) گوش دهد.

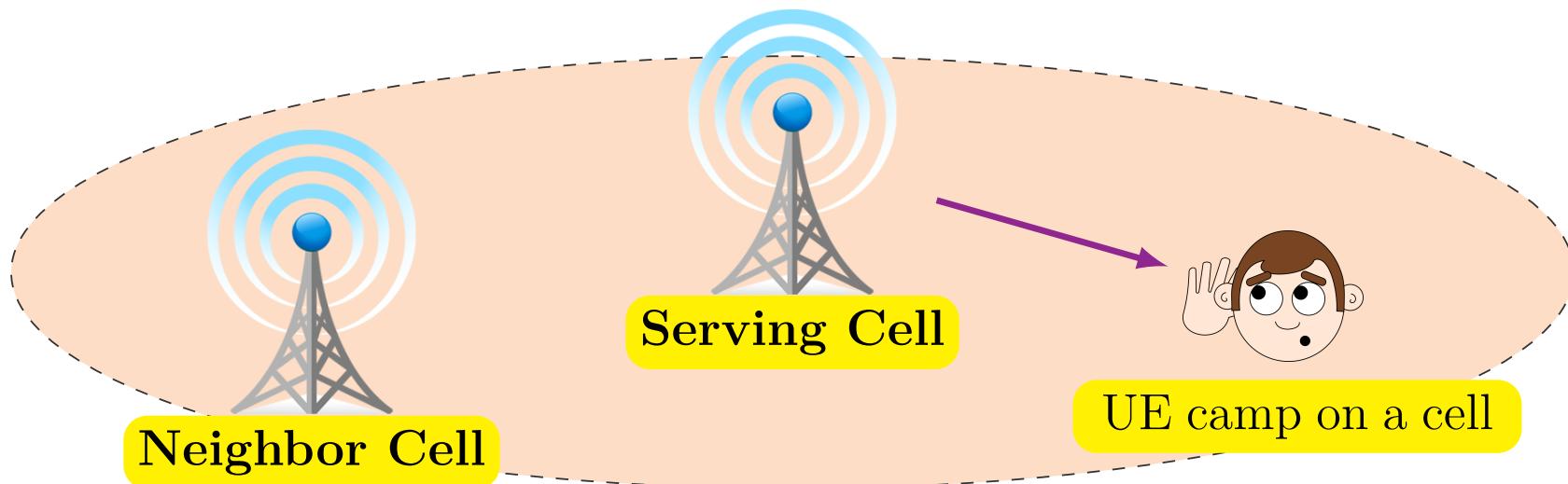
کانال‌های کنترلی - کانال‌های اختصاصی (Dedicated Channel)



- ☞ کانال‌های اختصاصی (Dedicated Channel)، کانال‌هایی هستند که تنها به یک کاربر تخصیص داده شده، و در آن تنها سیگنال‌دهی (Signalling) مخصوص به آن کاربر منتقل می‌شود.
- ☞ در صورت نیاز کانال اختصاصی به کاربر تخصیص داده شده و سپس از او گرفته می‌شود؟!



- دو حالت برای UE می‌توان متصور بود: مُد بیکار (Idle Mode) و مُد متصل (Connected Mode).
- به UE در مُد متصل، کanal اختصاصی (Dedicated Channel) تخصیص می‌یابد.
- UE در مُد بیکار تنها می‌تواند به کانال‌های کنترلی عمومی گوش دهد.

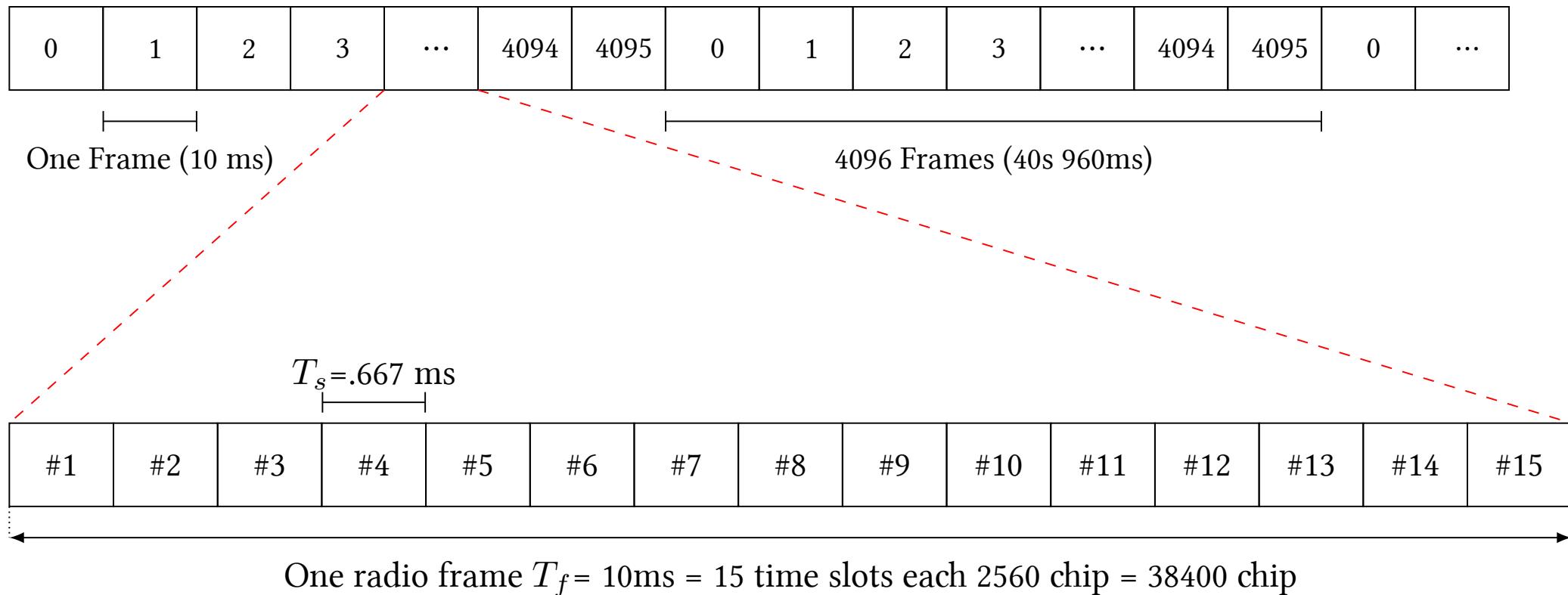


UE حتی در مُد بیکار (Idle Mode)، بر روی سلول خدمتگزار (Serving Cell) شبکه اردو زده است.

- باید با سلول خدمتگزار هم‌مان باشد (فرکانس و زمان).
- به پیام‌های رسیده در کanal کنترلی عمومی (Common Control Channel) گوش می‌دهد،
- توان دریافتی (Received Power) از سلول خدمتگزار (Serving Cell) را اندازه‌گیری می‌کند.
- توان دریافتی از سلول‌های همسایه را اندازه‌گیری می‌کند.

سلول خدمتگزار و سلول های همسایه (ادامه)

حوزه زمان از دیدگاه شبکه به قاب (Time Slot) و شیار زمانی (Frame) تقسیم‌بندی می‌گردد.



توان دریافتی از سلول خدمتگزار

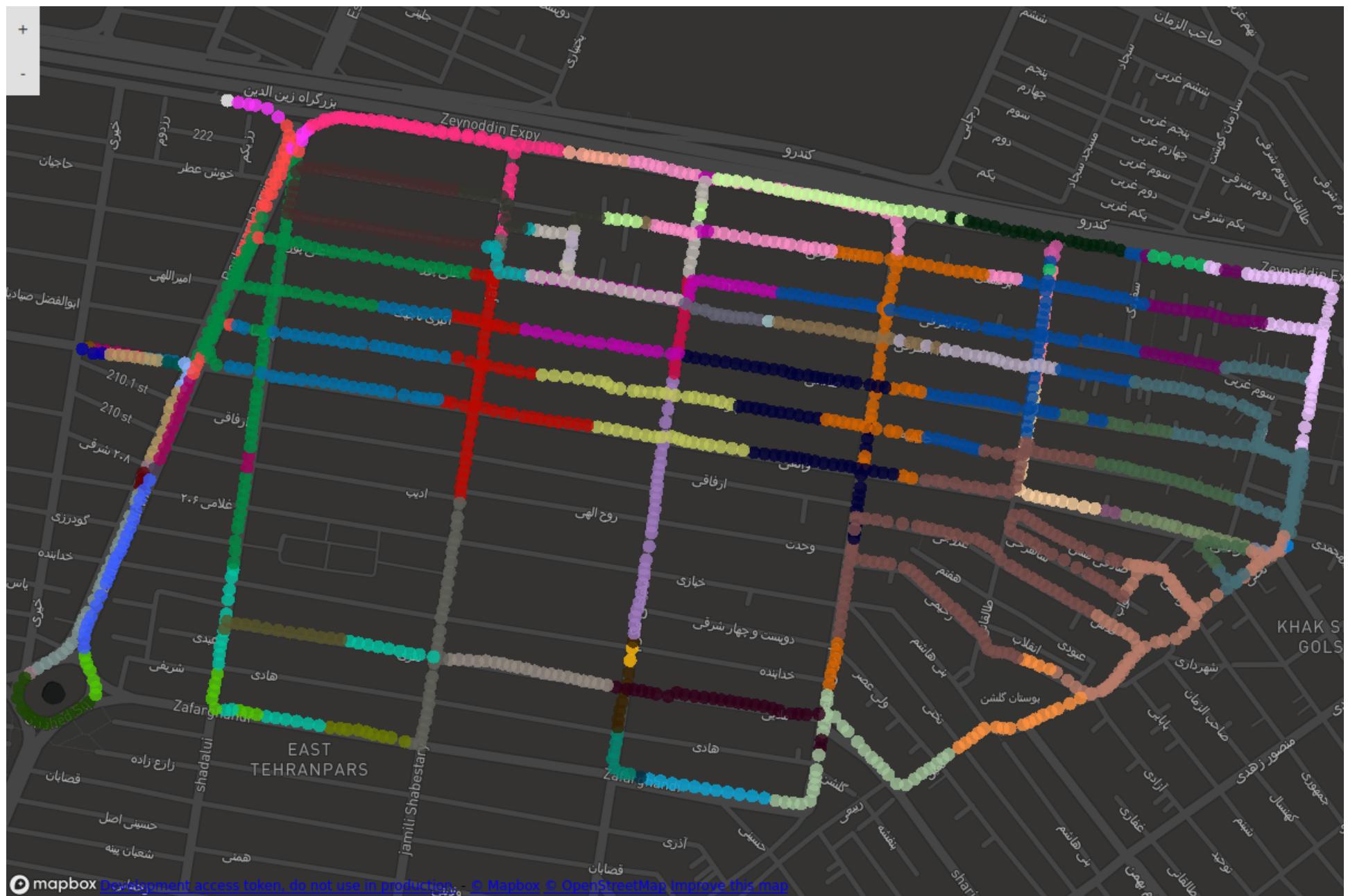


توان دریافتی از سلول همسایه



روپہ انتخاب سلوں و بازنگانیاں

تغییر سلول خدمتگزار در یک مسیر



رویه انتخاب سلول (Cell Selection) و بازانتخاب سلول (Cell Reselection)

در صورتی که گوشی روشن باشد (حتی اگر سیم کارت درون آن نباشد)، به صورت مداوم دو عملیات انتخاب سلول و بازانتخاب سلول اتفاق می‌افتد. تفاوت این دو؟!

UE در روش انتخاب سلول در تلاش است تا به یک سلول مناسب (Suitable Cell) متصل گردد.

گوشی تلاش می‌کند تا به سلول مناسب بهتری متصل شود (رویه بازانتخاب سلول).

نکته ۱ چرا که UE تنها از یک سلول مناسب، می‌تواند خدمات بهنجهار (Normal Service) شبکه را دریافت نماید.

رویه انتخاب سلول و بازانتخاب سلول (ادامه)

شرط سلول مناسب (Suitable Cell):

- سلول مسدودشده نباشد.
- سلول باید عضوی از شبکه انتخاب شده، شبکه ثبت شده و یا شبکه معادل باشد.
- سلول قیدی به نام S را برآورده سازد.
- منطقه مکانی سلول، جزو فهرست Forbidden LAs for roaming نباشد.

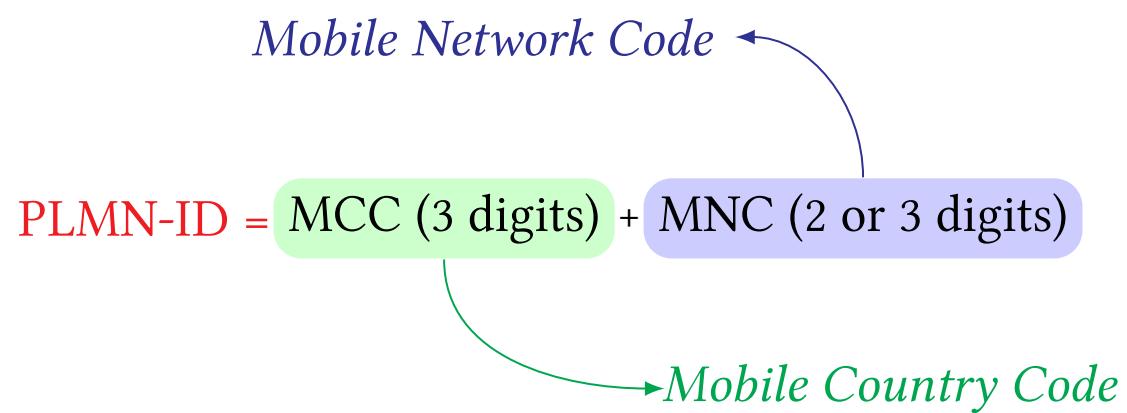
شروط سلول مناسب - سلول مسدودشده (Barred Cell) - سلول مناسب

UE می‌بایست به سراغ بازگشایی اطلاعات UMTS SIB3/4 و LTE SIB1 برود. در آن‌جا پارامتری به نام CellBarred وجود دارد که مسدود بودن و یا نبودن سلول را نشان می‌دهد.

▲	RRC	UL DCCH	Measurement Report
▲	RRC	UL DCCH	Measurement Report
▲	RRC	UL DCCH	Measurement Report
▲	RRC	UL DCCH	Measurement Report
▲	RRC	UL DCCH	Measurement Report
▲	RRC	UL DCCH	Measurement Report
▼	RRC	BCCH_BCH	MIB
▼	RRC	BCCH_SCH	SIB 1
▲	RRC	UL DCCH	Measurement Report
▲	RRC	UL DCCH	Measurement Report
▼	RRC	BCCH_SCH	System Information
▼	RRC	BCCH_BCH	MIB
▼	RRC	BCCH_SCH	System Information
▼	RRC	BCCH_SCH	SIB 1
▼	RRC	BCCH_SCH	SIB 1
▼	RRC	BCCH_SCH	System Information

```
c1: systemInformationBlockType1 (1)
    systemInformationBlockType1
        cellAccessRelatedInfo
            plmn-IdentityList: 1 item
                Item 0
                    PLMN-IdentityInfo
                        plmn-Identity
                            mcc: 3 items
                                Item 0
                                    MCC-MNC-Digit: 4
                                Item 1
                                    MCC-MNC-Digit: 3
                                Item 2
                                    MCC-MNC-Digit: 2
                            mnc: 2 items
                                Item 0
                                    MCC-MNC-Digit: 1
                                Item 1
                                    MCC-MNC-Digit: 1
            cellReservedForOperatorUse: notReserved (1)
            trackingAreaCode: b09e [bit length 16, 1011 0000 1001 1110 de]
            cellIdentity: 162be010 [bit length 28, 4 LSB pad bits, 0001 0110
                cellBarred: notBarred (1)
                intraFreqReselection: allowed (0)
                    .... ..0. csg-Indication: False
            cellSelectionInfo
                q-RxLevMin: -124dBm (-62)
                p-Max: 23 dBm
                freqBandIndicator: 7
                schedulingInfoList: 3 items
                    Item 0
```

PLMN در حقیقت یک شبکه تلفن همراه است که شامل یک شبکه دسترسی و یک هسته شبکه است. PLMN در اطلاعات SIB ارسال می‌گردد.



- 0: Test networks
- 2: Europe
- 3: North America and the Caribbean
- 4: Asia and the Middle East
- 5: Australia and Oceania
- 6: Africa
- 7: South and Central America
- 9: Worldwide

PLMN‌ای است که کاربر سیم‌کارت خود را از آن خریداری کرده است.

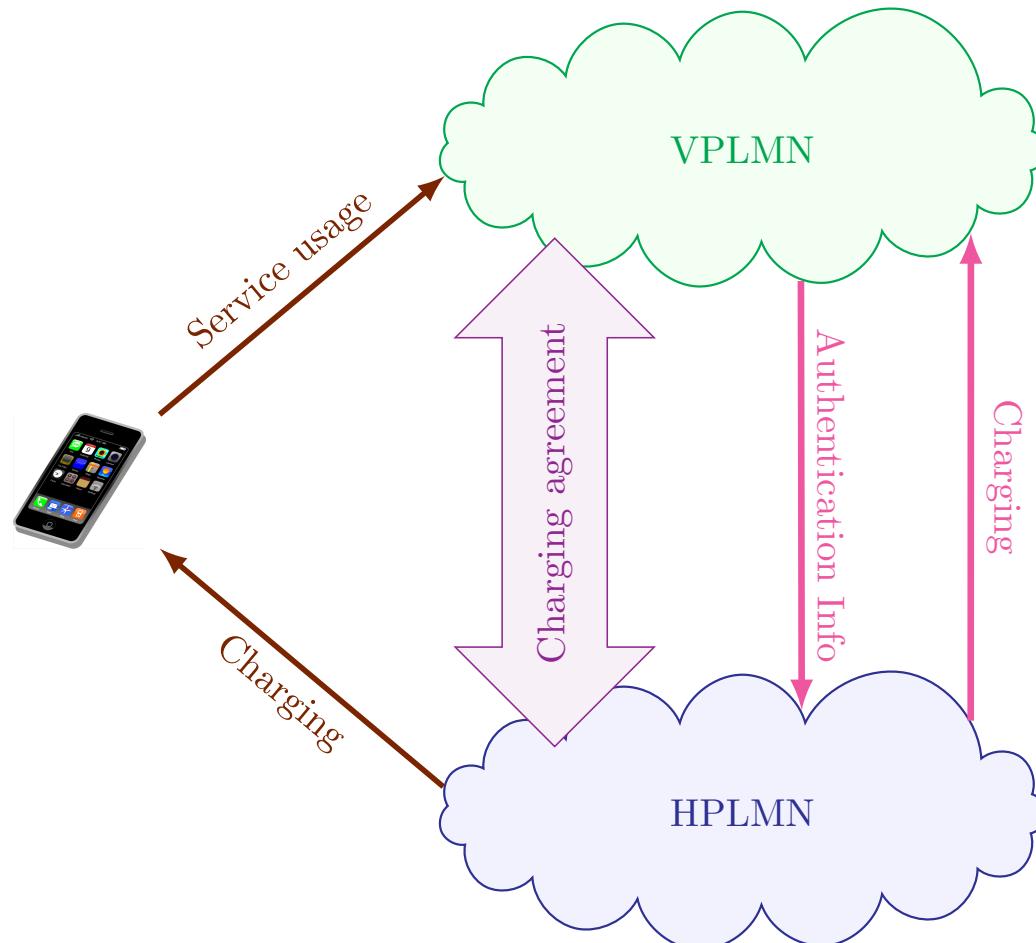
Home PLMN کاربر بیانگر شناسه International Mobile Subscriber Identity (IMSI) نخستین ارقام  است.

(HPLMN) است.

 اطلاعات کاربر در هنگام اجرای رویه‌هایی به مانند فراگردی از HPLMN گرفته می‌شود.

VPLMN

- VPLMN ای است متفاوت از HPLMN که UE اجازه فراگردی به آن را دارد.
- UE در صورت نبودن در پوشش Visited PLMN (VPLMN) به سراغ HPLMN می‌رود.



بیانگر شبکه‌هایی است که UE نمی‌تواند به آن‌ها فراگردی کند. FPLMN (ForbiddenPLMN) 

این لیست درون Universal Integrated Circuit Card (UIICC) ذخیره می‌شود. 

آخرین PLMN ای است که UE در آن با موفقیت ثبت شده است.

UE هنگامی در یک PLMN با موفقیت ثبت می‌گردد که اولاً یک سلول مناسب از آن PLMN بیابد و بر روی

آن اردو بزند، ثانیاً PLMN مذکور در خواست Location Register (LR) او را در این سلول بپذیرد.

VPLMN یا یک HPLMN می‌تواند Registered Public Land Mobile Network (RPLMN) باشد.

به مجموعه‌ای از PLMN ها گفته می‌شود که در رویه‌هایی نظیر انتخاب شبکه، انتخاب سلول، بازانتخاب سلول و واگذاری در یک مرتبه و سطح از اولویت قرار دارند. برای این‌که ذهن خواننده بیش از پیش با فلسفه وجود آشنا گردد، در ادامه مثالی ذکر خواهد شد.

مثال ۲ فرض کنید عملگری دو شبکه یکی (GSM) و دیگری Global System for Mobile Communication (UMTS) را در یک کشور راه‌اندازی کرده است. بنابر برخی دلایل ممکن است این عملگر دو شناسه UMTS مجرا برای این دو شبکه در نظر بگیرد. از سوی دیگر اگر این دو شبکه در دو کشور مختلف باشند، به دلیل تفاوت در Mobile Country Code (MCC) این دو شبکه PLMN کشورها، راه گریزی از تفاوت در شناسه PLMN داشت. اما عملگر مذکور دوست دارد که کاربران، این دو شبکه را در یک سطح اولویت قرار دهند. این مهم را می‌توان توسط EPLMN اجرا نمود.

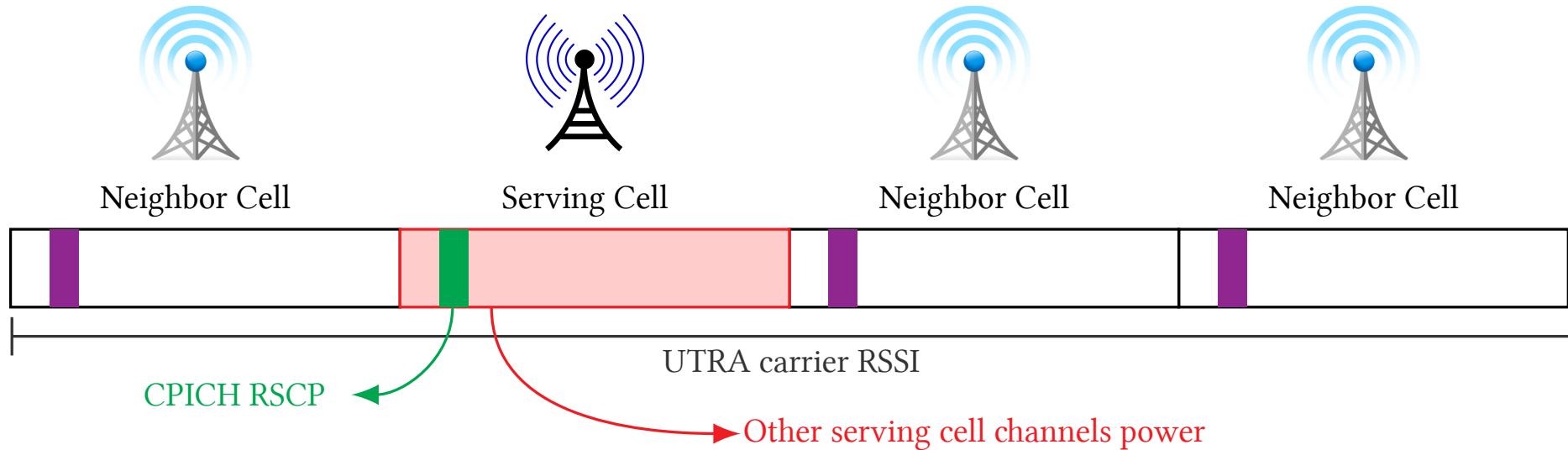
اولویت‌بندی در انتخاب شبکه

UE با توجه به معیارهای مشخصی اولویت‌بندی بر روی PLMN های موجود انجام می‌دهد.

