UNIVERZITET U SARAJEVU
ELEKTROTEHNIČKI FAKULTET
ODSJEK ZA TELEKOMUNIKACIJE

Analiza signalizacije na zračnom sučelju 4G mreže pri realizaciji servisa prenosa podataka

Hasanbegović Selma, 1574/17753
Mahovac Nerman, 1575/17919
Velić Nejra, 1634/17313

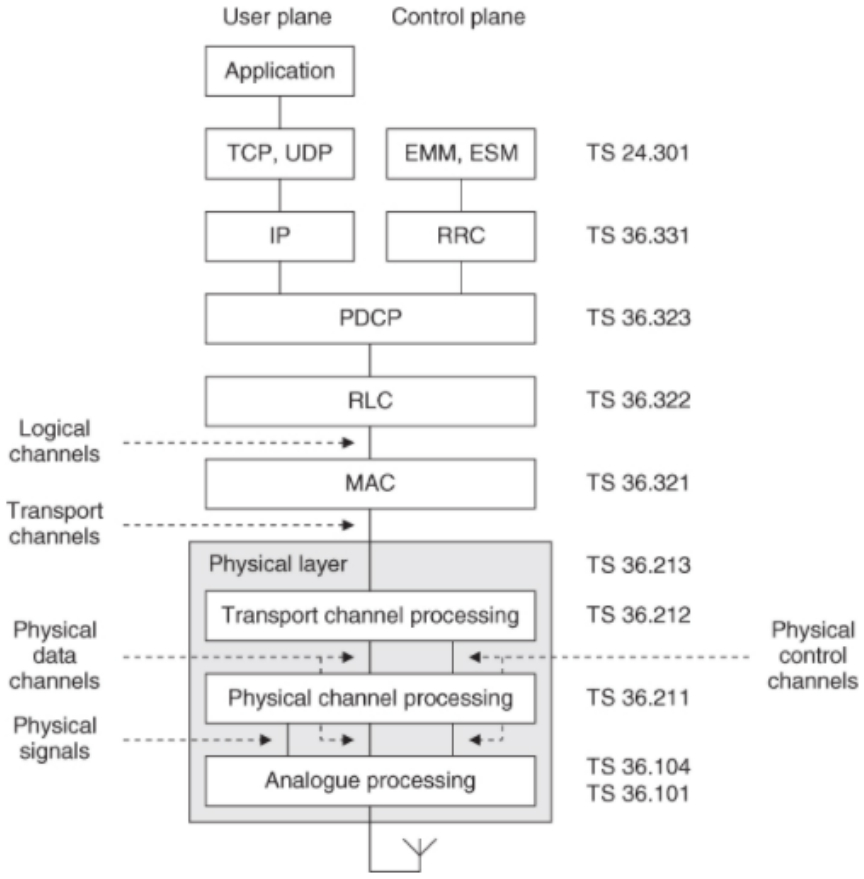
Sarajevo, 2021. godina

Sadržaj

Popis slika

1. Pregled protokola na zračnom sučelju 4G mreže

Protokoli zračnog sučelja 4G mreže prikazani su na slici 1.1, zajedno sa označenim dijelovima između protokola gdje se poruke prenose različitim kanalima. Unutar korisničke ravni protokoli TCP (engl. *Transmission Control Protocol*), UDP (engl. *User Datagram Protocol*) i IP (engl. *Internet Protocol*) procesiraju podatke od i prema aplikaciji, dok u kontrolnoj ravni RRC protokol vrši signalizaciju između eNodeB i UE. U oba slučaja, protokoli PDCP, RLC i MAC procesiraju pakete prije/nakon prolaska kroz fizički sloj [1]. NAS protokol se koristi u kontrolnoj ravni za slanje signalizacijskih poruka između UE i MME (engl. *Mobility Management Entity*).



Slika 1.1: Protokoli zračnog sučelja 4G mreže

Dakle, protokoli zračnog sučelja 4G mreže su:

- MAC (engl. *Medium Access Control*)
- RLC (engl. *Radio Link Control*)
- PDCP (engl. *Packet Data Convergence Protocol*)
- RRC (engl. *Radio Resource Control*)
- NAS (engl. *Non-access stratum*)

U nastavku će svaki od navedenih protokola biti detaljno objašnjen, dok protokoli TCP, UDP i IP se dalje neće detaljno razmatrati.

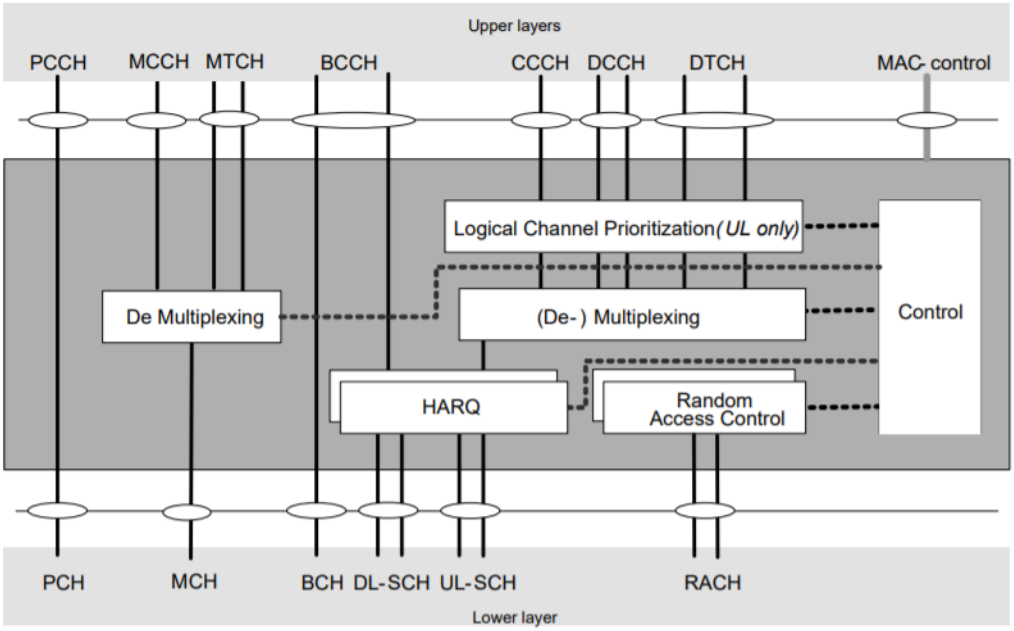
1.1. MAC protokol

MAC (engl. *Medium Access Control*) protokol predstavlja podsloj sloja 2, a obavlja sljedeće funkcije [2]:

- Mapiranje između logičkih i transportnih kanala
- Multipleksiranje/demultipleksiranje jednog ili više logičkih kanala u/iz transportnih blokova dostavljenih do/od fizičkog sloja putem transportnih kanala
- Ispravljanje grešaka korištenjem HARQ
- Izvještavanja o informacijama o raspoređivanju
- QoS menadžment
- Prioritetizacija logičkih kanala
- Odabir formata za transport
- Rukovanje prioritetima između logičkih kanala jednog korisnika
- Rukovanje prioritetima između korisnika u smislu dinamičkog raspoređivanja

MAC athitektura je prikazana na slici 1.2, i čine je sljedeći entiteti:

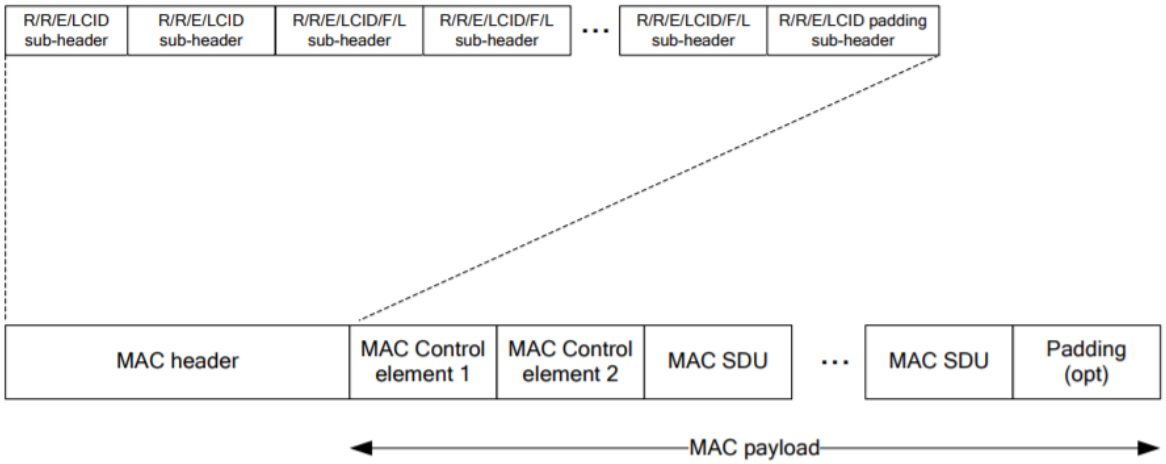
- **Entitet za multipleksiranje i demultipleksiranje** - multipleksiranje/demultipleksiranje podataka iz više logičkih kanala u/iz jednog transportnog kanala.
- **Entitet za prioritetizaciju logičkih kanala** - nalaže entitetu za multipleksiranje/demultipleksiranje da generiše MAC PDU-ove iz MAC SDU-ova (engl. *Service Data Units*), te odlučuje koliko podataka treba uključiti u MAC PDU iz svakog konfigurisanog logičkog kanala.



Slika 1.2: Pregled MAC strukture na strani korisnika

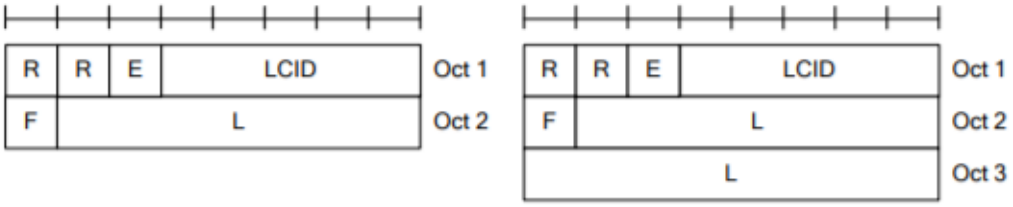
- **Kontrolni entitet** - zadužen za različite funkcije, kao na primjer DRX, zahtjeve za resursima, poravnavanje vremena za uplink i slično.
- **HARQ entitet** - Omogućava prenos i prijem transportnih blokova, retransmisiju blokova,kombinovanje i dekodiranje blokova, te, ukoliko je konfigurisano, slanje, prijem i obradu HARQ ACK/NACK poruka.