بر طبق [۱]، زیربخش 4.4.3.1.1 PLMN های:

- در صورت عدم وجود فهرست UICC Equivalent HPLMN (EHPLMN)، اولویت نخست با HPLMN است، و در صورت وجود چنین فهرستی، بالاترین PLMN در فهرست EHPLMN در اولویت نخست و مدخل‌های بعدی در اولویت‌های دوم، سوم و ... قرار می‌گیرند.
- بعد از EHPLMN و HPLMN به سراغ فهرستی به نام User controlled PLMN selector می‌رود. هر مدخل از این فهرست شامل شناسه PLMN و فناوری رادیویی برای دسترسی ارجح از دیدگاه کاربر است.

رویه انتخاب سلول و بازانتخاب سلول (ادامه)



$$\text{CPICH Ec/No [dB]} = \text{CPICH RSCP [dBm]} - \text{UTRA carrier RSSI [dBm]}$$

Common Pilot Channel (CPICH)-Received Signal Code Power (RSCP) دو پارامتر UMTS UE

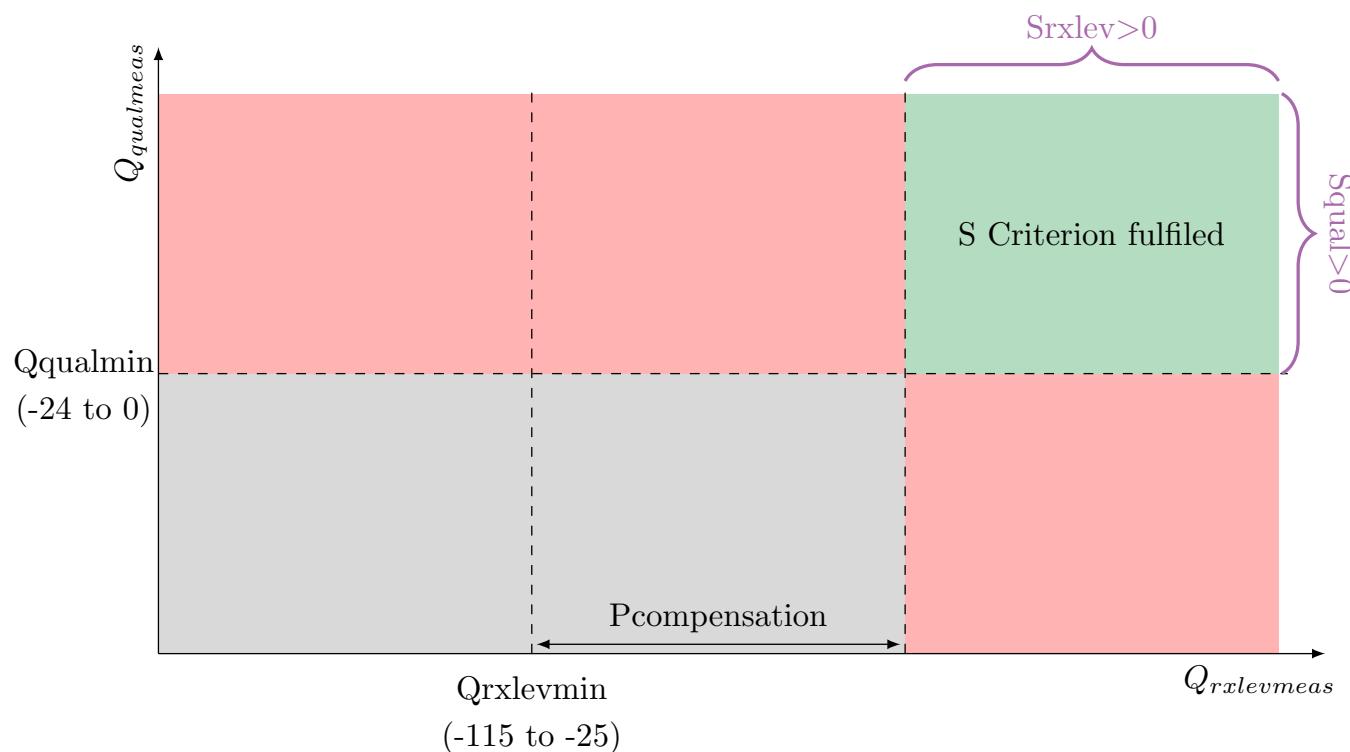
و Ec/N0 از سلول‌های اطراف خود اندازه‌گیری می‌کند، در LTE نیز دو پارامتر

.Reference Signal Received Quality (RSRQ) و Power (RSRP)

و RSRP به واحد dBm) معيار توان دريافتی و RSRQ بيانگر كيفيت توان دريافتی.

رویه انتخاب سلول و بازانتخاب سلول (ادامه)

$$S_{rxlev} = Q_{rxlevmeas} - Q_{rxlevmin} - P_{compensation}, \quad S_{qual} = Q_{qualmeas} - Q_{qualmin},$$



$$P_{compensation} = \max(\text{UE_TXPWR_MAX_RACH} - P_{\text{MAX}}, 0) \text{ [dB]}$$

در مورد پارامترهای زیر یک تحقیق مختصر انجام دهید. به صورت جداگانه برای هر نسل. همه این موارد پارامترهای مربوط به توان دریافتی و کیفیت توان دریافتی است.

- پارامترهای GSM Received Signal Strength Indication (RSSI)، RxLev در
- پارامترهای UMTS RSSI، Ec/N0، RSCP در
- پارامترهای Signal Inter-Carrier to Interference-plus-Noise Ratio (CINR)، RSSI، RSRQ، RSRP در
- پارامترهای 5G NR و LTE Reference Noise Ratio (SINR)

کارکرد پارامتر Pcompensation در روابط مربوط به شرط S چیست؟

نکته ۲ با یک جستجوی ساده در اینترنت می‌توانید در مورد این پارامترها اطلاعات زیادی کسب کنید.

UE در رویه انتخاب سلول در تلاش است تا به یک سلول مناسب متصل گردد؛ چراکه UE تنها از یک سلول مناسب، می‌تواند خدمات بهنجهار شبکه را دریافت نماید. می‌بایست چهار شرط زیر را دارا باشد. قید S [۲]

زیربخش 5.2.3.1.2 برای حالت Frequency Division Duplexing (FDD) به صورت زیر تعریف می‌گردد:

$$Srxlev > 0 \quad \& \quad Squal > 0. \quad (1)$$

این قید برای Time Division Duplex (TDD) نیز به صورت زیر درنظر گرفته می‌شود:

$$Srxlev > 0. \quad (2)$$

دو پارامتر Srxlev و Squal نیز از روابط زیر بدست می‌آید:

$$\begin{aligned} Srxlev &= Q_{rxlevmeas} - (Q_{rxlevmin} + Q_{rxlevminoffset}) - P_{compensation}, \\ Squal &= Q_{qualmeas} - (Q_{qualmin} + Q_{qualminoffset}), \end{aligned} \quad (3)$$

که پارامترهای روابط فوق به صورت زیر تعریف می‌گردند:

: این پارامتر به نوعی توان خالص دریافتی از سلول است. در حالت FDD این پارامتر برابر با $Q_{rxlevmeas}$ ♠ و در TDD برابر با CPICH-RSCP و در P-CCPCH RSCP است.

: همان طور که از رابطه ۳ مشهود است، این پارامتر فقط برای حالت FDD بکار گرفته می‌شود، $Q_{qualmeas}$ ♠ و برابر با $CPICH\ Ec/No$ است.

: این پارامتر به نوعی باند پایینی و حداقل مقداری برای مقدار پارامتر $Q_{rxlevmin}$ ♠ است. $Q_{rxlevmin}$ مقداری بین $115dBm$ – $25dBm$ با گام‌های دوتایی را می‌تواند اختیار کند، در اطلاعات SIB3/4 ارسال می‌گردد.

: این پارامتر نیز بیانگر حداقل کیفیت قابل قبول برای یک سلول FDD است. $Q_{qualmin}$ ♠ مقداری بین $0dB$ – $-24dB$ را می‌تواند اتخاذ کند و در SIB3/4 ارسال می‌گردد.

پارامترهای $Q_{qualminoffset}$ و $Q_{rxlevminoffset}$ تنها زمانی بکار گرفته می‌شوند که UE به طور معمول بر روی یکی از سلول‌های VPLMN اردوزده، و در حال اجرای رویه انتخاب سلول برای یافتن PLMN با ارجحیت

بالاتر است. در طی این عملیات UE برای بدست آوردن شرط S، از پارامترهای سلول‌های PLMN‌ای که Qrxlevminoffset و Qqualminoffset مقداری بین یک تا ۱۶ می‌خواهد به او متصل شود، استفاده می‌کند. هر دو پارامتر در SIB3/4 ارسال می‌گردد، و در مقداری بین ۲ تا ۱۶ با گام‌های دوتایی می‌تواند اتخاذ کند. هر دو پارامتر در صورت عدم ارسال، مقدار پیش‌فرض صفر در نظر گرفته می‌شود.

نکته ۳ برای سادگی مطالب، این پارامترها در کلاس مطرح نشد.

: این پارامتر از رابطه زیر حاصل می‌گردد. Pcompensation ♠

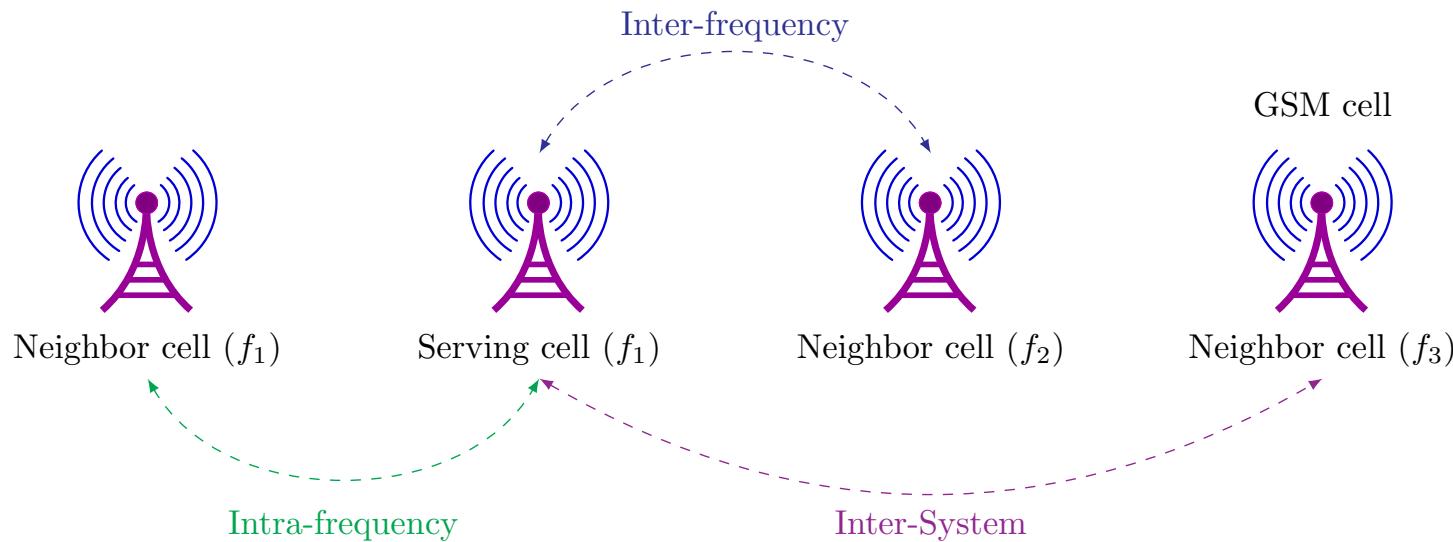
$$P_{compensation} = \max(UE_TXPWR_MAX_RACH - P_MAX, 0) \text{ [dB]} \quad (۴)$$

UE_TXPWR_MAX_RACH (به واحد dBm) بیشینه توانی است که یک UE می‌تواند در هنگام دسترسی به سلول از طریق Random Access Channel (RACH) ارسال کند [۳، زیربخش 10.3.6.39]. این پارامتر مقداری بین 33 dBm – 50 dBm را می‌تواند اختیار کند، به صورت اجباری (Mandatory Present) که مقداری بین

می بایست در SIB3/4 ارسال گردد. P_{MAX} نیز بیشینه توان (RF) است که Radio Frequency (RF) می تواند از UE ساطع گردد. P_{MAX} وابسته به کلاس توانی و باند عملکردی UE است.

با کمی دقت می توان دریافت که شرط S در حقیقت در تلاش است که مرزی برای حداقل دریافت UE از سلول مورد نظر تعیین کند.

انواع اندازه‌گیری



: [§§4.2.2، ۴] انواع اندازه‌گیری

- اندازه‌گیری‌های مربوط به سلول خدمتگزار.
 - اندازه‌گیری درون‌فرکانسی (Intra-frequency Measurement)
 - اندازه‌گیری بین‌فرکانسی (Inter-frequency Measurement)
 - اندازه‌گیری بین‌سامانه‌ای (Inter-system Measurement)

زنگ تفريح



چرا تایوان یا همان چین تایپه یا جمهوری چین برای آمریکا اهمیت حیاتی دارد؟



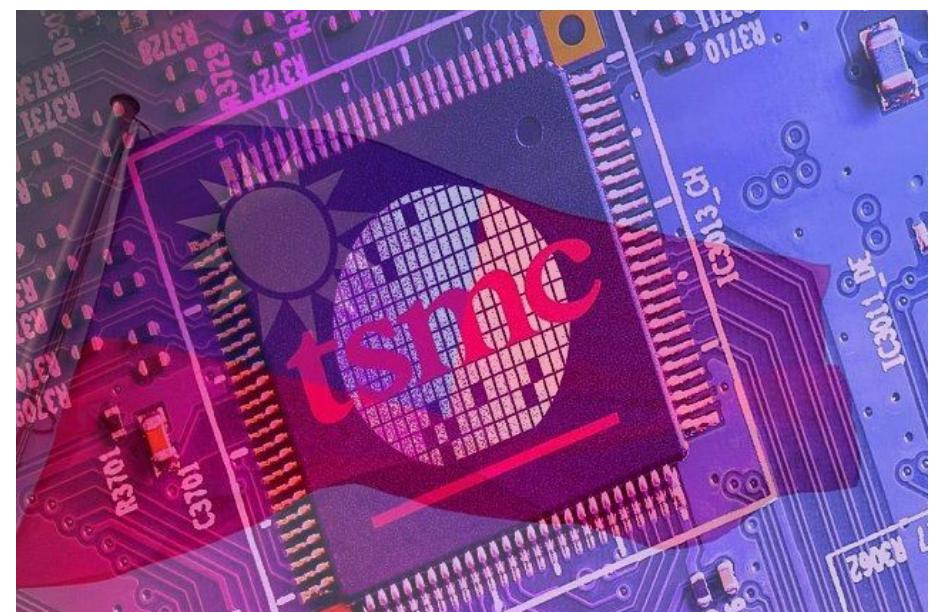
در جنگ داخلی چین در ۱۹۴۹، کمونیست‌ها به ریاست Mao Zedong پیروز شدند و جمهوری خلق چین را ایجاد کردند.



ملی‌گرها نیز به ریاست Chiang Kai-shek در جزیره تایوان مستقر شدند.

زنگ تفريح (ادامه)

به عنوان دو شرکت بزرگ تایوانی تولید تراشه در جهان، به تنها ی 65 درصد سهم بازار را به خود تخصیص داده اند.



شرکت‌های تولید نیمه‌هادی (Self Semiconductor)، کارخانه‌هایی هستند که در آن ویفرهای سیلیکونی ساخته می‌شود. از جمله این شرکت‌ها، می‌توان به موارد زیر اشاره کرد (برطبق آمار سال ۲۰۲۱):

- TSMC (Taiwan Semiconductor Manufacturing Company) - تایوان - ۵۷٪ بازار،

- Samsung - کره جنوبی - ۱۴.۵٪ بازار،

- UMC (United Microelectronics Corporation) - تایوان - ۸٪ بازار،

- Global Foundries - آمریکا - ۶.۵٪ بازار،

- SMIC (Semiconductor Manufacturing International Corporation) - چین - ۵.۵٪ بازار،

- ...

مشتریان اصلی این شرکت‌ها، طراحان تراشه هستند که برای ساخت تراشه از شرکت‌هایی یاد شده بهره می‌گیرند. البته برخی از شرکت‌های طراحی تراشه نظیر Intel، علاوه بر این راه کار خودشان نیز کارخانه تولید تراشه دارند. از نمونه تراشه‌های استفاده شده، می‌توان از موارد زیر یاد کرد:

شرط شروع اندازه‌گیری

تراشه Google - Tensor ✓

تراشه Qualcomm - Snapdragon ✓

تراشه Apple - Apple silicon ✓ که در Samsung و TSMC ساخته می‌شود.

تراشه Samsung - Exynos ✓

تراشه HiSilicon - Kirin ✓ در TSMC و SMIC ساخته می‌شود.

تراشه MediaTek - MediaTek ✓

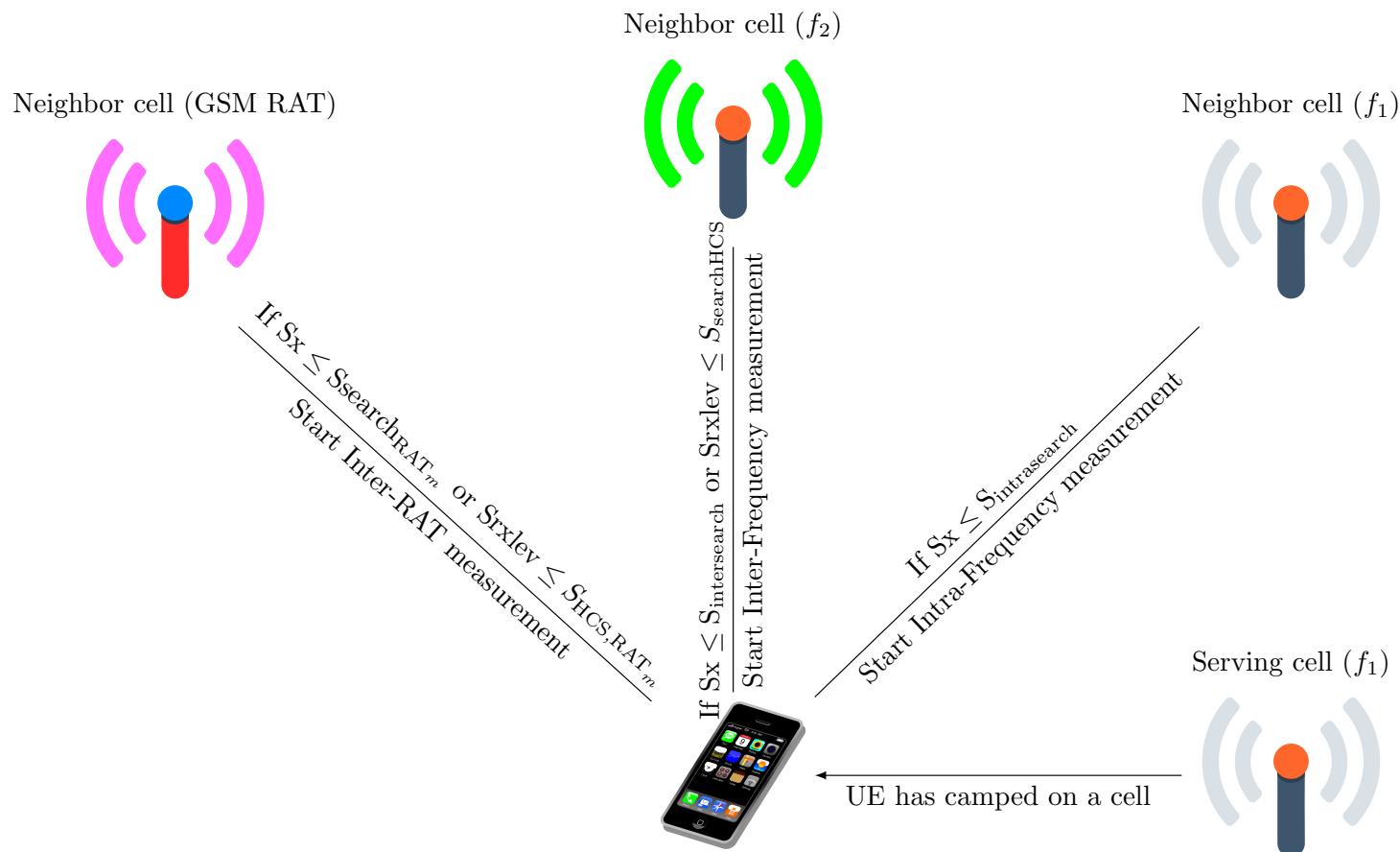
تراشه Intel ✓

تراشه AMD ✓

تراشه Nvidia ✓ اکثراً توسط TSMC تولید می‌شود.

تاهنگامی که شرایط سلول فعلی خراب نگشته، UE به خود زحمت اندازه‌گیری از شرایط سلول‌های دیگر را

نخواهد داد، و این بدان معنا است که رویه بازانتخاب سلول، اصلاً آغاز نخواهد شد.

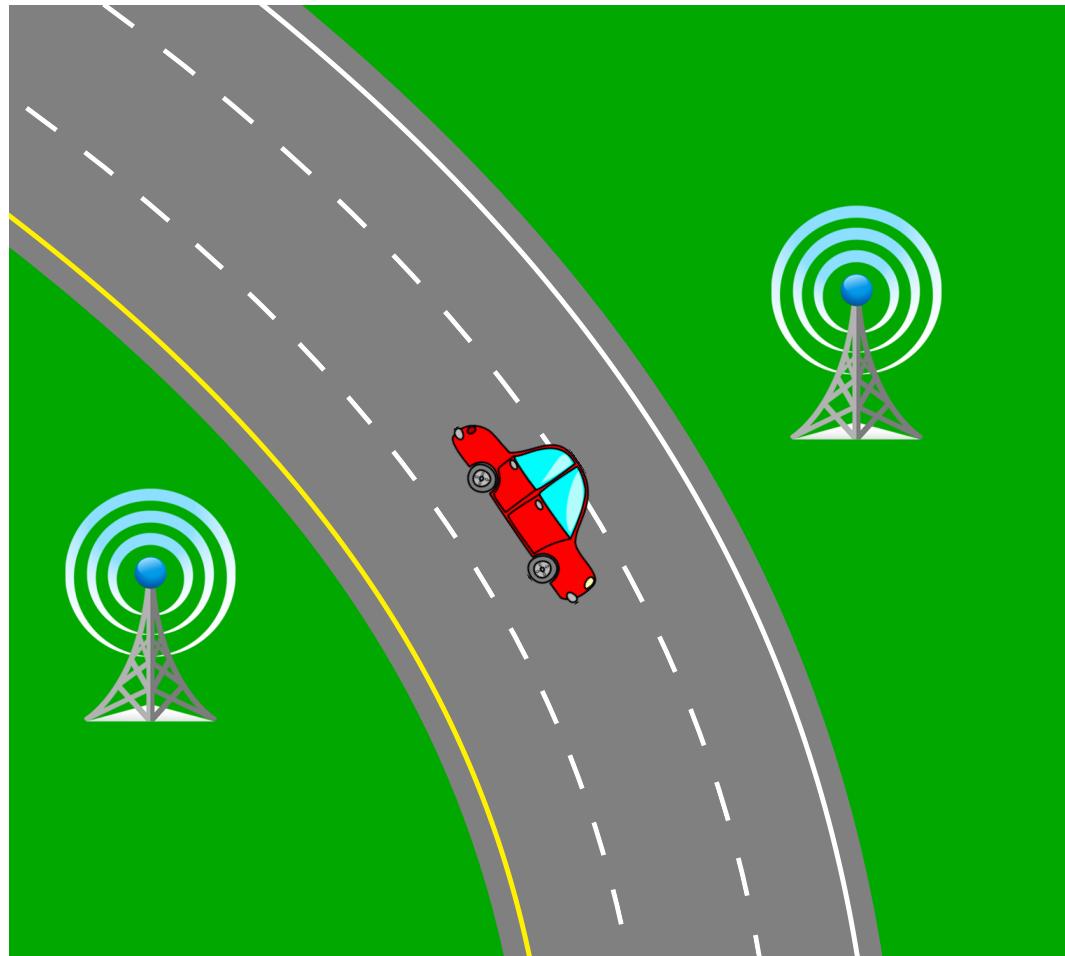


بازانتخاب سلول

UE دو معیار R_n و R_s را به ترتیب برای سنجش کیفیت سلول‌های همسایه و سلول فعلی بر می‌گزیند.

$$R_s = Q_{\text{meas},s} + \boxed{Q_{\text{hyst}_s}} + \boxed{Q_{\text{offsetmbms}}}$$

$$R_n = Q_{\text{meas},n} - \boxed{Q_{\text{offset}_{s,n}}} + \boxed{Q_{\text{offsetmbms}}} - \text{TO}_n \times (1 - L_n)$$

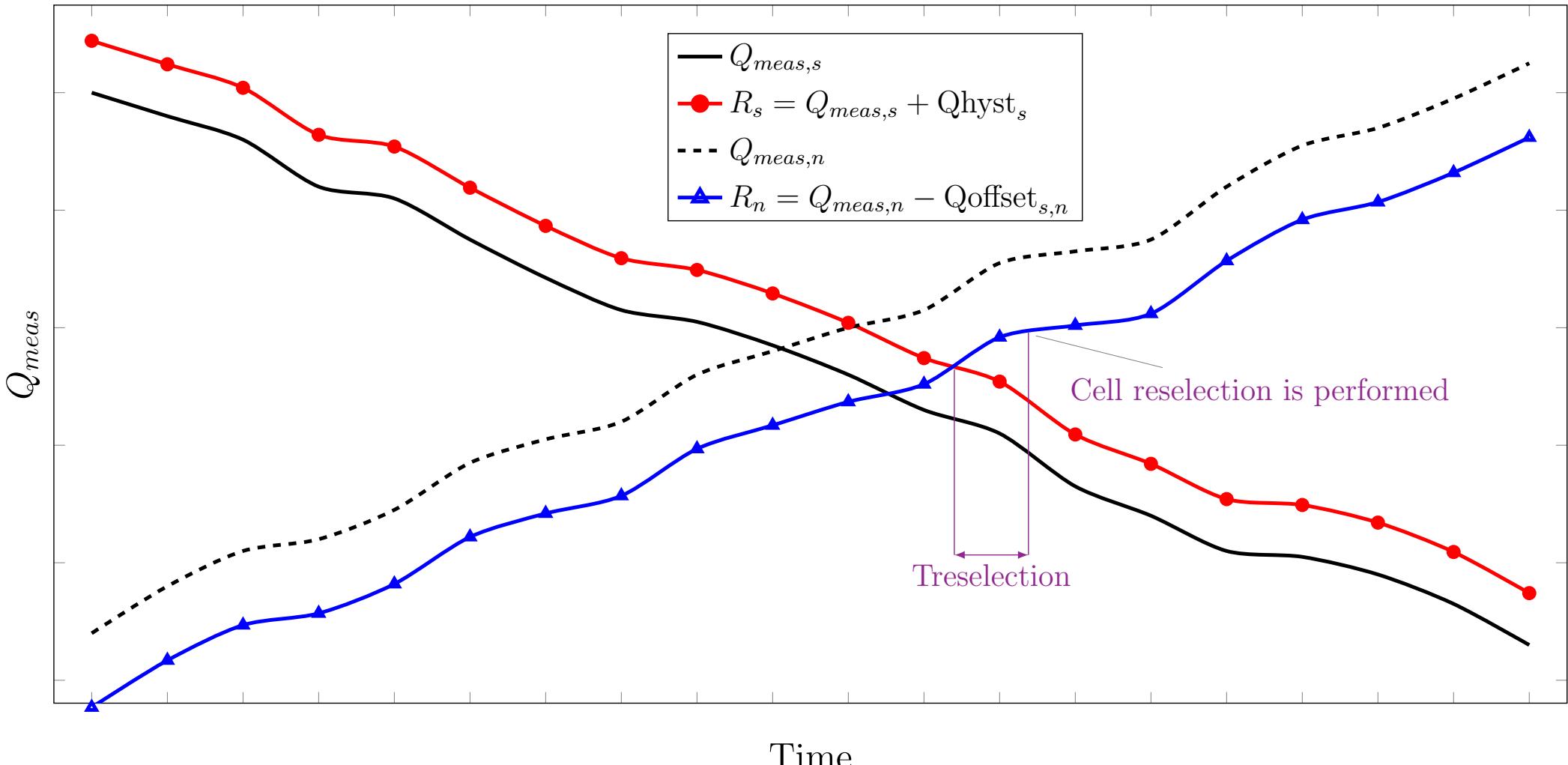


فرض کنید یک ماشین در یک اتوبان در حال حرکت است. دو سلول نیز در دو سوی اتوبان قرار داده شده است. میزان توان دریافتی از دو سلول در حرکت به شدت تغییر می‌کند. گاهی به سمت سلول A و گاهی به سمت سلول B . پس عملیات بازانتخاب سلول خیلی رخ خواهد داد. به این پدیده که موجب مصرف بیش از حد توان می‌شود، پدیده Ping-Pong می‌گوییم. راه حل؟

چالش Ping-Pong (ادامه)



در نظر گرفتن سه پارامتر هیسترزیس (Hysteresis) و $T_{reselection}$ و Q_{offset}



با اردو زدن بر روی سلول، UE می بایست حداقل در هر دوره DRX شرط S را چک نماید. حال اگر شرط S برای سلول خدمتگزار در تعداد N_{serv} دوره DRX برآورده نگشت، UE شروع به یافتن یک سلول مناسب دیگر از بین سلول های همسایه یاد شده در SIB11 می کند. مقدار پارامتر N_{serv} بر حسب طول دوره DRX ارایه شده است.

DRX Cycle [Seconds]	0.08	0.16	0.32	0.64	1.28	2.56	5.12
N_{serv} [Number of DRX cycle]	4	4	4	4	2	2	1

در صورتی که UE نتواند در مدت 12s، یک سلول مناسب از بین سلول های همسایه سلول خدمتگزار بیابد، به ناچار مجبور است که رویه انتخاب سلول را برای شبکه انتخاب شده آغاز نماید.

در رویه بازانتخاب سلول، فرض می شود که UE بر روی یک سلول اردو زده، اما با به دلایل مختلفی نظیر تحرک کاربر، ممکن است که سلول مورد نظر دیگر برای اتصال مناسب نباشد، بدینسان UE مجبور است برطبق اندازه گیری هایی که در بازه های زمانی معینی انجام می دهد، سلول دیگری را برای اردو زدن انتخاب نماید.

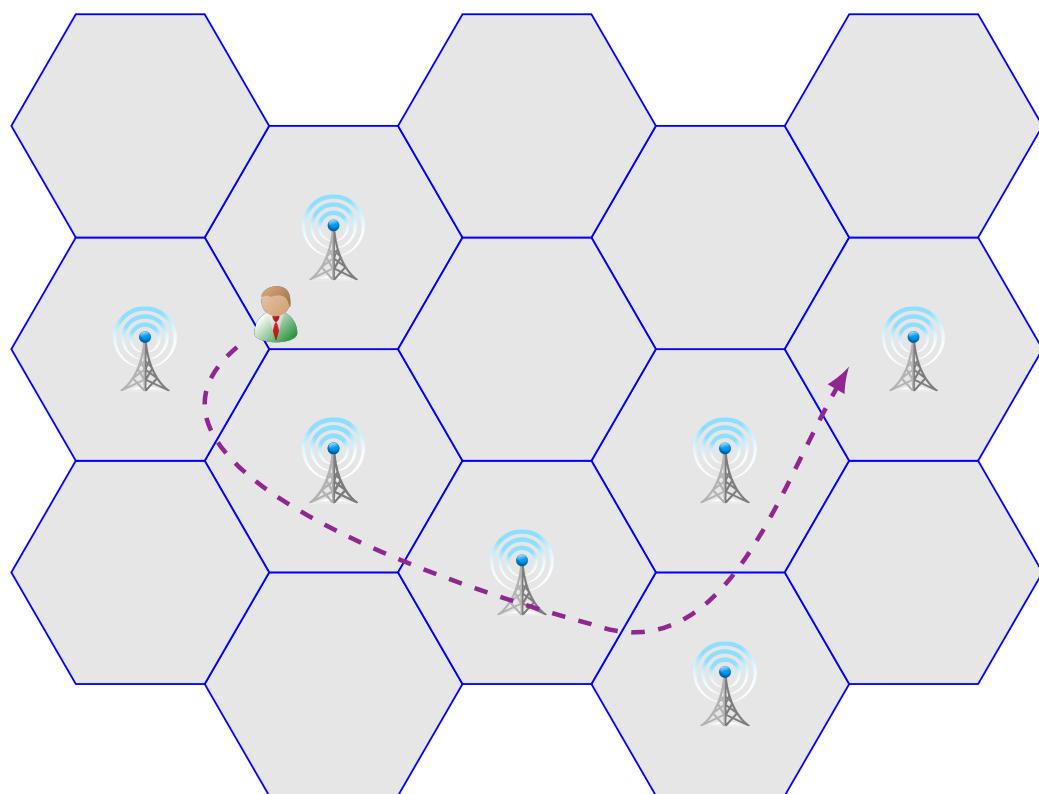
UE تا شرایطش وخیم نشده باشد، به اندازه گیری کیفیت توان دریافتی از سلول های دیگر شبکه، مبادرت

نمی‌ورزد؛ به عبارت بهتر، تا کیفیت سیگنال دریافتی از سلول خدمتگزار، از سطح آستانه معینی پایین‌تر نیاید،
UE به سراغ رویه بازانتخاب سلول نخواهد رفت.

برطبق اندازه‌گیری‌هایی که UE انجام می‌دهد، سلول‌هایی به عنوان کاندیدا برای رویه بازانتخاب سلول برگزیده
می‌گردد. کاندیداها بر اساس معیار مشخصی (شرط R و H) رتبه‌بندی می‌شوند. در صورتی که شرایط بهترین
کاندیدا به نسبت معینی از شرایط سلول فعلی (سلولی که در حال حاضر UE بر روی آن اردو زده است) بهتر باشد
و این بهتر بودن تا مدت زمانی مشخص حفظ گردد، UE بر روی سلول مذکور اردو خواهد زد.

رہنمائی مکانی پروزرسانی

رویه بروزرسانی منطقه مکانی (Location Area Update)

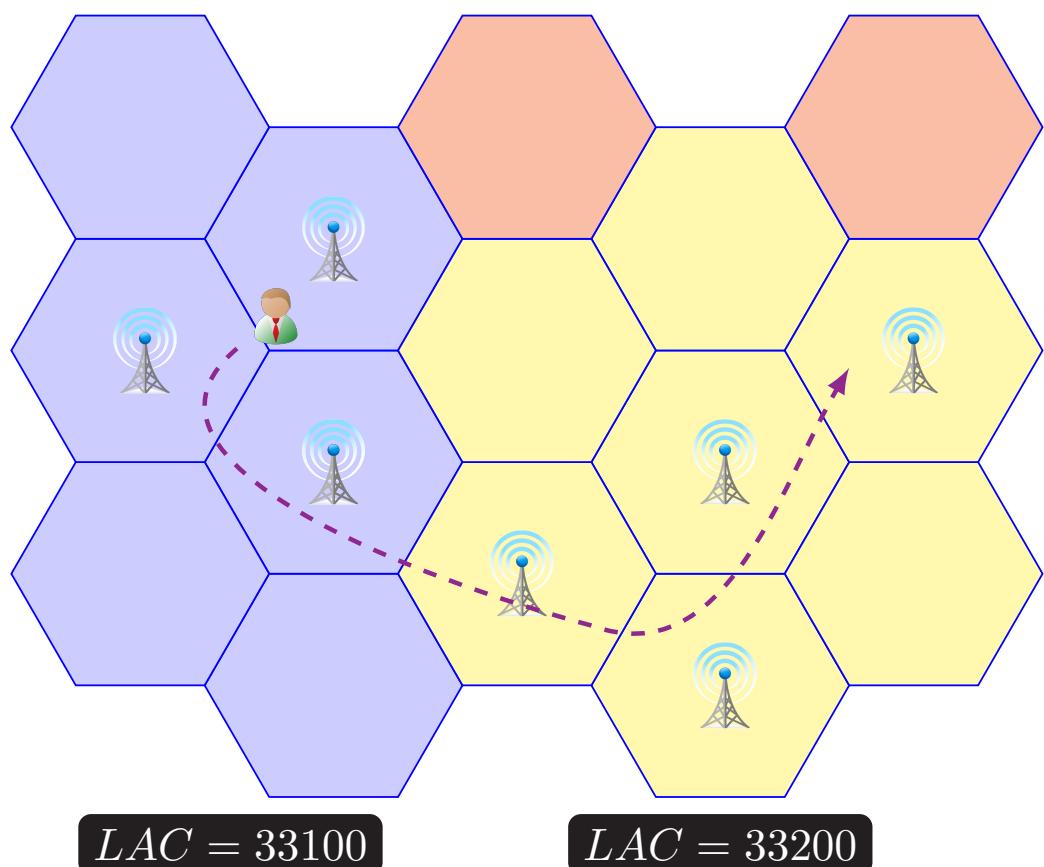


☞ فرض کنید شما به تلفن همراه دوستتان تماس گرفته اید، شبکه در کanal PCCH کدام سلول، شما

را پی جویی (Paging) کند؟

- در تمام سلول ها !!!
- کاربر هرگاه باز انتخاب سلول کرد، عملیات بروزرسانی منطقه مکانی را انجام دهد. شبکه نیز در پایگاه داده ای (Visitor Location Register) آخرین مکان را نگه می دارد.

رویه بروزرسانی منطقه مکانی (ادامه)



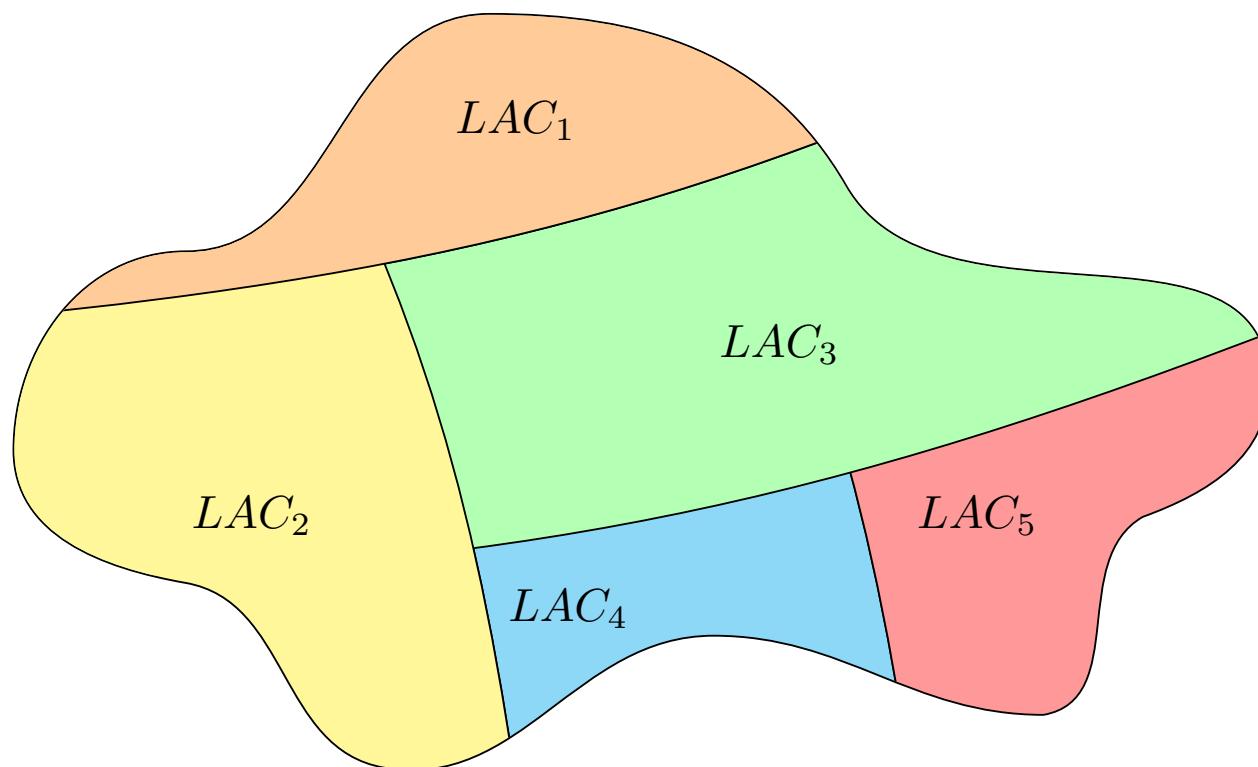
نقشه شبکه را به تعدادی ناحیه
با نام منطقه مکانی (Location Area) و تخصیص
یک کد به هر ناحیه به نام LAC (Location Area
.Code).

یک پارامتر ۱۶ بیتی است که در اطلاعات SIB توسط هر سلول
ارسال می‌شود.

در شبکه LTE به جای LAC پارامتر TAC
(Tracking Area Code) داریم.

رویه بروزرسانی منطقه مکانی - تمرین

- در شبکه GSM و UMTS در هر زمان، UE تنها می‌داند که در یک منطقه مکانی قرار دارد، و کد آن را در خود ذخیره می‌کند. تا زمانی که بر روی سلولی که در یک LAC متفاوت با LAC فعلی قرار داشته باشد، نرود، عملیات بروزرسانی منطقه مکانی را انجام نمی‌دهد. اما در LTE چه تفاوتی ایجاد شده است؟



به مجموعه‌ای از سلول‌ها در شبکه GSM یا در شبکه UMTS، که کاربر می‌تواند بدون بروزرسانی مکانش در Location Area (LA) در آن حرکت کند، اصطلاحاً منطقه مکانی (Visitor Location Register (VLR)) گفته می‌شود. هنگامی که کاربر از یک LA به LA دیگر می‌رود، لازم است تا با اجرای رویه بروزرسانی مکان، مکان خود را در VLR بروز نماید. بدین‌سان در هنگام پی‌جويي، شبکه پیام پی‌جويي را در تمامی سلول‌های LA ای که کاربر در آن قرار دارد، ارسال می‌کند.

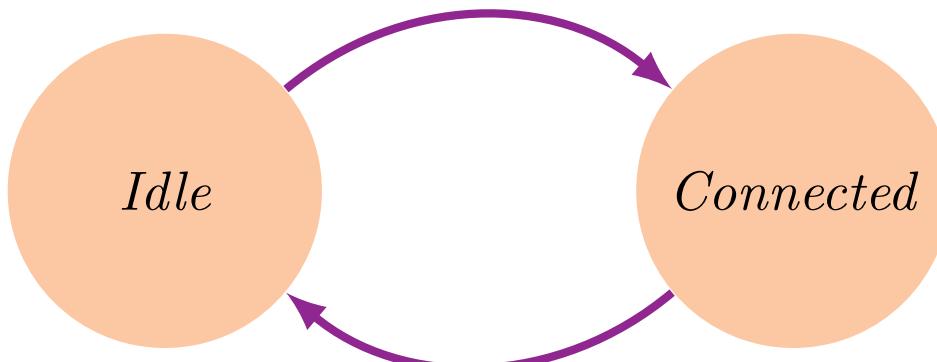
لازم به ذکر است که اگر LA خیلی بزرگ شود، و از آن‌جا که در هنگام پی‌جويي، پیام پی‌جويي به تمامی سلول‌های LA خواهد رسید، موجب می‌شود که مقدار زیادی پهنازی باند بیهوده مصرف گردد. از سوی دیگر، اگر LA بیش از اندازه کوچک باشد، تعداد درخواست بروزرسانی مکان توسط کاربران زیاد می‌گردد، که این خود موجب مصرف انرژی بیش از حد UE و همچنین بالارفتن ترافیک سیگنال‌دهی شبکه می‌گردد.

هر LA در یک شبکه، دارای کدی منحصر به‌فرد به نام LAC است که آن را از بقیه LA‌ها متمایز می‌سازد. پارامتری است چهار رقمی (۱۶ بیتی) که در اطلاعات سامانه ارسال می‌گردد. با همراه کردن پارامترهای MCC و

دست Location Area Identity (LAI)، به پارامتر دیگری به نام Mobile Network Code (MNC) در کنار خواهیم یافت.

ناحیه رهگیری مفهومی به مانند منطقه مکانی و منطقه مسیریابی است، که در شبکه LTE مورد استفاده قرار می‌گیرد. هر ناحیه رهگیری بیانگر ناحیه‌ای از شبکه LTE است که چندین eNodeB در آن جای داده شده است. بر طبق استانداردهای 3rd Generation Partnership Project (3GPP) در مُد بیکار می‌باشد در حد یک ناحیه رهگیری مشخص باشد. پر واضح است که این مهم زمانی صورت می‌پذیرد که در صورت تغییر ناحیه رهگیری، UE رویه بروزرسانی ناحیه رهگیری را انجام دهد، و ناحیه رهگیری فعلی خود را به اطلاع شبکه برساند.