MAC PDU čini MAC header i MAC payload, kojeg čine MAC SDU-ovi (nula ili više), MAC kontrolni elemenat (nula ili više) i neobavezni padding elementi, što se može vidjeti na slici 1.3. Pri tome, i MAC header i MAC SDU su promjenljive veličine, dok MAC SDU uvijek dolaze nakon MAC kontrolnih elemenata. MAC header se sastoji od jednog ili više MAC PDU subheader-a, pri čemu svaki od njih može odgovarati MAC SDU, MAC kontrolnom ili padding elementu.

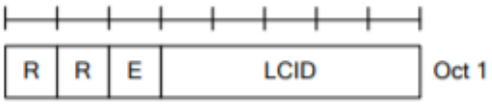


Slika 1.3: MAC PDU

MAC PDU subheader se, općenito, sastoji od 6 polja R/R/E/LCID/F/L (slika 1.4). Međutim, ukoliko je riječ o posljednjem subheader-u, o MAC kontrolnom elementu fiksne veličine ili o subheader-u koji odgovara padding elementu, subheader se sastoji od 4 polja R/R/E/LCID, a prikazan je na slici 1.5.



Slika 1.4: R/R/E/LCID/F/L MAC subheader: 2 okteta (lijevo); 3 okteta (desno)



Slika 1.5: R/R/E/LCID subheader

MAC PDU subheader-i unutar MAC header-a prate isti redoslijed kao i odgovarajući MAC SDU, MAC kontrolni elementi i padding elementi unutar MAC payload-a. Polja koja čine MAC PDU subheader su [3]:

- **R -** ***Reserved*** (1 bit) - rezervisani biti, postavljeni na vrijednost '0'
- **E -** ***Extension*** (1 bit) - ukoliko je postavljen na vrijednost '1' znači da unutar header-a postoji više subheader-a
- **LCID -** ***Logical Channel ID*** (5 bita) - šalje MAC CE zajedno sa ostalim informacijama
- **F -** ***Format*** (1 bit) - ukoliko je postavljen na vrijednost 1, subheader čine 3 okteta, u suprotnom 2 okteta
- **L -** ***Length*** (7 bita ili 15 bita) - označava dužinu MAC SDU u oktetima

1.2. RLC protokol

RLC (engl. *Radio Link Control*) je protokol sloja 2, a generalno obavlja kontrolu RLC konfiguracija. Neke od funkcija koje RLC podržava su [4]:

- Prenos PDU-ova viših slojeva
- Ipravljanje grešaka pomoću ARQ (samo za AM prenos podataka)
- Spajanje, segmentiranje i reasambliranje RLC SDU-ova (samo za UM i AM prenos podataka)

- Ponovna segmentacija RLC PDU-ova (samo za AM prenos podataka)
- Detekcija duplikata (samo za UM i AM prenos podataka)
- Odbacivanje RLC SDU-ova (samo za UM i AM prenos podataka)
- Ponovno uspostavljanje RLC-a
- Otkrivanje grešaka protokola (samo za AM prenos podataka)

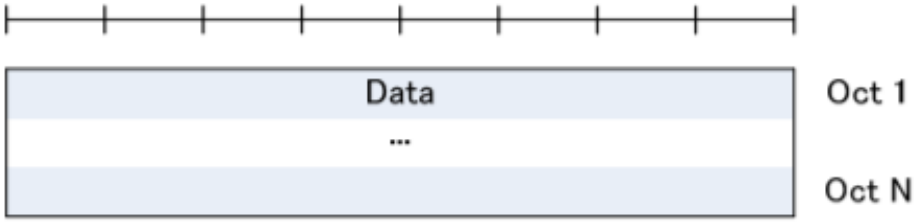
Navedene funkcije RLC protokola obavljaju RLC entiteti. Svaki RLC entitet može biti konfigurisan da vrši prenos podataka u nekom od sljedećih modova [4]:

- Transparentni mod (engl. *Transparent Mode*) (TM)
- Nepotrvđeni mod (engl. *Unacknowledged Mode*) (UM)
- Potvrđeni mod (engl. *Acknowledged Mode*) (AM)

RLC entitet, s obzirom na konfiguraciju i mod prenosa podataka, može biti TM RLC, UM RLC ili AM RLC entitet. Ukoliko je RLC entitet konfigurisan na eNode-B-u, onda postoji njegov *peer* RLC entitet na UE, i obrnuto.

RLC PDU-ovi mogu biti podatkovnog i kontrolnog tipa. RLC PDU-ovi podatkovnog tipa se mogu prenositi TM RLC, UM RLC i AM RLC entitetima za prenos PDU-uova viših slojeva, dok RLC PDU-ovi kontrolnog tipa se mogu prenositi samo AM RLC entitetima za izvršavanje ARQ procedura. U nastavku je dat prikaz PDU-a podatkovnog tipa za svaki mod prenosa podataka [4].