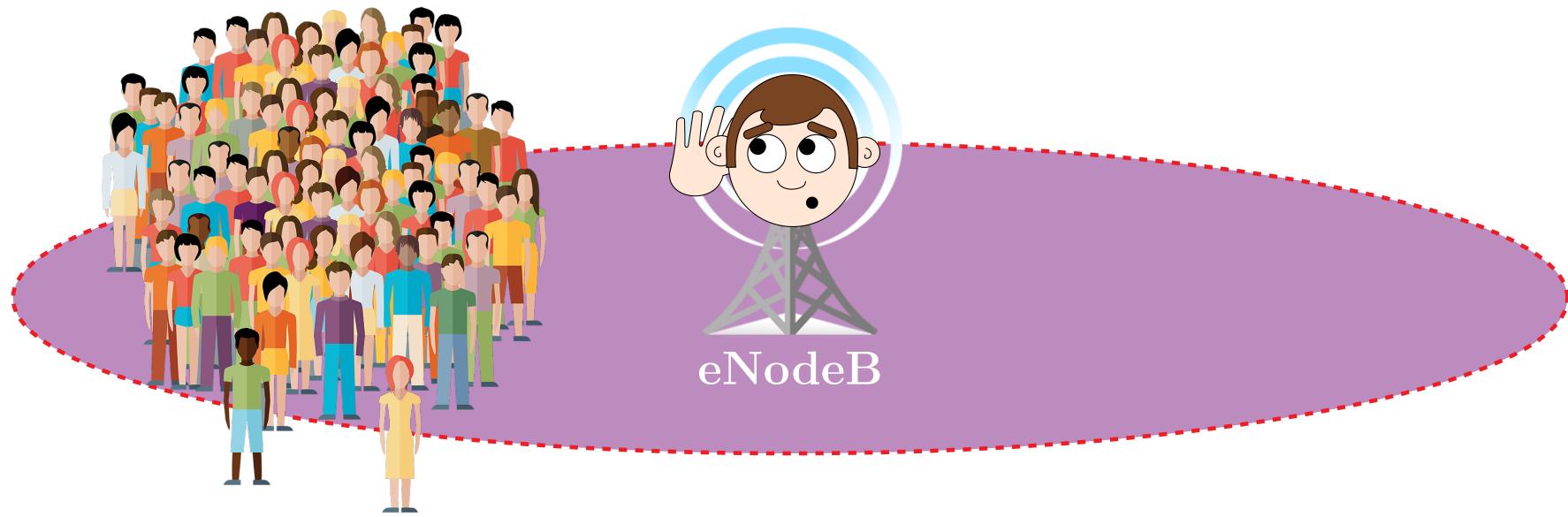
ریاضی تماریں



فرض کنید UE در مُد بیکار قرار دارد. چرا باید به مُد متصل برود؟

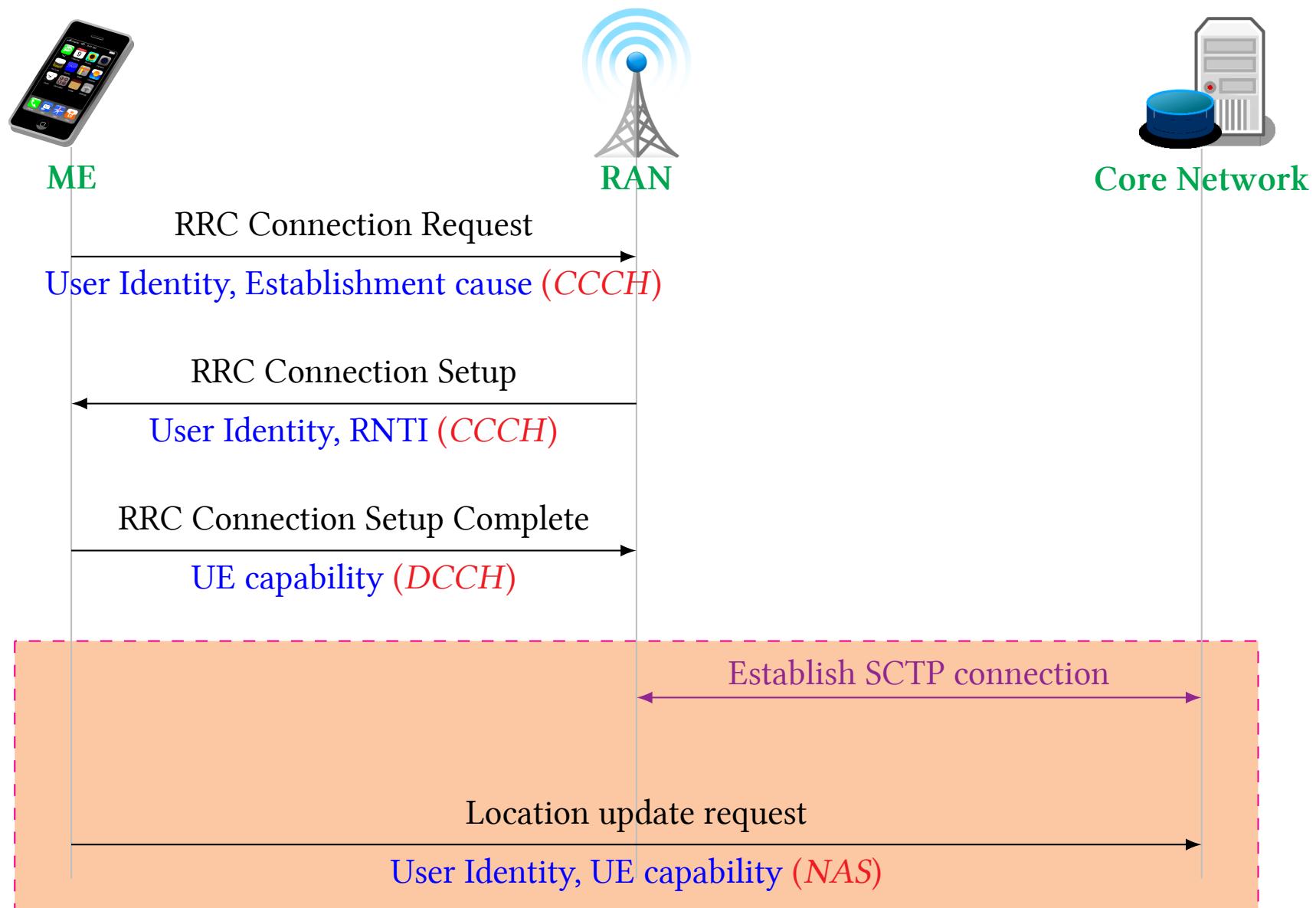
- دریافت خدمات بهنچار Short Message Service (SMS) از شبکه، به مانند ارسال Normal Service برقراری تماس و خدمات داده.
- UE پی‌جوبی شده است.
- کارهای کنترلی به مانند بروزرسانی منطقه مکانی.

رویه دسترسی تصادفی (ادامه)



- استفاده از یک سازوکار دسترسی تصادفی (Random Access) (RACH (Random Access Channel)) هر کس نیاز داشت، تقاضای خود را در یک کانال کنترلی عمومی در پیوند فراسو به نام Backoff Counter ارسال کند.
- اگر دو درخواست به صورت همزمان رسید، چه؟ سازوکار

رویه دسترسی تصادفی (ادامه)



نمونه پیام RRC Connection Request

ID	Timestamp	N	T	D	C	Type	Name	
1404	113585	2022-03-04 22:21:05.089	2320	3G	▼	RRC	DL DCCH	Security Mode Command
1405	113584	2022-03-04 22:21:05.053	2320	3G	▲	RRC	UL DCCH	Measurement Report
1406	113583	2022-03-04 22:21:05.009	2320	3G	▼	RRC	DL DCCH	Measurement Control
1407	113582	2022-03-04 22:21:04.969	2320	3G	▼	RRC	DL DCCH	Measurement Control
1408	113581	2022-03-04 22:21:04.930	2320	3G	▼	RRC	DL DCCH	Measurement Control
1409	113580	2022-03-04 22:21:04.929	2320	3G	▼	RRC	DL DCCH	Measurement Control
1410	113579	2022-03-04 22:21:04.609	2320	3G	▼	RRC	DL DCCH	Measurement Control
1411	113578	2022-03-04 22:21:03.965	2320	3G	▲	RRC	UL DCCH	Initial Direct Transfer
1412	113577	2022-03-04 22:21:03.965	2320	3G	▲	RRC	UL DCCH	Initial Direct Transfer
1413	113576	2022-03-04 22:21:03.965	2320	3G	▲	NAS	GPRS MM	Routing Area Update Request
1414	113575	2022-03-04 22:21:03.965	2320	3G	▲	NAS	MM	Location Updating Request
1415	113574	2022-03-04 22:21:03.965	2320	3G	▲	RRC	UL DCCH	RRC Connection Setup Complete
1416	113573	2022-03-04 22:21:03.908	2320	3G	▼	RRC	DL CCCH	RRC Connection Setup
1417	113572	2022-03-04 22:21:03.907	2320	3G	▼	RRC	BCCH_BCH	First Segment
1418	113571	2022-03-04 22:21:03.887	2320	3G	▼	RRC	BCCH_BCH	Complete SIB List
1419	113570	2022-03-04 22:21:03.867	2320	3G	▼	RRC	BCCH_BCH	Complete SIB List
1420	113569	2022-03-04 22:21:03.827	2320	3G	▼	RRC	BCCH_BCH	Last Segment Short
1421	113568	2022-03-04 22:21:03.797	2320	G	▲	RRC	UL CCCH	RRC Connection Request
1422	113567	2022-03-04 22:21:03.707	2320	3G	▼	RRC	BCCH_BCH	Complete SIB List
1423	113566	2022-03-04 22:21:03.687	2320	3G	▼	RRC	Extension SIB	
1424	113565	2022-03-04 22:21:03.687	2320	3G	▼	RRC	BCCH_BCH	Complete SIB List
1425	113564	2022-03-04 22:21:03.667	2320	3G	▼	RRC	BCCH_BCH	Complete SIB List
1426	113563	2022-03-04 22:21:03.647	2320	3G	▼	RRC	BCCH_BCH	No Segment
1427	113562	2022-03-04 22:21:03.627	2320	3G	▼	RRC	BCCH_BCH	Complete SIB List
1428	113561	2022-03-04 22:21:03.607	2320	3G	▼	RRC	BCCH_BCH	Complete SIB List
1429	113560	2022-03-04 22:21:03.587	2320	3G	▼	RRC	BCCH_BCH	No Segment
1430	113559	2022-03-04 22:21:03.567	2320	3G	▼	RRC	BCCH_BCH	Complete SIB List

Text Find
 292F162A5043208C2CC3156D577DA0
 DLT: 148, Payload: aww (Automator Wireshark Wrapper)
 Automator Wireshark Wrapper
 Protocol: 1
 Data length: 15
 UL-CCCH-Message
 message: rrcConnectionRequest (1)
 rrcConnectionRequest
 initialUE-Identity: tmsi-and-LAI (1)
 tmsi-and-LAI
 tmsi: 2f162a50 [bit length 32, 0010 1111 0001 0110 0010 1010 0101 0000 decimal value 789981776]
 lai
 plmn-Identity
 mcc: 3 items
 Item 0
 Digit: 4
 Item 1
 Digit: 3
 Item 2
 Digit: 2
 mnc: 2 items
 Item 0
 Digit: 1
 Item 1
 Digit: 1
 Mobile Country Code (MCC): Iran (Islamic Republic of) (432)
 Mobile Network Code (MNC): Telecommunication Company of Iran (TCI) (11)
 lac: 8598 [bit length 16, 1000 0101 1001 1000 decimal value 34200]
 establishmentCause: registration (12)
 protocolErrorIndicator: noError (0)
 v3d0NonCriticalExtensions
 rRCConnectionRequest-v3d0ext
 v4b0NonCriticalExtensions
 rrcConnectionRequest-v4b0ext
 accessStratumReleaseIndicator: rel-9 (5)
 v590NonCriticalExtensions
 rrcConnectionRequest-v590ext
 ...0 predefinedConfigStatusInfo: False
 v690NonCriticalExtensions
 rrcConnectionRequest-v690ext
 ueCapabilityIndication: hsdch-edch (1)
 domainIndicator: cs-domain (0)
 cs-domain
 csCallType: other (2)
 v6b0NonCriticalExtensions
 rrcConnectionRequest-v6b0ext
 v6e0NonCriticalExtensions
 rrcConnectionRequest-v6e0ext
 supportForFDPCN: true (0)
 v770NonCriticalExtensions
 rrcConnectionRequest-v770ext

نمونه پیام RRC Connection Setup

ID	Timestamp	N	T	D	C	Type	Name	ARFCN	Code	I
78943	2021-04-25 19:19:24.963	1058	3G	▼	NAS	GPRS MM	Identity Request	3021	181	
78942	2021-04-25 19:19:24.963	1058	3G	▼	RRC	DL DCCH	Downlink Direct Transfer	3021	181	
78941	2021-04-25 19:19:24.874	1058	3G	▲	RRC	UL DCCH	Security Mode Complete	3021	181	
78940	2021-04-25 19:19:24.873	1058	3G	▼	RRC	DL DCCH	Security Mode Command	3021	181	
78939	2021-04-25 19:19:24.833	1058	3G	▼	RRC	DL DCCH	Measurement Control	3021	181	
78938	2021-04-25 19:19:24.572	1058	3G	▲	RRC	UL DCCH	Initial Direct Transfer	3021	181	
78937	2021-04-25 19:19:24.572	1058	3G	▲	RRC	UL DCCH	Initial Direct Transfer	3021	181	
78936	2021-04-25 19:19:24.570	1058	3G	▲	NAS	GPRS MM	Routing Area Update Request	3021	181	
78935	2021-04-25 19:19:24.570	1058	3G	▲	NAS	MM	Location Updating Request	3021	181	
78934	2021-04-25 19:19:24.570	1058	3G	▲	RRC	UL DCCH	RRC Connection Setup Complete	3021	181	
78933	2021-04-25 19:19:24.519	1058	3G	▼	RRC	DL CCCH	RRC Connection Setup	3021	181	
78932	2021-04-25 19:19:24.514	1058	3G	▼	RRC	BCCH_BCH	Complete SIB List	3021	181	
78931	2021-04-25 19:19:24.494	1058	3G	▼	RRC	BCCH_BCH	Complete SIB List	3021	181	
78930	2021-04-25 19:19:24.474	1058	3G	▼	RRC	BCCH_BCH	Subsequent Segment	3021	181	
78929	2021-04-25 19:19:24.454	1058	3G	▼	RRC	BCCH_BCH	Subsequent Segment	3021	181	
78928	2021-04-25 19:19:24.434	1058	3G	▼	RRC	BCCH_BCH	First Segment	3021	181	
78927	2021-04-25 19:19:24.414	1058	3G	▼	RRC	BCCH_BCH	Complete SIB List	3021	181	
78926	2021-04-25 19:19:24.376	1058	3G	▲	RRC	UL CCCH	RRC Connection Request	3021	181	
78925	2021-04-25 19:19:24.337	1058	3G	▼	RRC	PCCH	Paging Type 1	3021	181	
78924	2021-04-25 19:19:24.294	1058	3G	▼	RRC	BCCH_BCH	Complete SIB List	3021	181	
78923	2021-04-25 19:19:24.274	1058	3G	▼	RRC	BCCH_BCH	Last Segment Short	3021	181	
78922	2021-04-25 19:19:24.254	1058	3G	▼	RRC	BCCH_BCH	Complete SIB List	3021	181	
78921	2021-04-25 19:19:24.234	1058	3G	▼	RRC	BCCH_BCH	Subsequent Segment	3021	181	
78920	2021-04-25 19:19:24.134	1058	3G	▼	RRC	BCCH_BCH	Last Segment Short	3021	181	
78919	2021-04-25 19:19:24.114	1058	3G	▼	RRC	BCCH_BCH	Subsequent Segment	3021	181	
78918	2021-04-25 19:19:24.094	1058	3G	▼	RRC	BCCH_BCH	Complete SIB List	3021	181	

Find

```

394724905943208BCF61F00819808161BEC0F000F9890727C108F865080009030FE8A163CC021484C727C508F8E5180009142727C92
8F96528002942727CD28F9E5380029320000C0F1A19E03E0090088ECDAC13EBF5CA82BE03067EE813F0A0142A46085A804202A500
0

DLT: 148, Payload: aww (Automator Wireshark Wrapper)
Automator Wireshark Wrapper
Protocol: 2
Data length: 107
DL-CCCH-Message
message: rrcConnectionSetup (3)
rrcConnectionSetup: later-than-r3 (1)
later-than-r3
initialUE-Identity: tmsi-and-LAI (1)
tmsi-and-LAI
tsni: 47249059 [bit length 32, 0100 0111 0010 0100 1001 0000 0101 1001 decimal value 1193578585]
lai
plmn-Identity
mcc: 3 items
Item 0
Digit: 4
Item 1
Digit: 3
Item 2
Digit: 2
mnc: 2 items
Item 0
Digit: 1
Item 1
Digit: 1
lac: 79ec [bit length 16, 0111 1001 1110 1100 decimal value 31212]
rrc-TransactionIdentifier: 0
criticalExtensions: criticalExtensions (1)
criticalExtensions: r9 (0)
r9
rrcConnectionSetup-r9
new-U-RNTI
srnc-Identity: 0400 [bit length 12, 4 LSB pad bits, 0000 0100 0000 ... decimal value 64]
s-RNTI: b0df60 [bit length 20, 4 LSB pad bits, 1011 0000 1101 1111 0110 ... decimal value 724470]
rrc-StateIndicator: cell-DCH (0)
utran-DRX-CycleLengthCoeff
drx-CycleLengthCoefficient: 6
capabilityUpdateRequirement
...1 .... ue-RadioCapabilityFDDUpdateRequirement-FDD: True
...0.. ue-RadioCapabilityTDDUpdateRequirement-TDD384: False
...0.. ue-RadioCapabilityTDDUpdateRequirement-TDD768: False
...0.. ue-RadioCapabilityTDDUpdateRequirement-TDD128: False
systemSpecificCapUpdateReqList: 1 item
Item 0

```

نمونه پیام RRC Connection Setup complete

ID	Timestamp	N	T	D	C	Type	Name	ARFCN	Code	I	Find
78943	2021-04-25 19:19:24.963	1058	3G	▼	NAS	GPRS MM	Identity Request	3021	181	 1... = SM capability (MT SMS pt to pt capability): Mobile station supports mobile terminated point to point SMS 0... = VBS notification reception: no VBS capability or no notifications wanted 0... = VGCS notification reception: no VGCS capability or no notifications wanted 0 = FC Frequency Capability: The MS does not support the E-GSM or R-GSM band 1... = CM3: The MS supports options that are indicated in classmark 3 IE .0... = Spare: 0 .1... = LCS VA capability (LCS value added location request notification capability): LCS value added location request notification capability supported .0.... = UCS2 treatment: the ME has a preference for the default alphabet .0... = SoLSA: The ME does not support SoLSA .1... = CMSP: CM Service Prompt: Network initiated MO CM connection request supported for at least one CM protocol .1... = A5/3 algorithm supported: encryption algorithm A5/3 available .0... = A5/2 algorithm supported: encryption algorithm A5/2 not available gsm-Classmark3: 6114042F65233b8800d2128000 0... = Spare bit(s): 0 .110 ... = Multiband supported field: 6 .1... = GSM 1800 Supported: true .1... = E-GSM or R-GSM Supported: true .0... = P-GSM Supported: false .0001 = A5 bits: 0x01 0... = A5/7 algorithm supported: encryption algorithm A5/7 not available .0... = A5/6 algorithm supported: encryption algorithm A5/6 not available .0... = A5/5 algorithm supported: encryption algorithm A5/5 not available .1... = A5/4 algorithm supported: encryption algorithm A5/4 available 0001 = Associated Radio Capability 2: 1 .0100 = Associated Radio Capability 1: 4 0... = R Support: false .0... = HSCSD Multi Slot Capability: false .0... = UCS2 treatment: the ME has a preference for the default alphabet .0... = Extended Measurement Capability: false .0... = MS measurement capability: false .1... = MS Positioning Method Capability present: true .00 001... = MS Positioning Method: 0x01 .0... = MS assisted E-OTD: MS assisted E-OTD not supported .0... = MS based E-OTD: MS based E-OTD not supported 0... = MS assisted GPS: MS assisted GPS not supported .0... = MS based GPS: MS based GPS not supported .1... = MS Conventional GPS: Conventional GPS supported .0... = ECSD Multi Slot Capability present: false .1... = 8-PSK Struct present: true .111 0110 ... = 8-PSK Struct: 0x76 .1... = Modulation Capability: 8-PSK supported for uplink transmission and downlink reception .1... = 8-PSK RF Power Capability 1 present: true .1 0... = 8-PSK RF Power Capability 1: Power class E2 (0x02) .1... = 8-PSK RF Power Capability 2 present: true .10 ... = 8-PSK RF Power Capability 2: Power class E2 (0x02) .0... = GSM 400 Band Information present: false .1... = GSM 850 Associated Radio Capability present: true .01 00... = GSM 850 Associated Radio Capability: 0x04 .1... = GSM 1900 Associated Radio Capability present: true .0 001. = GSM 1900 Associated Radio Capability: 0x01 .1... = UMTS FDD Radio Access Technology Capability: UMTS FDD supported .0... = UMTS 3.84 Mcps TDD Radio Access Technology Capability: UMTS 3.84 Mcps TDD not supported
78942	2021-04-25 19:19:24.963	1058	3G	▼	RRC	DL DCCH	Downlink Direct Transfer	3021	181		
78941	2021-04-25 19:19:24.874	1058	3G	▲	RRC	UL DCCH	Security Mode Complete	3021	181		
78940	2021-04-25 19:19:24.873	1058	3G	▼	RRC	DL DCCH	Security Mode Command	3021	181		
78939	2021-04-25 19:19:24.833	1058	3G	▼	RRC	DL DCCH	Measurement Control	3021	181		
78938	2021-04-25 19:19:24.572	1058	3G	▲	RRC	UL DCCH	Initial Direct Transfer	3021	181		
78937	2021-04-25 19:19:24.572	1058	3G	▲	RRC	UL DCCH	Initial Direct Transfer	3021	181		
78936	2021-04-25 19:19:24.570	1058	3G	▲	NAS	GPRS MM	Routing Area Update Request	3021	181		
78935	2021-04-25 19:19:24.570	1058	3G	▲	NAS	MM	Location Updating Request	3021	181		
78934	2021-04-25 19:19:24.570	1058	3G	▲	RRC	UL DCCH	RRC Connection Setup Complete	3021	181		
78933	2021-04-25 19:19:24.519	1058	3G	▼	RRC	DL CCCH	RRC Connection Setup	3021	181		
78932	2021-04-25 19:19:24.514	1058	3G	▼	RRC	BCCH_BCH	Complete SIB List	3021	181		
78931	2021-04-25 19:19:24.494	1058	3G	▼	RRC	BCCH_BCH	Complete SIB List	3021	181		
78930	2021-04-25 19:19:24.474	1058	3G	▼	RRC	BCCH_BCH	Subsequent Segment	3021	181		
78929	2021-04-25 19:19:24.454	1058	3G	▼	RRC	BCCH_BCH	Subsequent Segment	3021	181		
78928	2021-04-25 19:19:24.434	1058	3G	▼	RRC	BCCH_BCH	First Segment	3021	181		
78927	2021-04-25 19:19:24.414	1058	3G	▼	RRC	BCCH_BCH	Complete SIB List	3021	181		
78926	2021-04-25 19:19:24.376	1058	3G	▲	RRC	UL CCCH	RRC Connection Request	3021	181		
78925	2021-04-25 19:19:24.337	1058	3G	▼	RRC	PCCH	Paging Type 1	3021	181		
78924	2021-04-25 19:19:24.294	1058	3G	▼	RRC	BCCH_BCH	Complete SIB List	3021	181		
78923	2021-04-25 19:19:24.274	1058	3G	▼	RRC	BCCH_BCH	Last Segment Short	3021	181		
78922	2021-04-25 19:19:24.254	1058	3G	▼	RRC	BCCH_BCH	Complete SIB List	3021	181		
78921	2021-04-25 19:19:24.234	1058	3G	▼	RRC	BCCH_BCH	Subsequent Segment	3021	181		
78920	2021-04-25 19:19:24.134	1058	3G	▼	RRC	BCCH_BCH	Last Segment Short	3021	181		
78919	2021-04-25 19:19:24.114	1058	3G	▼	RRC	BCCH_BCH	Subsequent Segment	3021	181		
78918	2021-04-25 19:19:24.094	1058	3G	▼	RRC	BCCH_BCH	Complete SIB List	3021	181		