PDU podatkovnog tipa u transparentnom modu prenosa podataka (TMD PDU) ne sadrži RLC header, već samo payload, što se vidi na slici 1.6.



Slika 1.6: TMD PDU

Na slici 1.7 je prikazan PDU podatkovnog tipa u nepotvrđenom modu prenosa podataka (UMD PDU). UMD PDU se sastoji od header-a i payload polja. RLC header ima sljedeća polja:

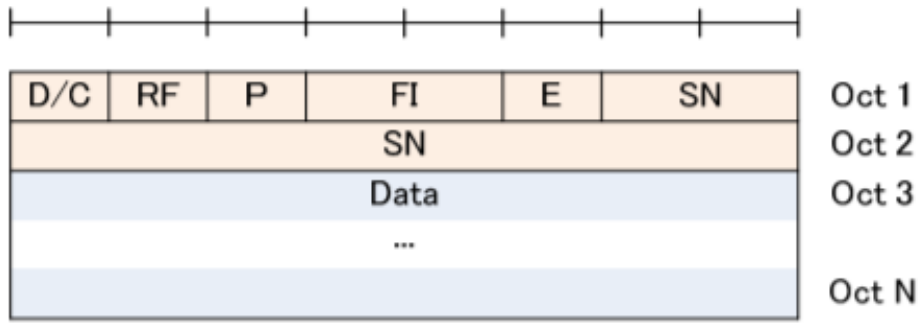
- **FI -** ***Framing Info*** (2 bita) - pokazuje da li je RLC SDU segmentiran na početku i/ili kraju podatkovnog polja. Tačnije, pokazuje da li prvi/posljednji oktet RLC PDU polja odgovara prvom/posljednjem oktetu RLC SDU polja, respektivno.
- **E -** ***Extension*** (1 bit) - označava da li slijedi podatkovno polje (vrijednost 0) ili set E polja (vrijednost 1)

Slika 1.7: UMD PDU (5 bit SN)

- **SN -** ***Sequence Number*** (5 ili 10 bita) - sekvencni broj koji odgovara pojedinom UMD PDU

PDU podatkovnog tipa u potvrđenom modu prenosa podataka (AMD PDU) je prikazan na slici 1.8, a čine ga header i podatkovno polje. Pored prethodno obrađenih polja unutar header-a, koja su zajednička sa UMD PDU-om (FI i E polje), header ima dodatna polja i to:

- **D/C -** ***Data/Control*** (1 bit) - označava da li je RLC PDU podatkovnog (vrijednost 1) ili kontrolnog (vrijednost 0) tipa
- **RF -** ***Re-segmentation Flag*** (1 bit) - pokazuje da li je AMD PDU segment (vrijendost 1) ili ne (vrijednost 0)
- **P -** ***Pooling*** (1 bit) - označava da li predajni AM RLC entitet zahtijeva izvještaj o statusu od njegovog peer AM RLC entiteta (vrijednost 1) ili ne (vrijednost 0)
- **SN -** ***Sequence Number*** (10 bita) - ukoliko je riječ o AMD PDU segmentu, vrijednost polja označava sekvencni broj AMD PDU iz kojeg je konstruisan



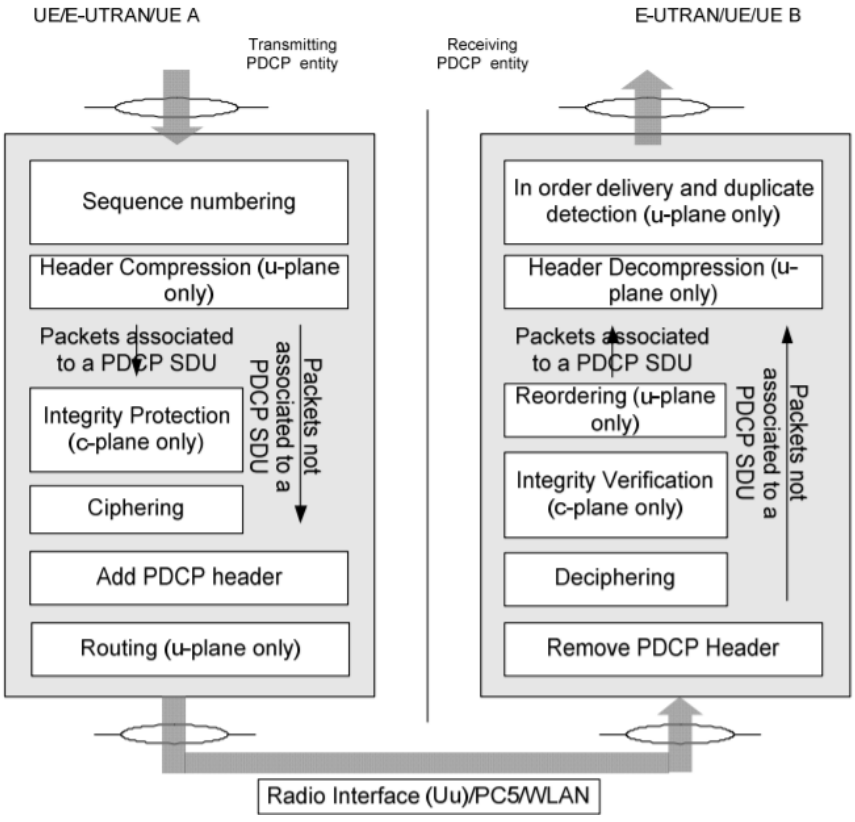
Slika 1.8: AMD PDU

1.3. PDCP protokol

PDCP (engl. *Packet Data Convergence Protocol*) obavlja sljedeće funkcije [5]:

- Kompresija i dekompresija header-a pomoću ROCH (engl. *Robust Header Compression*) protokola
- Prenos podataka (korisnička ili kontrolna ravan)
- Održavanje PDCP sekvencnog broja
- Šifriranje i dešifriranje podataka korisničke i kontrolne ravni
- Zaštita i verifikacija integriteta kontrolne ravni
- Rutiranje i preuređivanje
- Odbacivanje duplikata
- Odbacivanje na osnovu vremena

PDCP entiteti se nalaze unutar PDCP podsloja, a nekoliko PDCP entiteta se može definisati za jedan UE. Svaki PDCP entitet koji prenosi podatke korisničke ravni može biti konfigurisan da vrši kompresiju header-a pomoću ROCH protokola. Svaki PDCP entitet prenosi podatke jednog rado nosioca. U zavisnosti od radio nosioca čije podatke prenosi, PDCP entitet može biti pridružen podatkovnoj ili korisničkoj ravni [5].

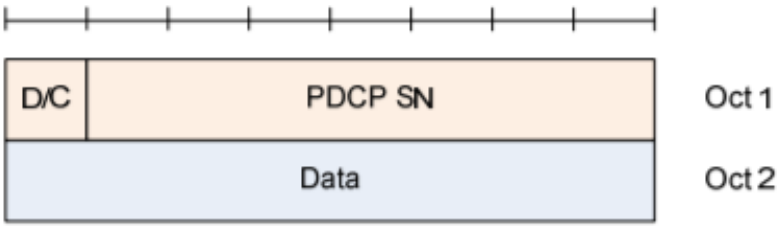


Slika 1.9: Funkcionalni pregled PDCP sloja

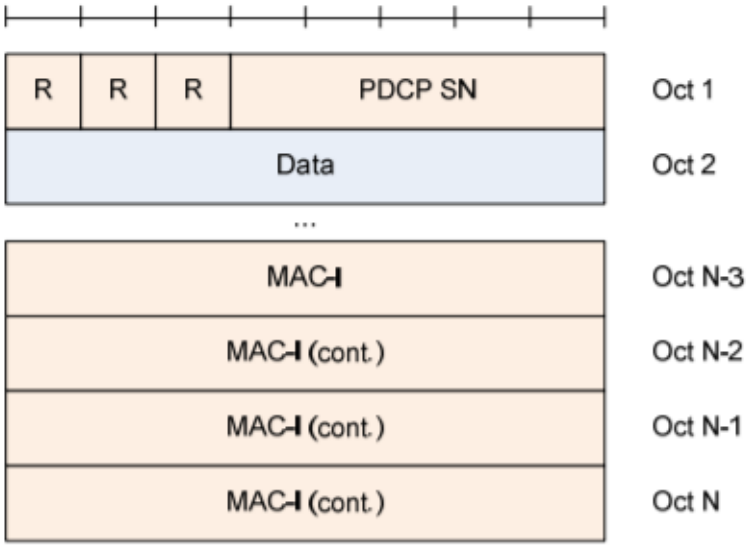
Funkcionalni pregled PDCP entiteta prikazan je na slici 1.9, pri čemu su prikazane i predajna i prijemna strana. Nakon što podaci stignu do PDCP (predajnog) entiteta, PDCP im dodaje sekvencni broj na osnovu kojeg, po prijemu podataka, prijemna strana može izvršiti odbacivanje duplikata. Nakon toga se u korisničkoj ravni vrši komepresija header-a, a u kontrolnoj ravni se omogućava zaštita integriteta podataka i šifriranje (samo ukoliko je paket pridružen PDCP SDU). Nakon dodavanja PDCP zaglavlja, u korisničkoj ravni se vrši rutiranje paketa prema odgobvarajućem nosiocu. Po prijemu paketa, vrši se uklanjanje PDCP zaglavlja, te dešifriranje, verifikacija integriteta i preuređivanje (ukoliko je potrebno). Nakon krajnje obrade, paket se šalje višim slojevima.

Na slici 1.10 je prikazan PDCP PDU podatkovnog tipa (Data) u korisničkoj ravni. Sastoji se od podatkovnog dijela i header-a, čija su polja:

- **D/C -** ***Data/Control*** (1 bit) - da li je riječ o kontrolnom (vrijednost 0) ili podatkovnom (vrijednost 1) polju
- **PDCP SN -** ***PDCP Sequence Number*** (5, 7, 12, 15, 16 ili 18 bita) - označava da li je riječ o SRB, DRB ili SLRB-ovima



Slika 1.10: PDCP Data PDU (Korisnička ravan) za DRB



Slika 1.11: PDCP Data PDU (Kontrolna ravan) za SRB

Na slici 1.11 je prikazan PDCP PDU podatkovnog tipa u kontrolnoj ravni. Značenje pojedinih polja sa slike su sljedeća:

- **R - *Reserved*** (1 bit) - postavljen na vrijednost '0', a na prijemnoj strani se zanemaruje
- **PDCP SN - PDCP Sequence Number** - prethodno objašnjeno
- **MAC-I** (32 bita) - prenosi kod za autentifikaciju poruka. Ukoliko podaci kontrolne ravni nemaju zaštitu integriteta, polje se nadopunjava *padding* bitima postavljenim na 0

DRB (engl. *Data Radio Bearer carrying user plane data*)
SRB (engl. *Signalling Radio Bearer carrying control plane data*)
SLRB (engl. *Sidelink Radio Bearer carrying Sidelink Communication or V2X sidelink communication data*)

1.4. RRC protokol

RRC (engl. *Radio Resource Control*) protokol obavlja sljedeće funkcije [6]:

- Broadcast sistemskih informacija (NAS i AS)
- Paging funkcije
- Uspostava, održavanje i prekid RRC konekcija
- Dodjela i modifikacija ARQ, HARQ i DRX konfiguracija
- Uspostava, modifikacija i prekid radio nosilaca (DRB)
- QoS kontrola
- AS sigurnosne konfiguracije
- Prenos NAS informacija

Korisnički uređaj se može nalaziti u jednom od dva stanja: *RRC_IDLE* i *RRC_CONNECTED*. Ukoliko RRC konekcija nije uspostavljenja, uređaj nije aktivan i nalazi se u stanju RRC_IDLE, a ukoliko uređaj ima uspostavljenu RRC vezu nalazi se u stanju RRC_CONNECTED. Navedena RRC stanja se mogu detaljnije prikazati [6]:

- **RRC_IDLE**:
  - Viši slojevi mogu konfigurisati DRX karakterističan za jednog korisnika
  - UE kontrolia mobilnosti
  - UE:
    - Vrši nadzor paging kanala u svrhu detekcije dolaznih poziva, promjene sistemskih informacija i sl.
    - Obavlja mjerenje susjednih ćelija i vrši ponovnu selekciju istih

        * Pribavlja informacije o sistemu

- **RRC_CONNECTED**:
  - Unicast prenos podataka od/prema UE
  - Na nižim slojevima UE može biti konfigurisan sa specifičnim UE DRX
  - Mrežna kontrola mobilnosti
  - UE:
    * Vrši nadzor paging kanala i/ili provjeru sadržaja *System Information Block Type 1* u svrhu otkrivanja promjene sistemskih informacija, ETWS i CMAS notifikacije i sl.
    * Vrši nadzor kontrolnih kanala koji su povezani sa dijeljenim podatkovnim kanalom da bi utvrdio da li su podaci namijenjeni njemu
    * Pruža informacije o kvaliteti kanala
    * Pribavlja informacije o sistemu

Formati RRC poruka se mogu pronaći u [6] i u ovom radu, zbog velikog broja poruka koje bi se trebale obraditi, oni nisu detaljno razmatrani.

1.5. NAS protokol

NAS (engl. *Non-access stratum*) je predstavlja set protokola u EPS-u (engl. *Evolved Packet System*). Koristi se kao najviši sloj u kontrolnoj ravni za prenos signalizacije između UE i MME, a obavlja sljedeće funkcije [7]:

- Podrška za mobilnost korisničkih terminala (UE)
- Podrška procedurama upravljanja sesijama za uspostavljanje i održavanje IP konekcije između UE i PDN GW

NAS sigurnost je dodatna funkcija koja pruža NAS protokolima zaštitu integriteta i šifriranje NAS signalnih poruka.
NAS procedure su grupisane u dvije kategorije [7]:

- **EMM (engl. *EPS Mobility Management*)** - podržava mobilnost UE u smislu obavještavanja mreže o njegovoj trenutnoj lokaciji i pružanja povjerljivosti identiteta korisnika. Također, pruža usluge upravljanja vezom za SM (engl. *Session Management*) podsloj, kao i SMS entitet za CM (engl. *Connection Management*) podsloj.
- **ESM (engl. *EPS Session Management*)** - podržava uspostavu i rukovanje korisničkim podacima u NAS-u, te podržava upravljanje kontekstom EPS nosioca unutar UE i MME.

2. Opis rada protokola

2.1. Konfiguracija bazne stanice 4G mreže

Za opis konfiguracije bazne stanice 4G mreže (eNode-B) koristit će se konfiguracijska datoteka *4g-enb.conf*. Ova skripta služi za opis rada bazne stanice, te daje sve detalje potrebne za njenu konfiguraciju.

Najprije je definisan način prenosa podataka, što je u ovom slučaju FDD (engl. *Frequency Division Duplex*). To znači da se koristi metoda za uspostavljanje *full-duplex* komunikacijskog linka koji koristi dvije različite radio frekvencije, za predajnik i prijemnik. Sa druge strane, ukoliko se ova vrijednost postavi na 1, tada se koristi TDD (engl. *Time Division Duplex*). To znači da će pri prenosu podaci biti podijeljeni na *duplex* komunikacijske linkove za *uplink* i *downlink*, alokacijom različitih vremenskih slotova u istom frekvencijskom opsegu. U ovoj konfiguraciji bazne stanice, ova vrijednost postavljena je na 0, što znači da se koristi FDD.