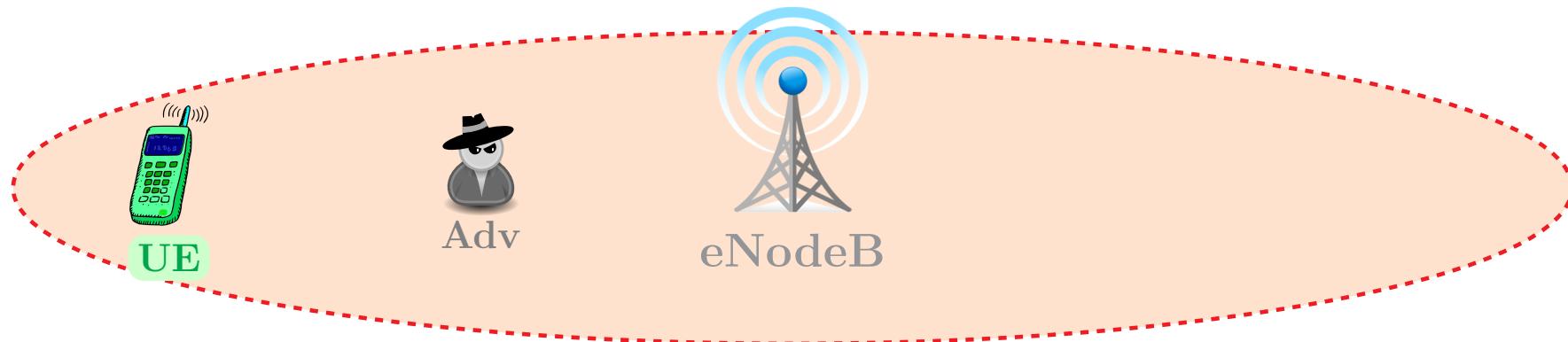
L3 Message پیام نمونه

ID	timestamp	N	T	D	Type	Channel type	Name
64	2020-11-24 08:34:02.254	101	4G	▼	RRC	DL_DCCH	RRC Connection Reconfiguration
63	2020-11-24 08:34:02.250	101	4G	▼	RRC	BCCH_DL_SCH	System Information
62	2020-11-24 08:34:02.219	101	4G	▲	RRC	UL_DCCH	UL Information Transfer
61	2020-11-24 08:34:02.218	101	4G	▲	NAS	EPS_Mobility_Management	Tracking Area Update Request
60	2020-11-24 08:34:02.216	101	4G	▼	RRC	BCCH_BCH	MIB
59	2020-11-24 08:34:02.215	101	4G	▼	RRC	BCCH_DL_SCH	System Information Block Type 1
58	2020-11-24 08:34:02.186	101	4G	▲	RRC	UL_DCCH	RRC Connection Reconfiguration Complete
57	2020-11-24 08:34:02.161	101	4G	▼	RRC	DL_DCCH	RRC Connection Reconfiguration
56	2020-11-24 08:34:02.114	101	4G	▲	RRC	UL_DCCH	Measurement Report
55	2020-11-24 08:34:01.634	101	4G	▲	RRC	UL_DCCH	Measurement Report
54	2020-11-24 08:34:00.594	101	4G	▲	RRC	UL_DCCH	Measurement Report
53	2020-11-24 08:34:00.154	101	4G	▲	RRC	UL_DCCH	Measurement Report
52	2020-11-24 08:33:59.972	101	4G	▲	RRC	UL_DCCH	RRC Connection Reconfiguration Complete
51	2020-11-24 08:33:59.971	101	4G	▼	RRC	DL_DCCH	RRC Connection Reconfiguration
50	2020-11-24 08:33:31.062	101	4G	▼	RRC	BCCH_BCH	MIB
49	2020-11-24 08:33:31.052	101	4G	▼	RRC	BCCH_DL_SCH	System Information Block Type 1
48	2020-11-24 08:33:30.416	101	4G	▼	RRC	BCCH_DL_SCH	System Information
47	2020-11-24 08:33:29.894	101	4G	▲	RRC	UL_DCCH	RRC Connection Reconfiguration Complete
46	2020-11-24 08:33:29.892	101	4G	▼	RRC	DL_DCCH	RRC Connection Reconfiguration
45	2020-11-24 08:33:29.847	101	4G	▼	RRC	BCCH_DL_SCH	System Information
44	2020-11-24 08:33:29.844	101	4G	▲	RRC	UL_DCCH	Measurement Report
43	2020-11-24 08:33:29.806	101	4G	▼	RRC	BCCH_DL_SCH	System Information
42	2020-11-24 08:33:29.796	101	4G	▼	RRC	BCCH_DL_SCH	System Information
41	2020-11-24 08:33:29.786	101	4G	▼	RRC	BCCH_DL_SCH	System Information
40	2020-11-24 08:33:29.785	101	4G	▲	RRC	UL_DCCH	RRC Connection Reconfiguration Complete
39	2020-11-24 08:33:29.784	101	4G	▼	RRC	BCCH_BCH	MIB
38	2020-11-24 08:33:29.783	101	4G	▼	RRC	DL_DCCH	RRC Connection Reconfiguration

00570220003103E5E03E1334F21185A211035758A6200D6114042F65233B8800D2F2800040080-
 DLT: 148, Payload: aww (Automator Wireshark Wrapper)
 Automator Wireshark Wrapper
 Protocol: 250
 Data length: 85
 Non-Access-Stratum (NAS)PDU
 0000 = Security header type: Plain NAS message, not security protected (0)
0111 = Protocol discriminator: EPS mobility management messages (0x07)
 NAS EPS Mobility Management Message Type: Tracking area update request (0x48)
 0... = Type of security context flag (TSC): Native security context (for KSlasme)
 .101 = NAS key set identifier: (5) ASME
0... = Active flag: No bearer establishment requested
001 = EPS update type value: Combined TA/LA updating (1)
 EPS mobile identity - Old GUTI
 Length: 11
0... = odd/even indic: 0
110 = Type of identity: GUTI (6)
 Mobile Country Code (MCC): Iran (Islamic Republic of) (432)
 Mobile Network Code (MNC): Mobile Communication of Iran (MCI) (11)
 MME Group ID: 32769
 MME Code: 136
 M-TMSI: 0xc5032f10
 UE network capability
 Element ID: 0x58
 Length: 5
 1.... = EEA0: Supported
 .1.... = 128-EEA1: Supported
 ..1.... = 128-EEA2: Supported
 ...1.... = 128-EEA3: Supported
 ...0... = EEA4: Not Supported
0.. = EEA5: Not Supported
0.= EEA6: Not Supported
0= EEA7: Not Supported
 0.... = EIA0: Not Supported
 .1.... = 128-EIA1: Supported
 ..1.... = 128-EIA2: Supported
 ...1.... = 128-EIA3: Supported
 ...0... = EIA4: Not Supported
0.. = EIA5: Not Supported
0.= EIA6: Not Supported
0= EIA7: Not Supported
 1.... = UEA0: Supported
 .1.... = UEA1: Supported
 ..0.... = UEA2: Not Supported
 ...0.... = UEA3: Not Supported
 ...0.. = UEA4: Not Supported
0.. = UEA5: Not Supported
0.= UEA6: Not Supported
0= UEA7: Not Supported
 0.... = UCS2 support (UCS2): The UE has a preference for the default alphabet
 .1.... = UMTS integrity algorithm UIA1: Supported
 ..0.... = UMTS integrity algorithm UIA2: Not Supported
 ...0.... = UMTS integrity algorithm UIA3: Not Supported
0.. = UMTS integrity algorithm UIA4: Not Supported

روپے شناسی

TMSI (Temporary Mobile Subscriber)



➡ ارسال IMSI در واسطه هوایی (Air Interface) از جنبه‌های امنیتی خطرناک است.

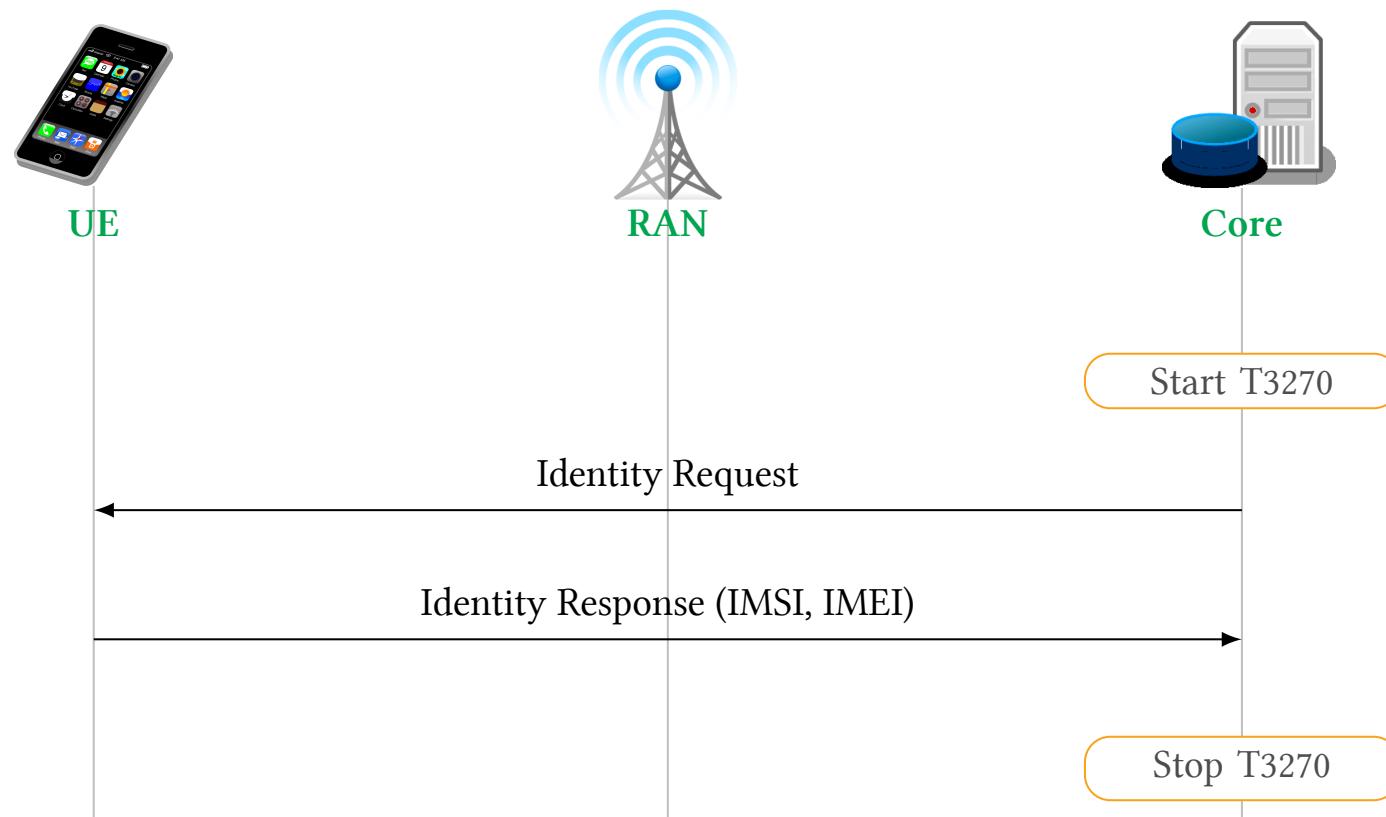
➡ راه کارها:

✖ رمز کردن IMSI

✓ تخصیص یک شناسه موقت به جای IMSI

رویه شناسایی (Procedure) (شناسایی)

اولین رویه‌ای که بعد از رسیدن اولین پیام از سمت هسته شبکه آغاز می‌گردد، رویه شناسایی است.



نمونه پیام Identity Response

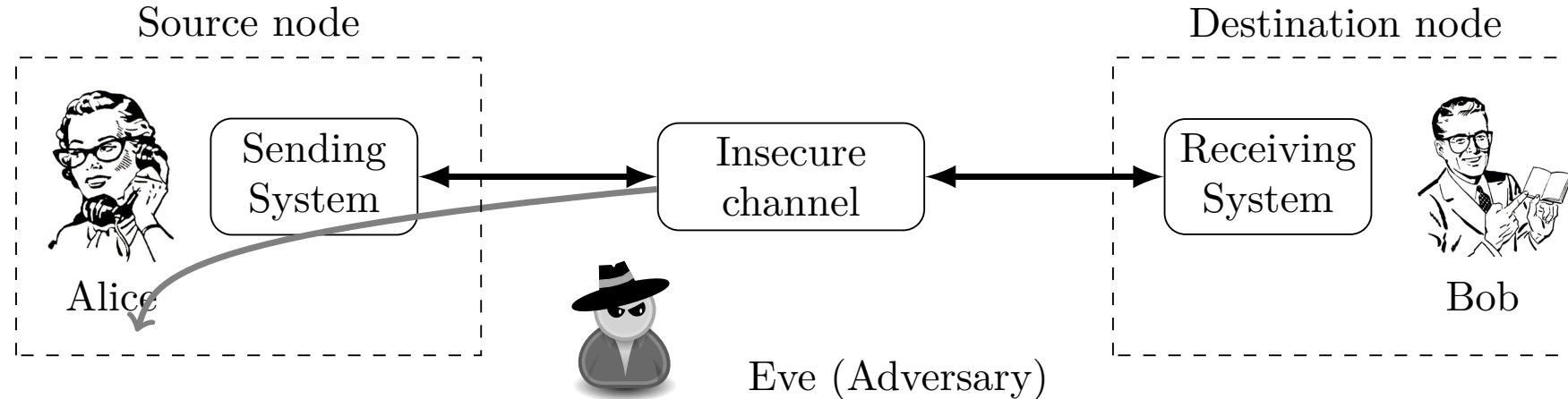
ID	timestamp	N	T	D	Type	Channel type	Name	
18174	2020-10-30 18:28:49.788	101	3G	▼	NAS	GPRS_Mobility_Management	Service Accept	
18173	2020-10-30 18:28:49.788	101	3G	▼	RRC	DL_DCCH	Downlink DirectTransfer	
18172	2020-10-30 18:28:49.671	101	3G	▲	RRC	UL_DCCH	Uplink Direct Transfer	
18171	2020-10-30 18:28:49.669	101	3G	▲	NAS	Call_RelatedSS_Management	Connect Acknowledge	
18170	2020-10-30 18:28:49.669	101	3G	▼	NAS	Call_RelatedSS_Management	Connect	
18169	2020-10-30 18:28:49.668	101	3G	▼	RRC	DL_DCCH	Downlink DirectTransfer	
18168	2020-10-30 18:28:49.588	101	3G	▼	NAS	Call_RelatedSS_Management	Alerting	
18167	2020-10-30 18:28:49.588	101	3G	▼	RRC	DL_DCCH	Downlink DirectTransfer	
18166	2020-10-30 18:28:49.514	101	3G	▲	RRC	UL_DCCH	Uplink Direct Transfer	
18165	2020-10-30 18:28:49.514	101	3G	▲	NAS	GPRS_Mobility_Management	Service Request	
18164	2020-10-30 18:28:49.510	101	3G	▲	RRC	UL_DCCH	Uplink Direct Transfer	
18163	2020-10-30 18:28:49.510	101	3G	▲	NAS	GPRS_Mobility_Management	Routing Area Update Complete	
18162	2020-10-30 18:28:49.508	101	3G	▼	NAS	GPRS_Mobility_Management	Routing Area Update Accept	
18161	2020-10-30 18:28:49.508	101	3G	▼	RRC	DL_DCCH	Downlink DirectTransfer	
18160	2020-10-30 18:28:49.268	101	3G	▲	RRC	UL_DCCH	Uplink Direct Transfer	
18159	2020-10-30 18:28:49.268	101	3G	▲	NAS	GPRS_Mobility_Management	Identity Response	
18158	2020-10-30 18:28:49.268	101	3G	▼	NAS	GPRS_Mobility_Management	Identity Request	
18157	2020-10-30 18:28:49.268	101	3G	▼	RRC	DL_DCCH	Downlink DirectTransfer	
18156	2020-10-30 18:28:48.989	101	3G	▲	RRC	UL_DCCH	Security Mode Complete	
18155	2020-10-30 18:28:48.988	101	3G	▼	RRC	DL_DCCH	Security Mode Command	
18154	2020-10-30 18:28:48.908	101	3G	▼	RRC	DL_DCCH	Measurement Control	
18153	2020-10-30 18:28:48.868	101	3G	▼	RRC	DL_DCCH	Measurement Control	
18152	2020-10-30 18:28:48.828	101	3G	▼	RRC	DL_DCCH	Measurement Control	
18151	2020-10-30 18:28:48.788	101	3G	▼	RRC	DL_DCCH	Measurement Control	
18150	2020-10-30 18:28:48.501	101	3G	▲	RRC	UL_DCCH	Radio Bearer Setup Complete	
18149	2020-10-30 18:28:48.208	101	3G	▼	RRC	DL_DCCH	Radio Bearer Setup	
18148	2020-10-30 18:28:47.878	101	3G	▼	NAS	Call_RelatedSS_Management	Call Proceeding	

0816088A16830374505405

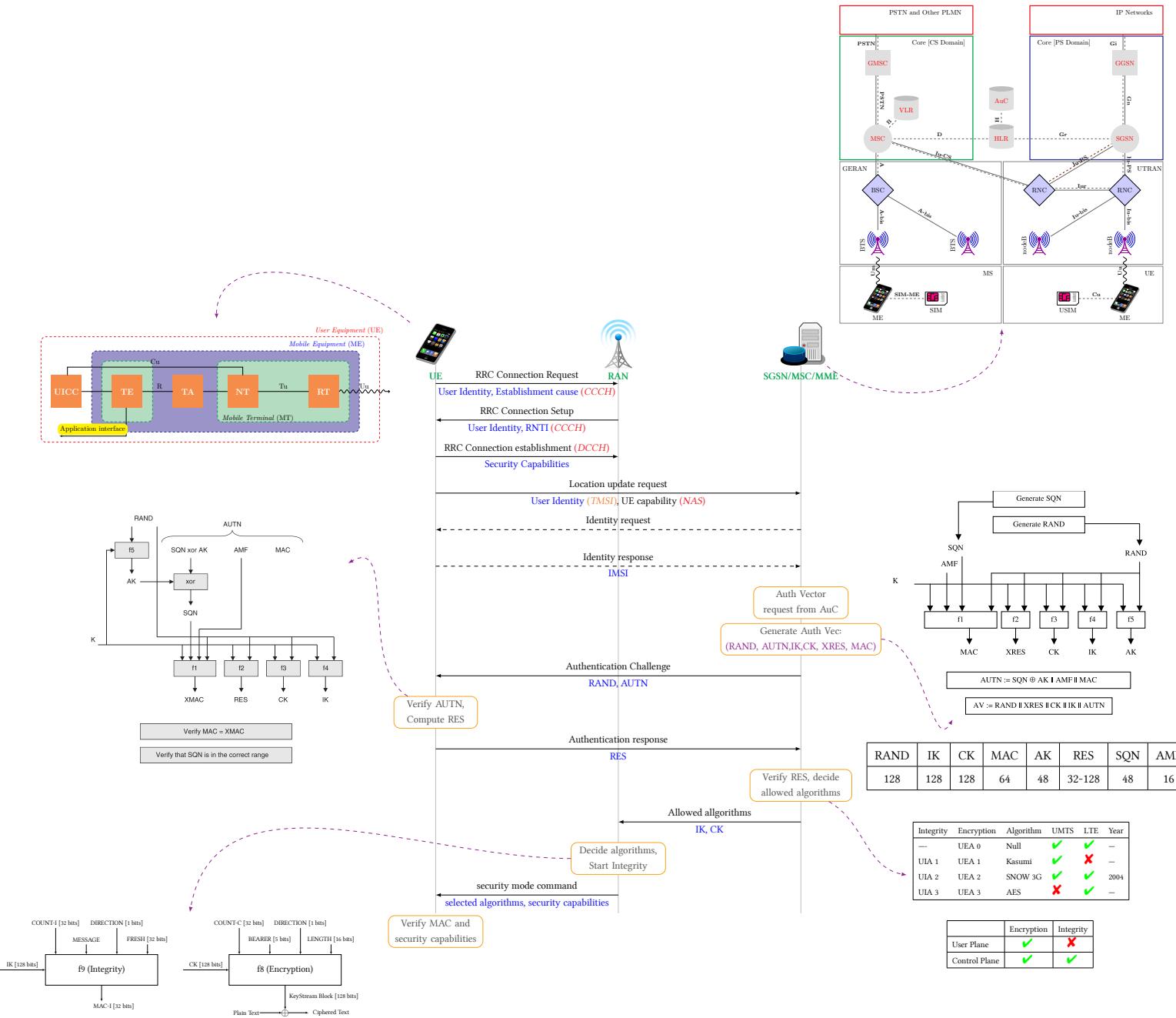
DLT: 148, Payload: aww (Automator Wireshark Wrapper)
 Automator Wireshark Wrapper
 Protocol: 193
 Data length: 11
 GSM A-I/F DTAP - Identity Response
 Protocol Discriminator: GPRS mobility management messages (8)
 ... 1000 = Protocol discriminator: GPRS mobility management messages (0x08)
 0000 = Skip Indicator: No indication of selected PLMN (0)
 DTAP GPRS Mobility Management Message Type: Identity Response (0x16)
 Mobile Identity - IMEI (861383047054550)
 Length: 8
 1000 = Identity Digit 1: 8
 ... 1... = Odd/even indication: Odd number of identity digits
010 = Mobile Identity Type: IMEI (2)
 BCD Digits: 861383047054550

امینت در شیگه‌های تلفن همراه

چرا به احراز اصالت (Authentication) نیاز داریم؟

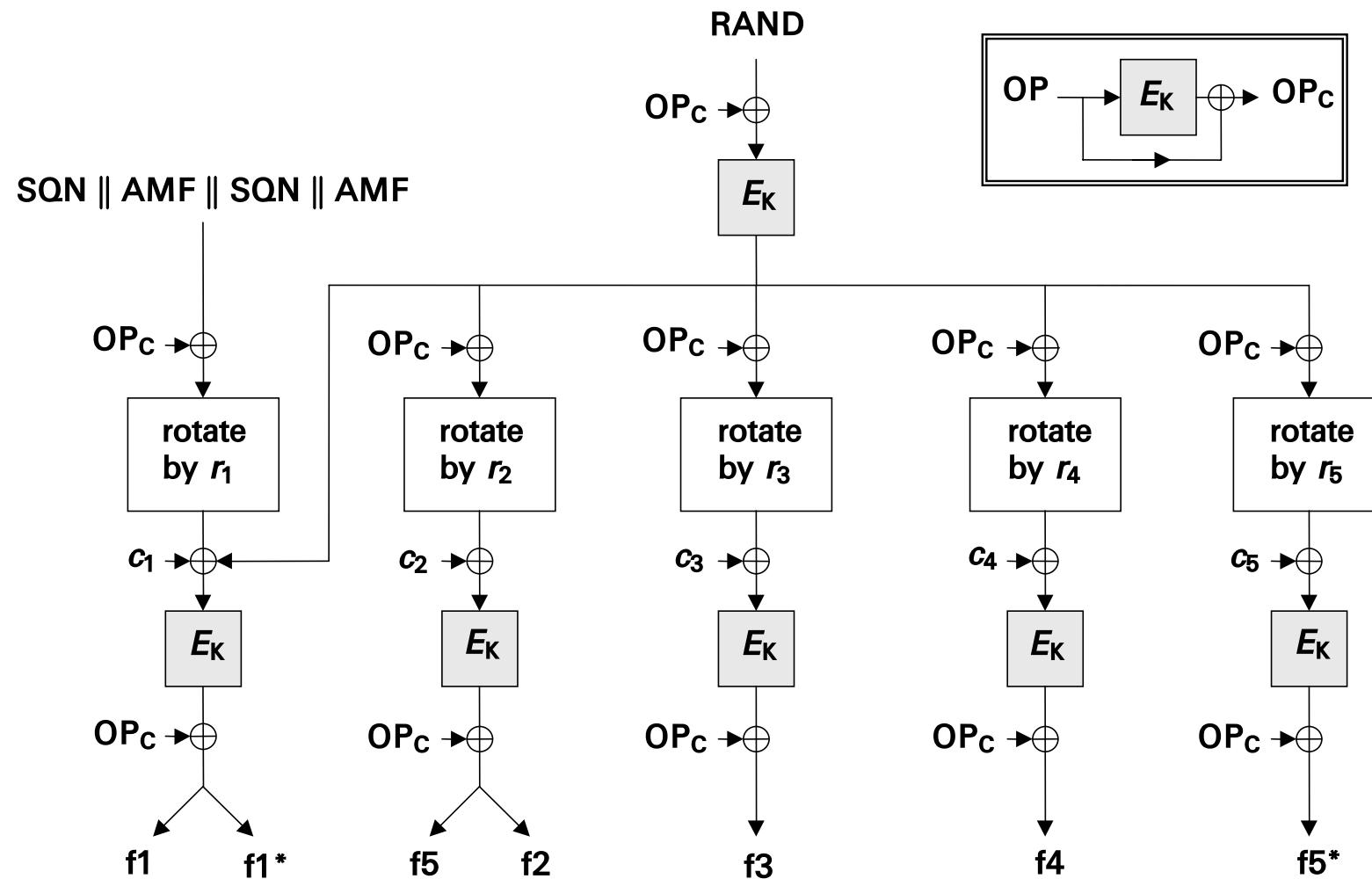


- برای محترمانه ماندن پیام می‌بایست از رمزگذاری (Encryption) استفاده کنیم، و برای آن نیاز به کلید داریم.
 - استفاده از سازوکارهای برقراری کلید (Key Establishment) [۵، فصل 12]
- تبدال کلید (Key Transport): یک سمت کلید را تولید کرده و در اختیار طرف مقابل نیز قرار می‌دهد.
- توافق کلید (Key Agreement): هر دو سمت، در فرایند تولید کلید مشارکت می‌کنند.