Na *downlink*-u su definisane širine kanala koje se mogu koristiti za prenos podataka. Prema broju RB-ova (engl. *Resource Block*) na koju je postavljena varijabla za definisanje širine kanala, koriste se različite širine. Ukoliko je ova vrijednost postavljena na 6 tada se koristi širina kanala od 1.4 MHz, ukoliko je ona jednaka 15 koristi se širina kanala od 3 MHz, 25 (5 MHz), 50 (10 MHz), 75 (15 MHz) i na kraju vrijednost 100 će označavati širinu kanala od 20 MHz. U ovoj konfiguraciji ova vrijednost je postavljena na 100, dakle koriste se kanali širine 20 MHz.

Definisan je i broj antena na *uplink*-u i *downlink*-u. Može se koristiti SISO ili MIMO 2x2 princip. SISO (engl. *Single Input Single Output*) je klasični princip sa jednom predajnom i jednom prijemnom antnom. Sa druge strane MIMO 2x2 (engl. *Multiple Input Multiple Output*) je sistem koji ima 2 predajne i 2 prijemne antene. Ovdje je korišten 2x2 MIMO.

Također, moguće je omogućiti simulator kanala, koji služi za testiranje zračnog sučelja. U ovom slučaju je on ugašen (onemogućen). Mogući slojevi su: PHY, MAC, RLC, PDCP, RRC, NAS, S1AP, X2AP, GTPU i "svi". Postoji opcija "*all*" kojom se označava da se vrši adresiranje svih navedenih slojeva u isto vrijeme. Vrijednosti polja svakog od navedenih slojeva su data u nastavku.

Level - Vrijednost ovog polja može biti postavljena na jednu od sljedećih vrijednosti: *'none'*, *'error'*, *'info'* ili *'debug'*, pri tome se posljednja opcija koristi ukoliko je potrebno logovati sve vrijednosti.

Max_ size - postavlja maksimalnu heksadecimalnu vrijednost, ukoliko je postavljena na 0 to znači da ne postoji, ukoliko je postavljena na -1 to znači da nema ograničenja na

njenu veličinu.

Omogućeno je i udaljeno API i Web sučelje ukoliko se koristi adresa 0.0.0.0:9001.

Prethodno je spomenuta mogućnost uključivanja simulatora kanala, koji je po *default*-u ugašen (postavljena vrijednost na 0). Ukoliko se ipak, ova vrijednost promijeni na 1, tada se koristi kanal sa Gausovim bijelim šumom - AWGN (engl. *Additive White Gaussian Noise*). Pri tome je snaga šuma -30 dB.

Kada govorimo o povezivanju bazne stanice na jezgrenu mrežu, ona je povezana na MME (engl. *Mobility Management Entity*). Njegova IP adresa za S1AP (engl. *S1 Application Protocol*) konekciju je 127.0.1.100. S1AP protokol služi za signalizaciju između E-UTRAN i evolvirane jezgrene mreže.
IP adresa Ethernet sučelja koje je povezano na MME je 127.0.1.1., to je tzv. *GTP bind* adresa. Obje navedene adrese se mijenjanju ukoliko se MME pokreće na različitom *host*-u.

Za identifikaciju ćelija koje poslužuje navedena bazna stanica, prije svega definira se 20b SIB1 (engl. *System Information Block 1*) poruke. SIB1 je prva od 24 SIB poruke i koristi se za selekciju i pristup ćeliji te raspoređivanje sistemskih informacija. U ovom slučaju definisano je 20b *SIB1.cellIdentifier* = 0x1A2D0. Ovo ujedno predstavlja ID bazne stanice, dok je ID ćeije 0x01.
Bazna stanica također vrši *broadcast* PLMN-ova. PLMN (engl. *Public Land Mobile Network*), je identificiran globalnim unikatnim PLMN kodom koji se sastoji od MCC (engl. *Mobile Country Code*) i MNC (engl. *Mobile Network Code*), te je njih 6 maksimalno podržano. Unutar razmatrane skipte imamo jedan PLMN sa identifikatorom 26201. Ovo je oznaka za Njemačkog operatera T-Mobile.

Definiše se *dl_ earfcn* koji je ustvati *downlink EARFCN - E-UTRA Absolute Radio Frequency Channel Number* i definiše opsege i centralne frekvencije za *downlink*. Ukoliko se koristi TDD postavljena su tri *dl_ earfcn* vrijednosti, ito: 38050, 40620 i 42590. U suprotnom, za FDD, definisano ih je mnogo više, ito: 300, 900, 1575, 2150, 2525, 3350, 6300, 38050, 40620 i 42590.

Definisani su *default*-ni parametri ćelije. Na *uplink*-u i *downlink*-u se koristi MIMO 2x2 tehnika. Koristi se *bandwith* od 20MHz, što znači da postoji 100 RB-ova. Koristi se normalan ciklični prefiks, kao i normalno trajanje PHICH kanala. LTE koristi HARQ (engl. *Hybrid Automatic Repeat Request*) unutar PHICH kanala, koji se koristi za slanje potvrda (pogrešnog) prijema podataka na *uplink*-u.