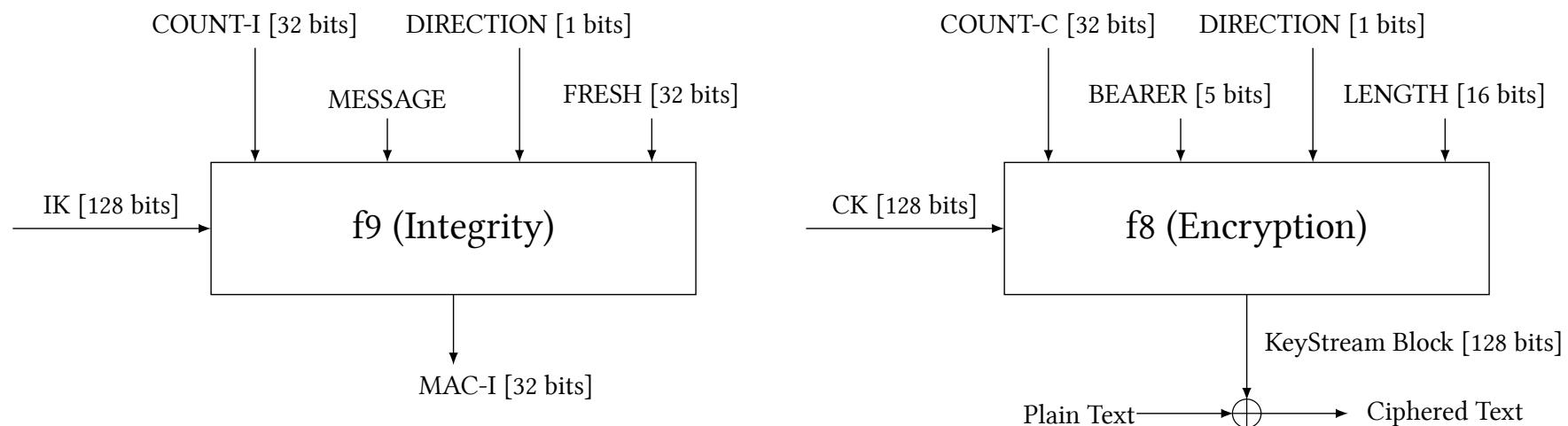
الگوریتم‌های تامین امنیت در UMTS

نمایی از توابع MILENAGE 



الگوریتم‌های تامین امنیت در UMTS (ادامه)

نمای کلی از ورودی‌های توابع f_8 و f_9 



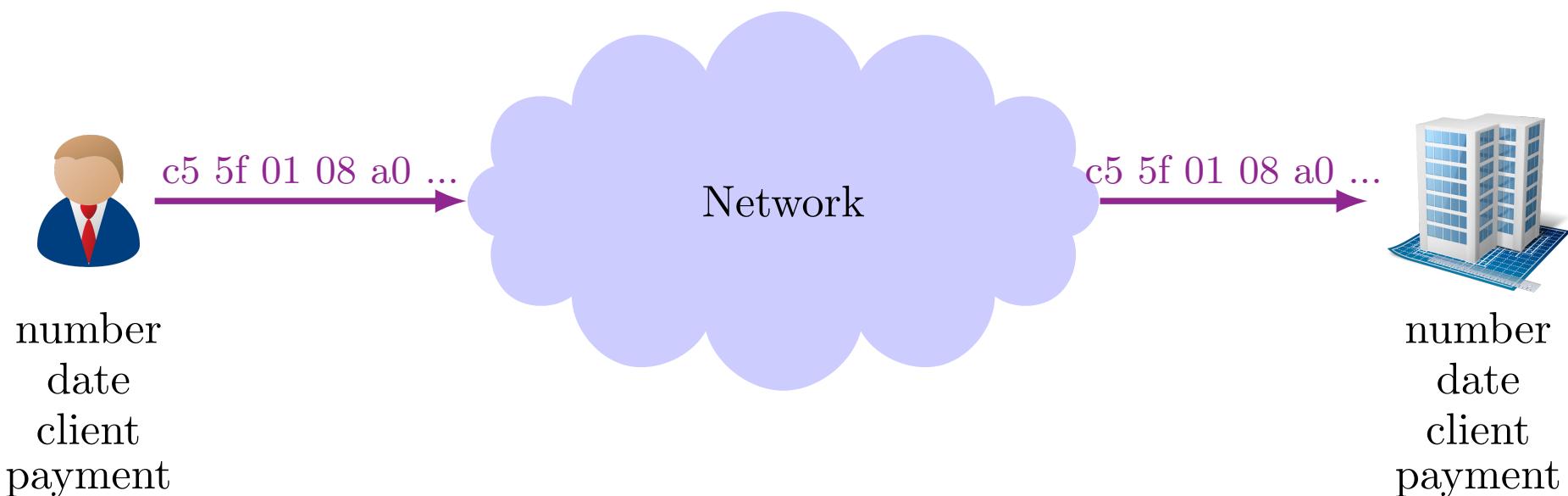
ASN.1

طرح مساله

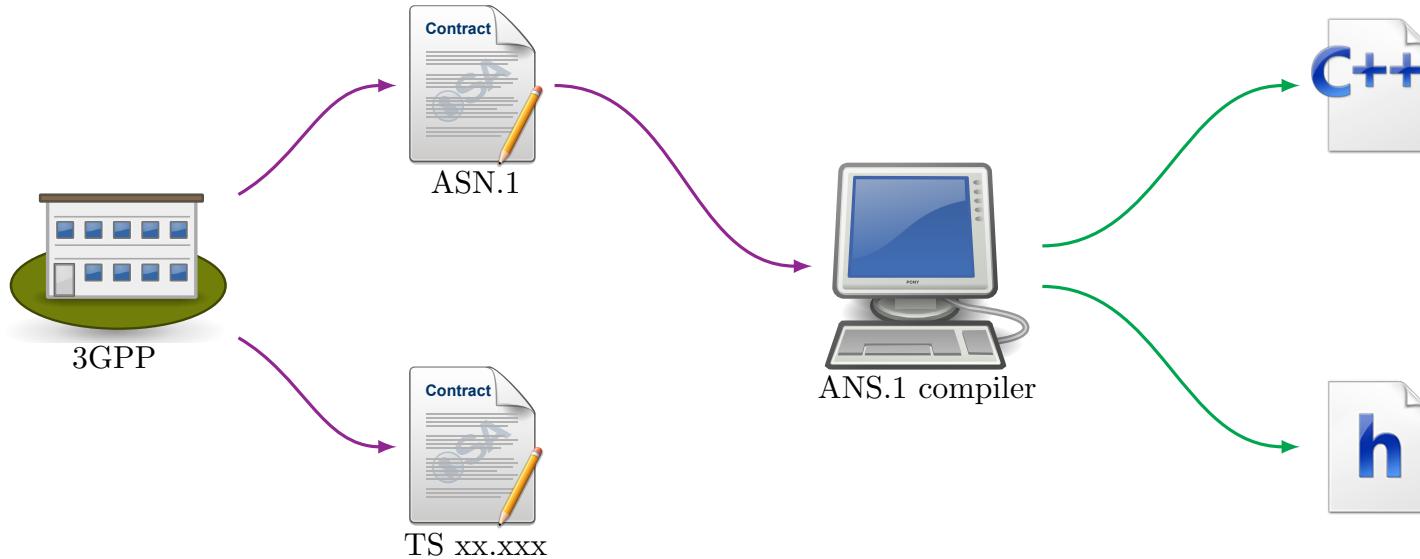
91 32.360241	0.0....	0.0.0.0	RRC	55 DownlinkDirectTransfer(cs-domain)(DTAP) (MM) Identity Request
92 32.422741	0.0....	0.0.0.0	RRC	64 UplinkDirectTransfer(cs-domain)(DTAP) (MM) Identity Response
93 32.540014	0.0....	0.0.0.0	RRC	77 DownlinkDirectTransfer(cs-domain)(DTAP) (MM) Location Updating Accept
94 32.602514	0.0....	0.0.0.0	RRC	54 UplinkDirectTransfer(cs-domain)(DTAP) (MM) TMSI Reallocation Complete
95 33.720080	0.0....	0.0.0.0	RRC	50 SignallingConnectionRelease(cs-domain)
message: downlinkDirectTransfer (5)				
downlinkDirectTransfer: r3 (0)				
r3				
downlinkDirectTransfer-r3				
rrc-TransactionIdentifier: 3				
cn-DomainIdentity: cs-domain (0)				
nas-Message: 050202f8012f461705f4083e45d44a0902f80102f81102f831				
GSM A-I/F DTAP - Location Updating Accept				
Protocol Discriminator: Mobility Management messages (5)				
.... 0101 = Protocol discriminator: Mobility Management messages (0x5)				
0000 = Skip Indicator: No indication of selected PLMN (0)				
00... = Sequence number: 0				
..00 0010 = DTAP Mobility Management Message Type: Location Updating Accept (0x02)				
Location Area Identification (LAI)				
Location Area Identification (LAI) - 208/10/12102				
Mobile Country Code (MCC): France (208)				
Mobile Network Code (MNC): Société Française du Radiotéléphone (10)				
Location Area Code (LAC): 0x2f46 (12102)				
Mobile Identity - TMSI/P-TMSI (0x83e45d4)				
Element ID: 0x17				
Length: 5				
1111 = Unused: 0xf				
.... 0.... = Odd/even indication: Even number of identity digits				
.... .100 = Mobile Identity Type: TMSI/P-TMSI/M-TMSI (4)				
TMSI/P-TMSI/M-TMSI/5G-TMSI: 138298836 (0x083e45d4)				
PLMN List Equivalent - 3 PLMNs				
Element ID: 0x4a				
Length: 9				
PLMN[1]				
Mobile Country Code (MCC): 208				
Mobile Network Code (MNC): 10				
PLMN[2]				
Mobile Country Code (MCC): 208				
90 05 02 02 f8 01 2f 46 17 05 f4 08 3e 45 d4 4a 09	/F.>E.	J.
10 02 f8 01 02 f8 11 02 f8 31	1

طرح مساله (ادامه)

یکی از چالش‌های شبکه‌های ارتباطی، تبادل اطلاعات بین سامانه‌های گوناگون و ناهمگون است، به گونه‌ای که دو نهاد درگیر در این تبادل، مستقل از نحوه نمایش اطلاعات و پیاده‌سازی سامانه، بتوانند به درک مشترکی از اطلاعات دست یابند.



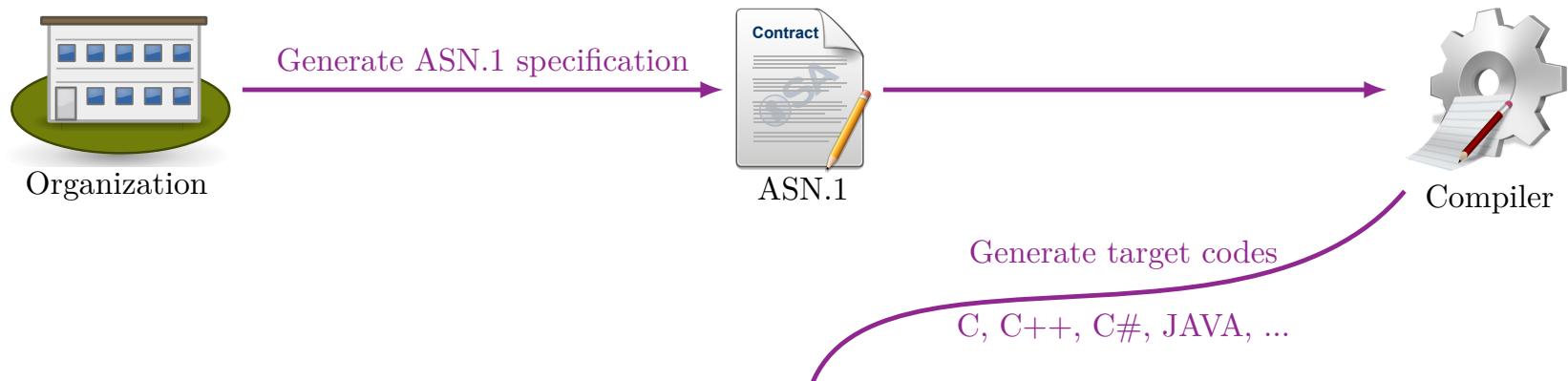
معرفی ASN.1



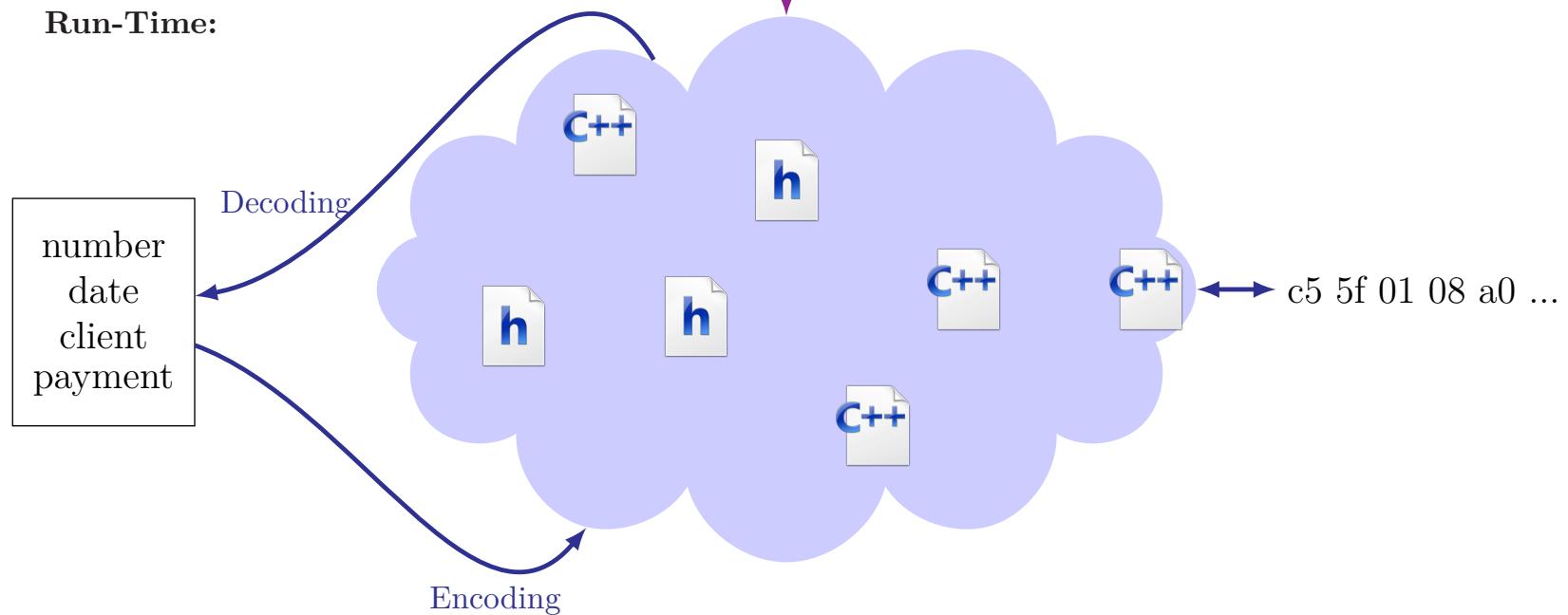
- اگر بخواهیم برای هر پروتکل، یک استاندارد در نحوه کدگذاری و کدگشایی داشته باشیم، می‌بایست یک پیاده‌سازی مجزا صورت پذیرد که این یعنی افزایش بی‌رویه هزینه پیاده‌سازی.
- استاندارد (ASN.1) (Abstract Syntax Notation One) در واقع یک «زبان توصیف داده» است.
- توسعه‌ی این استاندارد که به صورت مشترک توسط (ITU-T) و International Organization for Standardization (ISO) انجام پذیرفته است، از سال ۱۹۸۱ آغاز شد. هدف غایی از طرح

این استاندارد، ارائه یک زبان توصیف برای پروتکل‌های مختلف بوده است.

Development Phase:



Run-Time:



- ✓ پیاده‌سازی پروتکل‌های 3GPP
- ✓ پروتکل‌های تبادل صوت و تصویر بر روی اینترنت نظری H.263
- ✓ پروتکل‌های امنیتی تبادل گواهینامه، تبادل امن پست الکترونیکی، تبادلات Asynchronous Transfer Mode (ATM) و Kerberos
- ✓ پیاده‌سازی بسیاری از سامانه‌های مخابرات رادیویی نظری Worldwide Interoperability for Microwave Access (WiMAX) و، Wireless Fidelity (Wi-Fi)
- ✓ پروتکل‌های سامانه‌های ITS (Intelligent Transportation System) نظری Cooperative Awareness
- FAST Networking and Decentralized Environmental Notification (DENM)، Messaging (CAM) و Transfer Protocol (FNTCP) FAST Service Advertisement Protocol (FSAP)
- ✓ پیاده‌سازی پروتکل‌های Radio Frequency Identification (RFID) و حتی کارت هوشمند نظری Sub-

Wireless Identifier, Universal Subscriber Identity Module (USIM), Subscriber Identity Module (SIM)

... و Communication Module (WIM)

X.509 گواهینامه‌های ✓

مثال ۳

فرض کنید که میزبان A در شبکه، قصد دارد تا اطلاعات عرض، ارتفاع و عنوان یک تصویر را برای میزبان B در سوی دیگر، ارسال نماید. پر واضح است که این دو میبایست به این کار تحت یک پروتکل معین مبادرت ورزند، تا بدینسان بتوانند مفهوم پیامهای مبادله شده را درک نمایند. در [کد ۱](#) پروتکل مذکور توسط زبان ASN.1 توصیف گشته است.

```

1 ImageTest DEFINITIONS ::= 
2 BEGIN
3   Image ::= SEQUENCE {
4     width    INTEGER (1..4800), -- Width of the image
5     height   INTEGER,      -- Height of the image
6     title    UTF8String
7   }
8 END

```

یک پروتکل ارتباطی را در نظر بگیرید. مثلا فرض کنید که می خواهیم اطلاعات یک کارمند نظیر نام و نام خانوادگی، تاریخ تولد، کدملی و سن را از طریق یک پروتکل ارتباطی بدست گیرنده برسانیم.

- پروتکل پیشنهادی خود را با زبان توصیفی ASN.1 بنویسید؟
- با استفاده از کامپایلر مجازی asn1c پروتکل مذکور را کامپایل کنید.
- یک برنامه با C++ بنویسید و در آن فرایندهای Encode و Decode را تست کنید.

نکته



این پروژه به صورت گروههای حداکثر دو نفری می‌تواند انجام شود.

اجازه دهید تا برای فهم هر چه بهتر این موضوع، کار را با ارائه یک مثال به پیش بریم. یک شرکت تولیدی را در نظر بگیرید که کالایی به نام X را تولید می‌کند. هر مشتری در شبکه ارتباطی متصل به این شرکت، می‌تواند تقاضای سفارش X را به ثبت رساند. در ثبت هر سفارش می‌بایست اطلاعات زیر به سمت شرکت ارسال گردد:

تعداد کالای مورد نظر. Order-number •

تاریخ دریافت سفارش. Date •

اطلاعات مربوط به مشتری از قبیل نام و آدرس او. Client •

روش پرداخت هزینه محصول مورد نظر. Payment-method •

همان‌طور که می‌دانید اطلاعات مشتریان به صورت آرایه‌ای از بایت‌ها ارسال می‌گردد. مثلاً:

c5 5f 01 08 a0 0b 10 10 14 c3 03 85 c5 cc 55

سوال مهمی که در این مثال برای هر طراح و پیاده‌ساز پروتکل‌های شبکه‌ای ممکن است پیش آید این است که چگونه می‌توان مشتریان مختلف با سامانه‌های گوناگون، به یک درک مشترک برسند؟ پاسخ این پرسش احتمالاً

واضح است. به نظر می‌رسد وجود یک استاندارد می‌تواند چاره کار باشد. به عبارت بهتر هر دو نهاد درگیر در پروتکل، باید به صورت دقیق بدانند که چند بایت برای هر یک از چهار عنصر یاد شده در نظر گرفته است. این عناصر به چه ترتیب و در چه ساختاری به سوی آن‌ها ارسال می‌شود.

روشن است که اگر بخواهیم برای هر پروتکل، یک استاندارد مشخص در نحوه کدگذاری، کدگشایی و توصیف ساختار داده‌ها داشته باشیم، می‌بایست برای هر پروتکل، یک پیاده‌سازی مجزا صورت پذیرد که این خود موجب افزایش بی‌رویه هزینه پیاده‌سازی می‌گردد. یکی از راه‌کارهای حل این چالش، تبعیت پروتکل‌های مختلف از یک استاندارد مشخص و معین است.

) Abstract Syntax Notation One (ASN.1) پاسخ‌گوی تمامی معضلاتی که مطرح شد، استانداردی به نام (Abstract Syntax Notation کوتاه‌نوشت است.

ASN.1 در واقع یک «زبان توصیف داده» است. از دیگر زبان‌های توصیف Data Description Language می‌توان به SQL اشاره کرد که در پایگاه داده‌ها به کار می‌رود.

توسعه‌ی این استاندارد که به صورت مشترک توسط ITU-T و ISO انجام پذیرفته است، از سال ۱۹۸۱ آغاز شد.

هدف غایی از طرح این استاندارد، ارائه یک زبان توصیف برای پروتکل‌های مختلف بوده است. خواهیم دید که استاندارد ASN.1 موجب می‌گردد تا تمامی نهادهای درگیر در یک شبکه، بتوانند مستقل از نحوه پیاده‌سازی پروتکل (زبان برنامه‌نویسی، سیستم‌عامل و ...)، به یک درک مشترک از اطلاعات تبادل شده برسند.

تصمیم‌گیری در مورد استفاده از ASN.1 همواره تصمیم مناسب و کارایی به شمار می‌آید. این تصمیم زمانی کاراتر می‌گردد که دریافته باشد که پروتکلی که قصد پیاده‌سازی آن را دارد از همان زمان طراحی با استاندارد ASN.1 طراحی شده است. طیف وسیعی از پروتکل‌های شبکه از این استاندارد تبعیت می‌کنند. به عنوان مثال می‌توان به موارد زیر اشاره نمود:

- اگر شما قصد پیاده‌سازی یکی از پروتکل‌های 3GPP نظیر

Transaction Ca-، Radio Resource Control (RRC)، Node-B Application Part (NBAP)، (RANAP)

Media Transfer Protocol، Mobile Application Part (MAP)، pabilities Application Part (TCAP)

، Intelligent Networking Application Part (INAP) ، CAMEL Application Part (CAP) ، (MTP)

X2 Application Protocol ، Radio Network Subsystem Application Part (RNSAP) ، ISDN User Part (ISUP)

S1 ، M3 Application Protocol (M3AP) ، M2 Application Protocol (M2AP) ، X2 Application Protocol (X2AP)

Customised Applications for Mobile networks Enhanced Logic ، Application Protocol (S1AP)

(CAMEL) و ... را دارد، به دلیل این که این پروتکل‌ها از همان لحظه نخست بر پایه ASN.1 توسعه یافته

است، استفاده از ASN.1 در این زمینه قطعاً کارا خواهد بود.

• پروتکل‌های تبادل صوت و تصویر بر روی اینترنت نظیر H.263، پروتکل‌های امنیتی تبادل گواهینامه، تبادل

امن پست الکترونیکی، تبادلات ATM و Kerberos نیز بر طبق استاندارد ASN.1 پیاده‌سازی شده است.

• بسیاری از سامانه‌های مخابرات رادیویی نظیر شبکه‌های تلفن همراه (UMTS و LTE که پیشتر ارائه شد)،

Wi-Fi و WiMAX و ...، نیز بر مبنای ASN.1 است.

• پروتکل‌های سامانه‌های Intelligent Transportation System (ITS) نظیر CAM و DENM و FNTP و FSAP

نیز بر مبنای ASN.1 است.

- گستره و ناهمگونی بسیار زیاد در RFID ها و سامانه هایی که در آن از RFID استفاده شده است، راه چاره ای جز استفاده از ASN.1 در این نوع از سامانه ها نخواهیم داشت. این گستره استفاده حتی کارت هوشمند نظیر SIM، USIM، WIM و ... را نیز در بر می گیرد.
- استاندارد ASN.1 نقش بی بدیلی در دنیای سامانه های امنیتی ایفا می کند. به عنوان مثال استاندارد X.509 از ASN.1 استفاده می کند، و یا به عنوان مثالی دیگر Cryptographic Message Syntax (CMS) که توسط Internet Engineering Task Force (IETF) در RFC 5652 استاندارد شده است، نیز از ASN.1 استفاده می کند. لازم به ذکر است که CMS به منظور رمزگذاری، احراز اصالت، امضای الکترونیکی و نحوه کپسوله بندی داده ها را مشخص می نماید.
- در مدل OSI برای تبادل داده بین لایه های شش و هفت (یعنی لایه های Application و Presentation). در واقع ISO قید کرده که تمام داده های مبادله شده بین این دو لایه باید با استفاده از یک کد ASN1 توصیف

شود [۶].

البته کاربردهای استاندارد ASN.1 بسیار فراتر از مواردی است که بیان شد. از پروتکل‌های مورد استفاده در صنایع هوایپیمایی و فضایی گرفته تا پروتکل‌های مطرح در صنعت، همه و همه از این استاندارد تبعیت می‌کنند.

تاریخچه

Consultative Committee for International ASN.1 را که از آن با عنوان X.409 یاد می‌شود، در سال ۱۹۸۸ در CCITT (Telephony and Telegraphy) ایجاد کرد. در سال ۱۹۸۴ بعد از چهار سال تلاش ارائه داد. در حوالی سال ۱۹۸۸ نسخه جدیدی از این استاندارد با همکاری CCITT و ISO تحت عنوان X.208 (برای CCITT در سال ۱۹۸۸) و ISO (برای ISO در سال ۱۹۹۰) ارائه شد. این دو نهاد بار دیگر در سال ۱۹۹۴، با همکاری یکدیگر یک نسخه دیگر از ASN.1 را منتشر نمودند. در سال ۱۹۹۳، با تغییر نام CCITT به ITU-T، استانداردهای ASN.1 نیز از آن به بعد با نام ITU-T منتشر گشت. استانداردهای ۱۹۹۴ دو نهاد ISO و ITU-T در [جدول ۱](#) ارائه شده است.

جدول ۱: سری استانداردهای ISO و ITU-T برای ASN.1 در سال ۱۹۹۴.

ITU-T X.680	ISO/IEC 8824-1
ITU-T X.681	ISO/IEC 8824-2
ITU-T X.682	ISO/IEC 8824-3
ITU-T X.683	ISO/IEC 8824-4
ITU-T X.690	ISO/IEC 8825-1
ITU-T X.691	ISO/IEC 8825-2

بعدها در سال ۲۰۰۲ اصلاحات جزیی بر روی ASN.1 سال ۱۹۹۴ اعمال گشت. استانداردهای سری X.680 بار دیگر در سال ۲۰۱۵ مورد تصحیح قرار گرفت. عدد ۱ در انتهای نام ASN.1 برای این اضافه شده که نسخه‌های بعدی را بتوان با شماره‌های بالاتر نام‌گذاری کرد. با این حال، تاکنون چنین اتفاقی نیفتاده است.

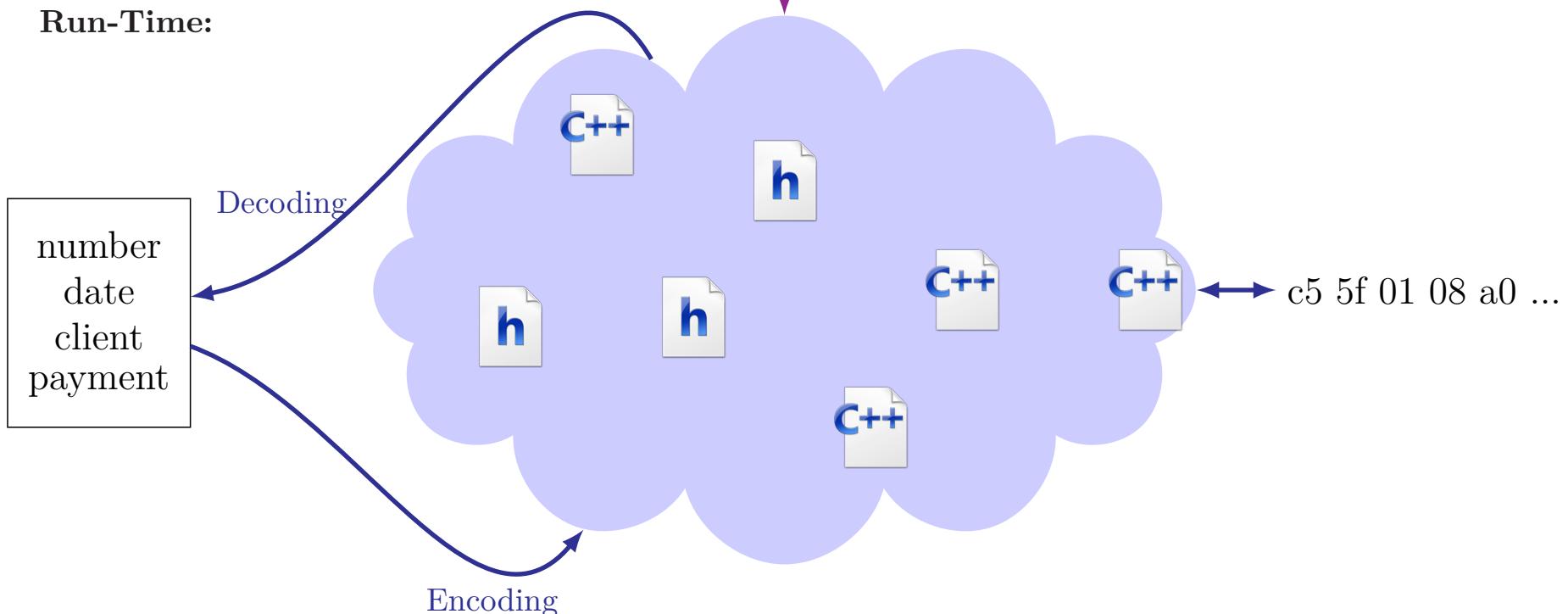
نحوه به کارگیری استاندارد ASN.1

در این بخش بدین پرسش پاسخ خواهیم داد که چگونه می‌توان از ASN.1، برای توصیف و پیاده‌سازی یک پروتکل استفاده نمود. منظور از پیاده‌سازی، مجموعه‌ای از کدها (مثلاً به زبان C) است که داده‌ی مورد نظر برای مبادله را در سمت فرستنده کدگذاری کرده و در سمت دیگر کدگشایی کند. مزیت بزرگ ASN.1 این است که از قبل کامپایلرهایی وجود دارد که تولید این کدها را به طور خودکار انجام می‌دهند. [شکل ۲](#) این روند را به زیبایی نشان می‌دهد.

Development Phase:



Run-Time:



برای به کارگیری ASN.1، لازم است دو گام برداشته شود:

گام اول نخستین گام برای به کارگیری استاندارد ASN.1، توصیف ساختار داده مورد استفاده توسط زبان توصیفی ASN.1 است.

گام دوم در گام دوم نیاز به استفاده از کامپایلرهای مخصوص ASN.1 داریم. در حقیقت کار اصلی این کامپایلرهای ASN.1 است. پر واضح است که انتظار تولید کدهای مورد نیاز برای عملیات کدگذاری و کدگشایی از روی فایل ASN.1 است. در حقیقت کار اصلی این کامپایلرهای ASN.1 در حالتی است که انتظار داریم صرف نظر از نحوه کامپایل و نوع کد تولیدی (اعم از کدهای C، C#، C++، JAVA و ...)، نتیجه حاصل از اجرای عملیات کدگذاری و کدگشایی یکسان باشد.

یک مثال ساده

کدهای ASN.1 را می‌توان بسان یک زبان سطح بالا برای توصیف انواع پروتکل‌ها در نظر گرفت. برای کسب یک درک اولیه از این زبان، از مثال ساده‌ی زیر استفاده می‌کنیم.

مثال ۴

فرض کنید که میزبان A در شبکه، قصد دارد تا اطلاعات عرض، ارتفاع و عنوان یک تصویر را برای میزبان B در سوی دیگر، ارسال نماید. پر واضح است که این دو میبایست به این کار تحت یک پروتکل معین مبادرت ورزند، تا بدمیسان بتوانند مفهوم پیامهای مبادله شده را درک نمایند. در کد ۱ پروتکل مذکور توسط زبان ASN.1 توصیف گشته است.

کد ۱ : کد ASN.1 برای توصیف اطلاعات یک تصویر

```
1 ImageTest DEFINITIONS ::=  
2 BEGIN  
3   Image ::= SEQUENCE {  
4     width   INTEGER (1..4800), -- Width of the image  
5     height  INTEGER,    -- Height of the image  
6     title   UTF8String  
7   }  
8 END
```

هر کد ASN.1 از تعدادی مازول تشکیل شده است. هر مازول خود در برگیرنده تعریف و توصیف ساختار

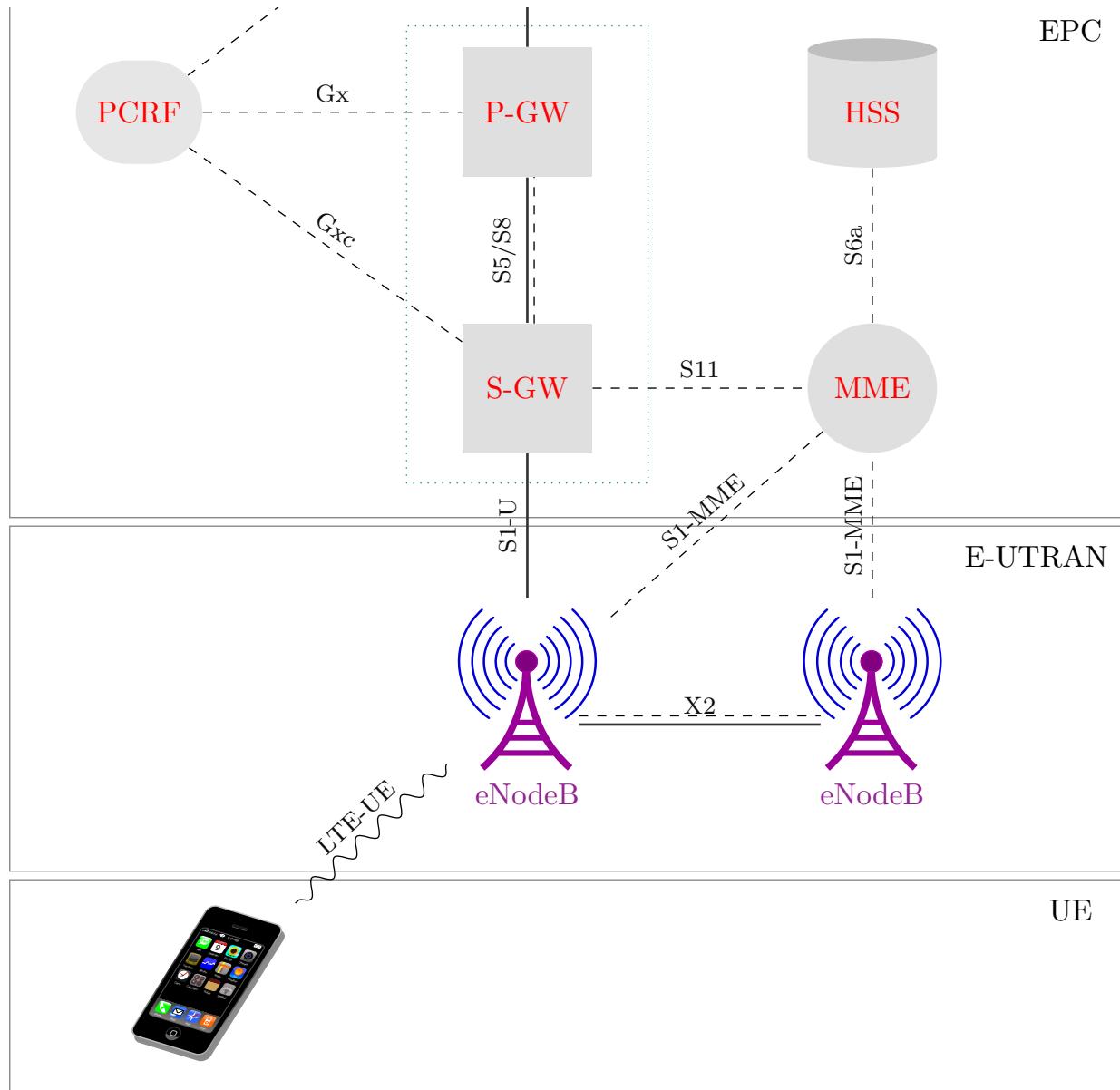
داده‌های مورد استفاده در آن پروتکل است. هر مازول در بین دو عبارت BEGIN و END محصور می‌گردد. به عنوان مثال در کد یاد شده تنها یک مازول، آن هم با نام ImageTest تعریف شده است. در ضمن به یاد داشته باشید که تمامی کاراکترهای بعد از علامت -، به عنوان comment در نظر گرفته می‌شود. در ASN.1، نام و نوع داده‌ها می‌بایست به صورت دقیق مشخص شود. در همین مثال، دو داده height و width با نوع INTEGER تعریف شده‌اند. از سوی دیگر، داده title بازه 1 تا 4800 محدود شده است. نیز از جنس UTF8String تعریف شده‌اند. SEQUENCE نوع داده‌ای پیشرفته‌است که خود می‌تواند انواع مختلف داده را در برگیرد.

اجزای اصلی تشکیل‌دهنده‌ی زبان ASN.1 عبارت‌اند از:

- نوع داده‌ها و مقادیر،
- زیرنوع‌ها،
- نام‌ها،
- مازول‌ها.

RAN پروٹوکول پسندیده

در کجای داستان قرار داریم؟



معماری پروتکلی در LTE مبتنی بر لایه‌بندی است.

- هر لایه وظیفه‌ای مشخص را برعهده دارد.
- هر لایه به صورت مستقل پیاده‌سازی شده،
- عملکرد درونی هر لایه می‌تواند بدون تاثیرگذاری بر بقیه لایه‌ها تغییر کند.

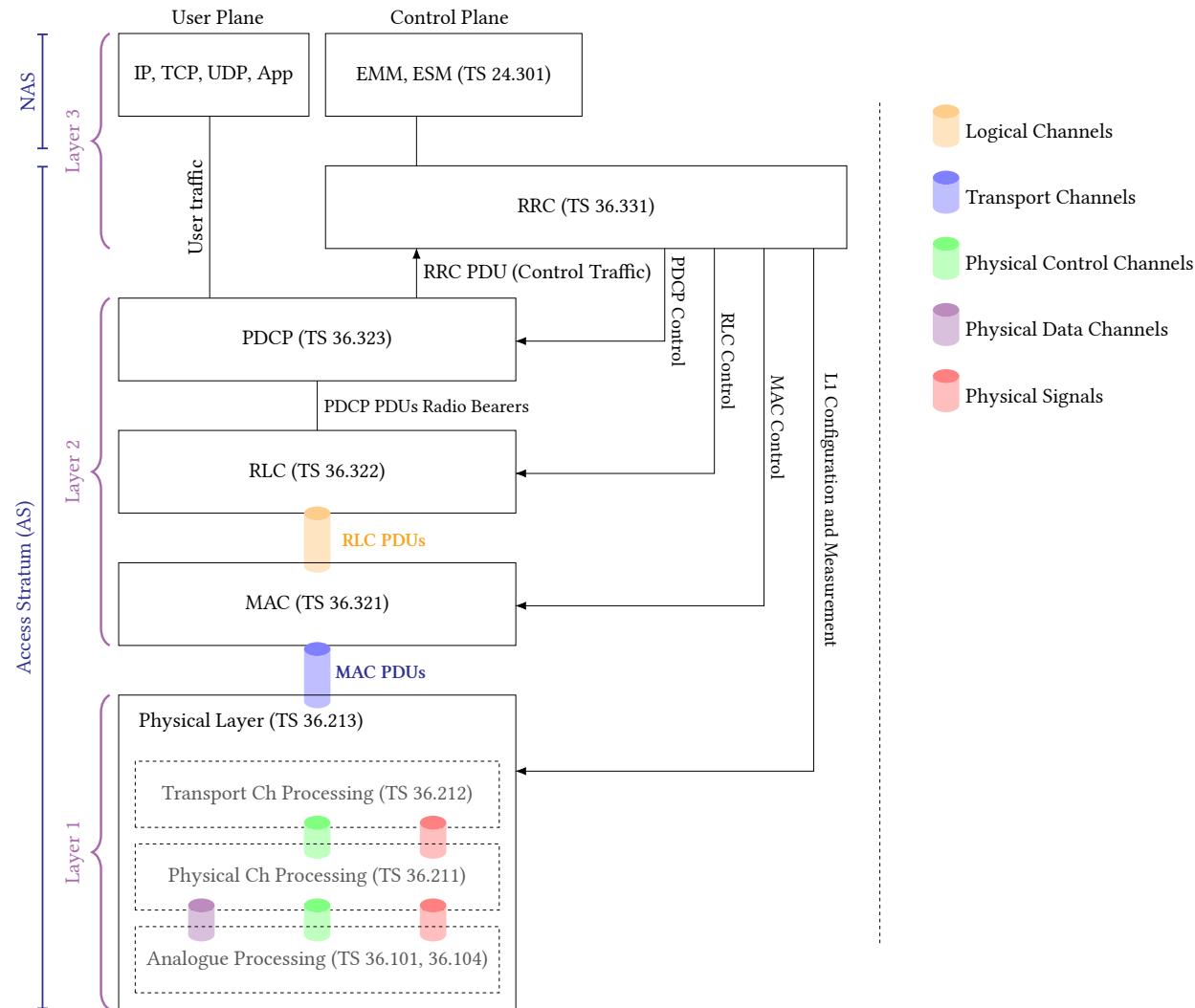
سه نوع سطح:

① سطح کنترلی (Control Plane)

② سطح مدیریتی (Management Plane)

③ سطح کاربر (User Plane)

لایه‌های پروتکلی در سطح کنترلی و سطح کاربر



در واژگان LTE به بسته‌های ورودی به یک لایه Service Data Unit (SDU) و به بسته‌های خارج شده

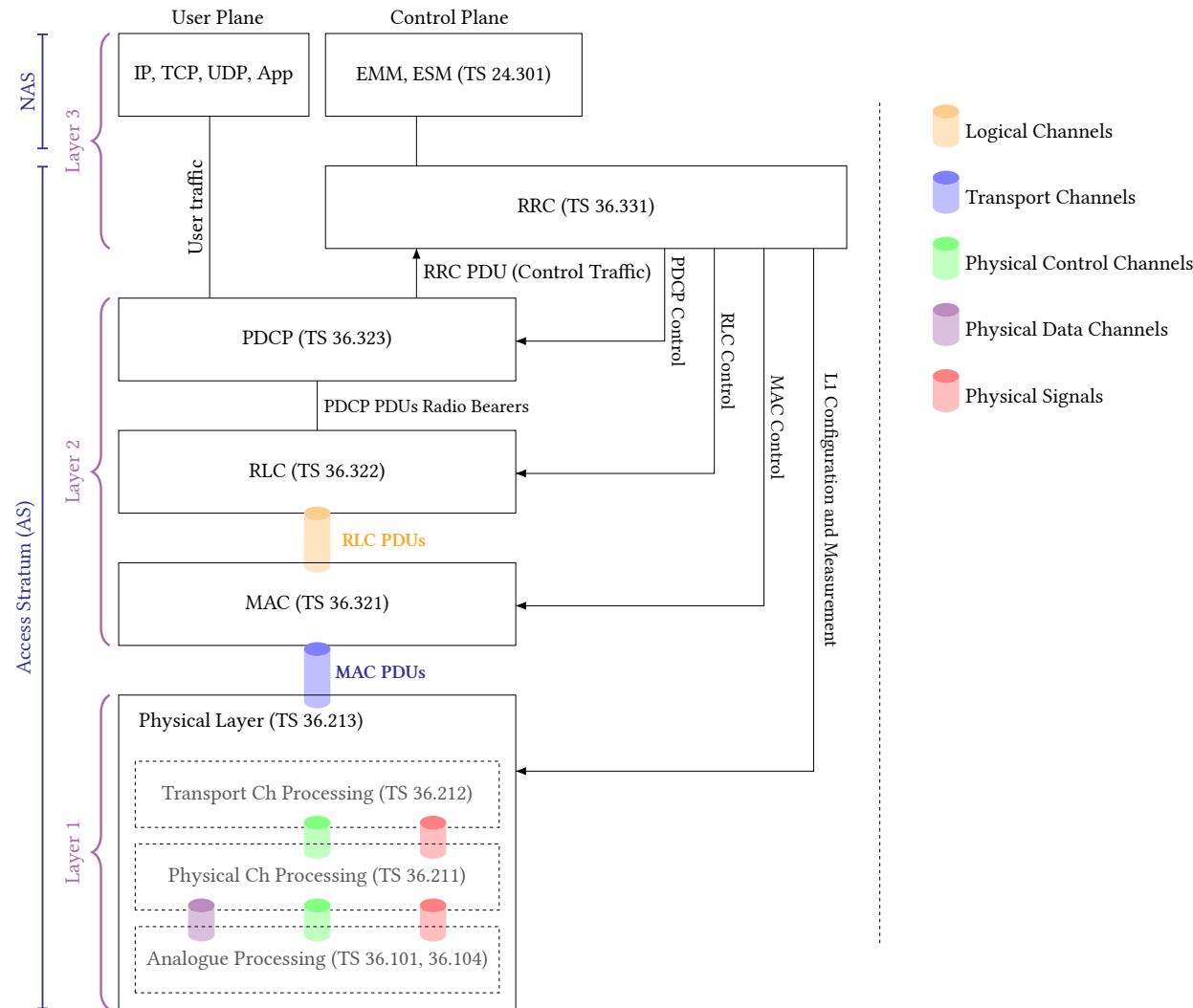
Protocol Data Unit (PDU) گفته می‌شود.

نمایی از معماری پروتکلی LTE در واسطه هوایی (بین UE و eNodeB) را از دیدگاه UE، در شکل اسلاید قبل نشان می‌دهد. همان‌طور که می‌دانید در شبکه‌های تلفن‌همراه برای هر کاربر دو نوع سطح ارتباطی به نام‌های سطح کاربر و سطح کنترلی در نظر گرفته می‌شود. در سطح کاربر، بسته‌های داده در لایه Packet Data Convergence کاربرد فرستنده، تولید می‌شود، و بعد از گذر از لایه انتقال و لایه شبکه وارد لایه EPS Mobility Management Protocol (PDCP) می‌شوند. در سوی دیگر، داده‌های تولید شده توسط لایه‌های RRC، EPS Session Management (ESM) و EMM در سطح کنترلی داده می‌شود. لایه RRC مسئولیت مبادله پیام‌های کنترلی بین UE و eNodeB را برعهده دارد. در ادامه راه، داده‌های سطح کاربر و سطح کنترلی به صورت مشترک از لایه‌های MAC، Radio Link Control (RLC)، PDCP و PDU گفته در واژگان LTE به بسته‌های ورودی به یک لایه اصطلاحاً SDU و به بسته‌های خارج شده از یک لایه RLC می‌شود. بدین ترتیب PDU لایه n ، SDU لایه $n+1$ خواهد شد. به عنوان مثال بسته‌های خروجی از لایه RLC را

RLC PDU نام می‌نہیم. RLC ها به عنوان ورودی لایه MAC SDU، MAC نام می‌گیرند. لایه MAC PDU نیز بعد از اجرای فرایندهایی بر روی MAC SDU ها آن‌ها را به لایه فیزیکی می‌دهد. PDU خارج شده از لایه n در برگیرنده SDU این لایه به اضافه سربسته اضافه شده به آن است.

$$\begin{aligned} \text{PDU Layer } n &= \text{SDU Layer } n + \text{Header Layer } n \\ &= \text{PDU Layer } n-1 + \text{Header Layer } n \end{aligned} \quad (5)$$

سطح Access Stratum (AS) در سطح کنترلی



بخش AS مسئولیت تمامی وظایف و عملکردهای مرتبط با واسط رادیویی و کنترل آن را برعهده دارد.

پشته پروتکلی نشان داده شده، به دو بخش Non Access Stratum (NAS) و AS تقسیم‌بندی می‌شود. بخش AS مسئولیت تمامی وظایف و عملکردهای مرتبط با واسط رادیویی و کنترل آن را بر عهده دارد. از سوی دیگر پروتکل‌های NAS، به منظور ارتباط مستقیم بین UE و هسته شبکه، بکار گرفته می‌شود. پروتکل‌های NAS، هیچ‌گونه تاثیر مستقیمی بر روی ایجاد و نگهداری Radio Access Bearer (RAB)‌ها بر عهده ندارد. به عبارت دیگر، پروتکل‌های NAS، نسبت به شبکه رادیویی شفاف هستند.

همان‌طور که می‌دانید پروتکل‌های شبکه مخابراتی از لحاظ معماری با ساختار پروتکلی شبکه رایانه‌ای اندکی متفاوت است. یک نگاشت تقریبی بین مدل پنج لایه‌ای شبکه رایانه‌ای [۷] و پشته پروتکلی شبکه LTE در [۸] نشان داده شده است. در ادامه به مروری مختصر بر روی هر یک از لایه‌های LTE، مبادرت می‌ورزیم.

- پروتکل‌های سطح NAS به منظور انتقال سیگنال‌دهی غیررادیویی بین UE و Mobility Management Entity (MME) بکار گرفته می‌شود.
- از دیدگاه پشتۀ پروتکل‌ها بالاترین لایه‌ها در سطح کنترلی را تشکیل می‌دهند.
- پروتکل‌های لایه NAS
 - ESM (EPS Session Management)
 - EMM (EPS Mobility Management)

- ☞ پروتکل ESM بیانگر وجود و یا عدم وجود ارتباط سیگنال دهی بین کاربر و شبکه است.
- ☞ وضعیت UE در این لایه توسط دو حالت ESM-IDLE و ESM-CONNECTED به طور کامل توصیف می‌گردد.

نکته



در برخی از مراجع برای نام این لایه عبارت Electronic Countermeasure (ECM) را به جای ESM برگزیدند.

پروتکل EMM در پشته پروتکلی UE و MME به منظور مدیریت تحرک‌پذیری UE قرار داده شد.

وظایف:

- توصیف حالت UE با یک دیاگرام حالت، به منظور تعیین اتصال و یا عدم اتصال UE به شبکه.
- نگهداری و مراقبت از ارتباط سیگنال‌دهی کاربر با شبکه در حین حرکت UE.
- رهگیری UE در زمانی که ارتباط سیگنال‌دهی بین کاربر ثبت‌شده و شبکه وجود ندارد.
- برقراری مجدد ارتباط سیگنال‌دهی در هنگامی که UE فعال می‌شود.

نکته



عملکرد و وظیفه این لایه، به مانند لایه (MM) در UMTS و GSM و یا General Packet Radio Service (GPRS) در GPRS Mobility Management (GMM) است.

بیشتر رویه‌هایی که در این لایه انجام می‌پذیرد، مربوط به مرحله اتصال UE به شبکه است.

- تخصیص .GUTI (Globally Unique Temporary Identity)
- احراز اصالت (Authentication)
- کنترل حالت امنیتی.
- رویه شناسایی (Identification)
- اطلاعات EMM

لایه RRC، را می‌توان قلب پشتۀ پروتکلی LTE نامید.

وظایف:

- تولید اطلاعات سامانه مرتبط با سطوح AS و NAS
- پی‌جویی
- مدیریت ارتباط‌های RRC
- مدیریت کلید

وظایف زیر بر عهده لایه PDCP، قرار داده شده است.

- ❶ فشرده سازی سربسته لایه Internet Protocol (IP) به منظور کمتر نمودن حجم بسته ارسالی، به جای سربسته SDU IP‌های رسیده از لایه‌های بالاتر، یک سربسته جدید با حجم کمتر جایگزین می‌کند.
- ❷ نگهداری دنباله ترتیبی PDU‌ها. این لایه موظف است که PDU‌های لایه‌های بالاتر را در صورت برقراری مجدد لایه‌های پایینی، به ترتیب به لایه‌های بالاتر تحويل دهد.
- ❸ عملیات رمزگذاری نیز در این لایه انجام می‌پذیرد.

لایه RLC در حالت کلی، وظیفه انتقال اطلاعات لایه‌های بالاتر به لایه‌های زیرین، را برعهده دارد.

لایه RLC دارای سه حالت عملکردی به صورت Unacknowledged Mode، Transparent Mode (TM)

و Acknowledged Mode (AM) و (UM) است.

وظایف:

- تصحیح خطا بر طبق Automatic Repeat Request (ARQ)، در حالت عملکردی AM.
- الحاق و بخشندی SDU‌های RLC برای حالت‌های UM و AM.
- تشخیص بسته‌های تکراری در حالت‌های UM و AM.
- تشخیص رخداد خطا در پروتکل و برقراری مجدد در حالت AM.
- مرتب‌سازی مجدد PDU‌های RLC در حالت UM و AM.
- بخشندی مجدد، البته تنها در حالت AM.

پروتکل لایه دسترسی به رسانه

مهم‌ترین وظیفه لایه دسترسی به رسانه و یا به صورت مختصر لایه MAC، نگاشت کanal منطقی به کanal ترابری است.

در لایه MAC، SDU‌های یک یا چند کanal منطقی، با یکدیگر همتافت گشته، و تحت بلوک انتقال، از طریق کanal ترابری، به سوی لایه فیزیکی می‌رود.

در پیوند فراسو نیز در سوی UE، عملیات و اتفاقگری اتفاق خواهد افتاد.

برخی از وظایف لایه MAC، به شرح زیر است.

- زمان‌بندی پویا.
- گزارش‌دهی از نحوه زمان‌بندی.
- تصحیح خطأ از طریق Hybrid Automatic Repeat Request (HARQ).
- اولویت‌بندی کanal منطقی.

پروتکل لایه فیزیکی

- ﴿ لایه فیزیکی تمامی داده‌های حمل شده توسط کانال ترابری را در واسط هوایی ارسال می‌کند.
- ﴿ عملیاتی نظیر تطابق پیوند، کنترل توان، جستجوی سلول و برخی اندازه‌گیری‌ها تحت نظرارت لایه RRC در لایه فیزیکی انجام می‌پذیرد.

- [1] 3GPP TS 23.122, “GSM (Phase 2+); UMTS; NAS functions related to MS in idle mode,” *Version 9.5.0 Release 9*, 2011.
- [2] ETSI TS 25.304 V8.7.0, “UMTS; UE procedures in idle mode and procedures for cell reselection in connected mode,” *3GPP TS 25.304 version 8.7.0 Release 8*, vol.0, 2009.
- [3] 3GPP TS 25.331, “UMTS; Radio Resource Control (RRC); Protocol specification,” *Version 7.22.0 Release 7*, 2012.
- [4] 3GPP TS 25.133, “UMTS; Rements for support of radio resource management (FDD),” *Version 7.15.0 Release 7*, 2009.
- [5] A. J. Menezes, P. C. Van Oorschot, and S. A. Vanstone. *Handbook of Applied Cryptography*. Discrete Mathematics and Its Applications, CRC Press, 1996.
- [6] O. Dubuisson and P. Fouquart. *ASN.1: Communication Between Heterogeneous Systems*.

Morgan Kaufmann, 2000.

- [7] J. F. Kurose and K. W. Ross. *Computer Networking: A Top-down Approach*. Always learning, Pearson, 2013.

فهرست اختصارات

Numbers

٣GPP ٣Rd Generation Partnership Project

A

AM Acknowledged Mode

ARQ Automatic Repeat Request

AS Access Stratum

ASN.1 Abstract Syntax Notation One

ATM Asynchronous Transfer Mode

B

BCCH Broadcast Control Channel

C

CAM Cooperative Awareness Messaging

CAMEL Customised Applications for Mobile networks Enhanced Logic

CAP CAMEL Application Part

CCCH Common Control Channel

CCITT Consultative Committee for International Telephony and Telegraphy

CMS Cryptographic Message Syntax

CPICH Common Pilot Channel

D

DENM Decentralized Environmental Notification

E

ECM	Electronic Countermeasure
EHPLMN	Equivalent HPLMN
EMM	EPS Mobility Management
eNodeB	Evolved NodeB
EPLMN	Equivalent PLMN
ESM	EPS Session Management
E-UTRAN	Evolved Universal Terrestrial Radio Access Network

F

FDD	Frequency Division Duplexing
FNTP	FAST Networking and Transfer Protocol
FPLMN	ForbiddenPLMN
FSAP	FAST Service Advertisement Protocol

G

GMM	GPRS Mobility Management
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communication

GUTI Globally Unique Temporary Identity

H

HARQ Hybrid Automatic Repeat Request

HPLMN Home PLMN

I

IETF Internet Engineering Task Force

IMSI International Mobile Subscriber Identity

INAP Intelligent Networking Application Part

IP	Internet Protocol
ISO	International Organization for Standardization
ISUP	ISDN User Part
ITS	Intelligent Transportation System
ITU-T	ITU Standardization
L	
LA	Location Area
LAC	Location Area Code
LAI	Location Area Identity

LR Location Register

LTE Long Term Evolution

M

MAP M Application Protocol

MAP M Application Protocol

MAC Medium Access Control

MAP Mobile Application Part

MCC Mobile Country Code

MIB Master Information Block

MM Mobility Management

MME Mobility Management Entity

MNC Mobile Network Code

MP Mandatory Present

MTP Media Transfer Protocol

N

NAS Non Access Stratum

NBAP Node-B Application Part

P

PCCH	Paging Control Channel
PDCP	Packet Data Convergence Protocol
PDU	Protocol Data Unit
PLMN	Public Land Mobile Network

R

RAB	Radio Access Bearer
RACH	Random Access Channel
RAN	Radio Access Network

RANAP	Radio Access Network Application Part
RF	Radio Frequency
RFID	Radio Frequency Identification
RLC	Radio Link Control
RNSAP	Radio Network Subsystem Application Part
RPLMN	Registered Public Land Mobile Network
RRC	Radio Resource Control
RSCP	Received Signal Code Power
RSRP	Reference Signal Recieved Power
RSRQ	Reference Signal Recieved Quality
RSSI	Received Signal Strength Indication

S

S \ AP	S \ Application Protocol
SDU	Service Data Unit
SIB	System Information Block
SIM	Subscriber Identity Module
SINR	Signal Interference Noise Ratio
SMS	Short Message Service

T

TAC	Tracking Area Code
TCAP	Transaction Capabilities Application Part
TDD	Time Division Duplex
TM	Transparent Mode
TMSI	Temporary Mobile Subscriber

U

UE	User Equipment
UICC	Universal Integrated Circuit Card

UM Unacknowledged Mode

UMTS Universal Mobile Telecommunications System

USIM Universal Subscriber Identity Module

V

VLR Visitor Location Register

VPLMN Visited PLMN

W

Wi-Fi	Wireless Fidelity
WIM	Wireless Identification Module
WiMAX	Worldwide Interoperability for Microwave Access

X

XAP	X Application Protocol
-----------	------------------------

واژه‌نامه انگلیسی به فارسی

B

Bandwidth پهنای باند Access Network شبکه دسترسی

Barred Cell سلوی مسدودشده Authentication احراز اصالت

Broadcast همه‌پخشی Air Interface واسطه هوایی

Application Layer لایه کاربرد

C

Architecture معماری

Call تماس

Coverage	پوشش	Call Maintenance	نگهداری تماس
Common Control Channel	کanal کنترلی عمومی	Call Release	آزادسازی تماس
Computer Network	شبکه رایانه‌ای	Call Setup	برقراری تماس
Concatenation	الحاق	Camping On Cell	اردو زدن بر سلول
Connected Mode	مُدمتصل	Cell	سلول
Constraint	قید	Cell Identity	شناسه سلول
Control Plane	سطح کنترلی	Cell Reselection	بازانتخاب سلول
Core Network	هسته شبکه	Cell Search	جستجوی سلول
		Cell Selection	انتخاب سلول
		Certificate	گواهینامه
		Client	مشتری

Encoding	کدگذاری	D
Encryption	رمزگذاری	پایگاه داده
Entity	نهاد	کدگشایی
Equivalent PLMN	شبکه معادل	کanal اختصاصی
Error Correction	تصحیح خطأ	واتافتگری
		پیوند فروسو
F		DRX Cycle DRX دوره
Forwarding	جلورانی	
Frame	قاب	E
		پست الکترونیکی
	Email	

Idle Mode	H مُد بیکار
Information Element	عنصر اطلاعات
Inter-frequency	اندازه‌گیری بین فرکانسی
Measurement	نامهمگون
Inter-system	اندازه‌گیری بین سامانه‌ای
Measurement	هیسترزیس
Intra-frequency	اندازه‌گیری درون فرکانسی
Measurement	میزبان
	I
	Identification
	Identity
	شناسایی
	شناسه
	واگذاری
	سربسته
	Handover
	Header

K بروزرسانی منطقه مکانی .. Location Area Update

توافق کلید .. Key Agreement بروزرسانی مکان .. Location Update

برقراری کلید .. Key Establishment کanal منطقی .. Logical Channel

مدیریت کلید .. Key Management ..

تبدال کلید .. Key Transport ..

سطح مدیریتی .. Management Plane

L اندازه‌گیری .. Measurement

تطابق پیوند .. Link Adaption لایه دسترسی به رسانه .. Medium Access Layer

مکان .. Location پیام .. Message

منطقه مکانی .. Location Area چند رسانه‌ای .. Multimedia

Optional	اختیاری Mobility	تحرک پذیری
	MobilityManagement	مدیریت تحرک پذیری
P		
	N	
Paging	پی جویی	
Physical Layer	لایه فیزیکی Neighbor Cell	سلول همسایه لایه شبکه
PLMN Selection	نتخاب شبکه Network Layer	لایه شبکه
Power Control	کنترل توان Normal Service	خدمات بهنجار
Procedure	رویه	
Protocol Stack	پشته پروتکلی	O
		عملگر
	Operator	

Routing Area منطقه مسیریابی Q

کیفیت خدمت Quality of Service

S

Scheduling زمانبندی R

Scheduling Block بلوک زمانبندی منبع رادیویی Radio Resource

Segmentation بخشبندی دسترسی تصادفی Random Access

Selected PLMN شبکه انتخاب شده توان دریافتی Received Power

Sequence Number دنباله ترتیبی ثبت شده Registered

Serving Cell سلول خدمتگزار شبکه ثبت شده Registered PLMN

Suitable Cell سلول مناسب فراغردی Roaming

Tracking	رهگیری	System Information	اطلاعات سامانه
Tracking Area	ناحیه رهگیری	Signaling	سیگنال دهی
Transmitted Power	توان ارسالی	Signalling	سیگنال دهی
Transparent	شفاف	Smart Card	کارت هوشمند
Transport Block	بلوک انتقال	State	حالت
Transport Channel	کanal ترابری	State Machine	ماشین حالت
Transport Layer	لایه انتقال			

T

U	شبکه مخابراتی
Uplink	پیوند فراسو
	Time Slot
	شیار زمانی

کاربر

User

سطح کاربر

واژه‌نامه فارسی به انگلیسی

PLMN Selection	انتخاب شبکه	۱
Measurement	اندازه‌گیری	آزادسازی تماس
Inter-system	اندازه‌گیری بین سامانه‌ای	احراز اصالت
Measurement Optional	Authentication	اختیاری
Inter-frequency	اندازه‌گیری بین فرکانسی	اردو زدن بر سلول
Measurement System Information	Camping On Cell	اطلاعات سامانه
Intra-frequency	اندازه‌گیری درون فرکانسی	الحق
Measurement Cell Selection	Concatenation	انتخاب سلول

ب

پ

Database	پایگاه داده	Cell Reselection بازنخاب سلول
Email	پست الکترونیکی	Segmentation بخش‌بندی
Protocol Stack	پشته پروتکلی	Call Setup برقراری تماس
Coverage	پوشش	Key Establishment برقراری کلید
Bandwidth	پهنه‌باند	Location Update بروزرسانی مکان
Message	پیام	Location Area Update بروزرسانی منطقه مکانی
Paging	پی‌جویی	Transport Block بلوک انتقال
Uplink	پیوند فراسو	Scheduling Block بلوک زمان‌بندی

پیوند فروسو Received Power Downlink توان دریافتی

ش

تبادل کلید Registered Key Transport ثبت شده ..

تحرك پذيرى Mobility ..

تصحیح خط Error Correction ..

ج

تطابق پیوند Cell Search جستجوی سلول ..

Link Adaption ..

تماس Forwarding جلوه رانی ..

Call ..

توافق کلید Key Agreement ..

توان ارسالی Transmitted Power ..

ج

د

Random Access	دسترسی تصادفی	Multimedia
Sequence Number	دنباله ترتیبی	
DRX Cycle	دوره DRX	

ح

حالت

ر

Encryption	رمزگذاری	
Procedure	رویه	
Tracking	رهگیری	خدمات بهنجار

خ

Barred Cell	سلول مسدودشده ..	ز
Suitable Cell	سلول مناسب ..	زمانبندی ..
Neighbor Cell	سلول همسایه ..	
Signalling	سیگنال دهنده ..	
	Header	سربرسته ..
	User Plane	سطح کاربر ..
Selected PLMN	شبکه انتخاب شده ..	سطح کنترلی ..
Registered PLMN	شبکه ثبت شده ..	سطح مدیریتی ..
Access Network	شبکه دسترسی ..	سلول ..
Computer Network	شبکه رایانه ای ..	سلول خدمتگزار ..
	Serving Cell	

Information Element	عنصر اطلاعات	Telecommunication Network	شبکه مخابراتی
		Equivalent PLMN	شبکه معادل
		Transparent	شفاف
	ف	Identification	شناسایی
Roaming	فراگردی	Identity	شناسه
		Cell Identity	شناسه سلول
	ق	Time Slot	شیار زمانی
Frame	قاب		
Constraint	قيد		ع
		Operator	عملگر

گ	User کاربر
Certificate گواهینامه	Smart Card کارت هوشمند
	Dedicated Channel کanal اختصاصی
	Transport Channel کanal ترابری
ل	Common Control Channel . کanal کنترلی عمومی .
Transport Layer	Logical Channel کanal منطقی
Medium Access Layer	Encoding کدگذاری
Network Layer	Decoding کدگشایی
Physical Layer	Power Control کنترل توان
Application Layer	Quality of Service کیفیت خدمت

Radio Resource	منبع رادیویی ..
Routing Area	منطقه مسیریابی ..
Location Area	منطقه مکانی ..
Host	میزبان ..
	State Machine
	Idle Mode
	Connected Mode
	مدیریت حرکت پذیری ..
Tracking Area	ناحیه رهگیری ..
Heterogeneous	ناهمگون ..
Call Maintenance	نگهداری تماس ..
Entity	نهاد ..
	Location
	مکان ..
	مشتری ..
	Client
Key Management	مدیریت کلید ..
MobilityManagement	مدیریت حرکت پذیری ..
	ن
Architecture	معماری ..
	م ..

۹

واتافتگری

واسط هوایی

واگذاری

۵

هسته شبکه

همه پخشی

هیستریزیس