Neki od SIB1 parametara su vrijednost tag-a, koja je u ovom slučaju 0. Dužina prozora je 40 ms, maksimalna snaga dozvoljena na UE (engl. *User Entity*) je 10 dBm, minimalni nivo predaje je -70.

Ako je broj resursnih blokova RB=6, tada je maksimalna brzina za SI/RA/P-RNTI poruke 0.3, u suprotnom je 0.2.

U skripti su konfigurisani sljedeći kanali: PDCCH, PDSCH, PRACH, PUCCH i PUSCH.

- PDSCH (engl. *Physical Downlink Shared Channel*) je fizički kanal zračnog sučelja na *downlink*-u te služi za prenos DL-SCH i PCH transportnih kanala, te ostalih sistemskih informacija putem SIB-ova [8]. Njegova konfiguracija je trenutno jednaka za sve UE-ove. Ako je broj predajnih antena na *downlink*-u 4 definiše se p_a = -6, ukoliko je broj predajnih antena na *downlink*-u 2 definiše se p_a = -3,

u suprotnom je 0. Ako je definisana modulacijska šema - MCS (engl. *Modulation and Coding Scheme*) onda se ona koristi za sve UE, u suprotnom se računa iz CQI (engl. *Channel Quality Indicator*).

- PDCCH (engl. *Physical Downlink Control Channel*) je fizički kanal zračnog sučelja na *downlink*-u te služi za obavještavanje mobilnog uređaja o trenutku i vrsti podatka koji mu je raspoređen na dijeljenom kanal, te koje RB-ove smije koristiti na *uplink*-u [8]. Ako je definisan, broj CCE-ova (engl. *Control Channel Element*) i obično je jednak 2^{pdcch_format} gdje je pdcch_format u rasponu od 0 do 3. Dakle, CCE može imati vrijednosti 1,2,4 i 8 a služi za podršku pri slanju velikih poruka putem PDCCH kanala. Ukoliko nije definisan onda se proračunava iz CQI. Za sistem kod kojeg je definisano 6 resursnih blokova, CCE = 2, u suprotnom je 4.

- PRACH (engl. *Physical Random Access Channel*) je fizički kanal zračnog sučelja na *uplink*-u te služi za nadmetanje više mobilnih uređaja koji pokušavaju ostvariti slučajni pristup mreži [8]. Ako je broj resursnih blokova RB = 6, tada se korisnicima daje svaki deveti podokvir i nadmetanje se vrši svakih 20 ms. U suprotnom im se dodjeljuje svaki četvrti podokvir i nadmetanje se vrši svakih 10 ms. PRACH frekvencijski ofset je automatski.

- PUCCH (engl. *Physical Uplink Control Channel*) je fizički kanal zračnog sučelja na *uplink*-u te služi za prenos kontrolnih informacija kada ne postoje rezervisani resursni blokovi na PUSCH kanalu [8]. Njegova konfiguracija je trenutno jednaka za sve UE-ove. Ukoliko je u sistemu samo jedan UE tada postoji samo jedan CQI za PUCCH kanal, pri čemu se ova vrijednost povećava sa povećavanjem broja UE.

- PUSCH (engl. *Physical Uplink Shared Channel*) je fizički kanal zračnog sučelja na *uplink*-u te služi za slanje podataka i kontrolnih informacija od strane mobilnog uređaja [8]. Njegova konfiguracija je ista za sve UE-ove. Definisan je β_{offset} koji se koristi za kontrolu dodatnog kodnog pojačanja za UCI (engl. *Uplink Control Information*) kontrolne informacije. Različito je definisana za ACK, CQI i RI, gdje ovi indeksi iznose 9,6,6, respektivno. Kada se ne primi nikakva informacija od UE o CQI, tada se smatra da je za sistem sa RB = 6 CQI = 5, u suprotnom je CQI = 3. Ako je definisan MCS PUSCH kanala je jednak za sve UE, u suprotnom se proračinava iz posljednjeg primljenog SRS-a. Ovdje je definisan MCS = 18.

Period za slanje zahtjeva za raspoređivanje (engl. *Scheduling request*) mora biti veći od 40 ms za HD-FDD. Ovdje je za TDD definisan na 20 ms.

CQI period mora biti veći od 32 ms za HD-FDD, a u ovoj skripti definisan je na 40 ms.

Ako je broj antena na *downlink*-u veći od 2, tada se period slanja RI izvještja računa kao $m_{ri} * cqi_{period}$. Vrijednost m_ri je 0 po *default*-u, što znači da slanje izvještaja nije omoućeno. Ovdje je definisano na 8.

SRS (engl. *Sounding Reference Signal*) koristi se od strane bazne stanice za dobijanje boljeg pogleda na *uplink* kanal specifičnog korisnika. Definisan je različito u odnosu na broj RB-ova koji se koriste. Te je za svaki definisan konfiguracijski indeks i pozicija u frekvencijskoj domeni. Period slanja SRS-a mora bit veći od 40 ms za HD-FDD. Ovdje je definisan na 40 ms.

Za slanje potvrda pogrešnog prijema na *uplink*-u se koristi HARQ (engl. *Hybrid automatic repeat request*). Definisan je maksimalan broj transmisija na *uplink*-u i *downlink*-u i iznosi 5.

Ograničen je broj iteracija upotrebe turbo dekodera kako bi se smanjilo vrijeme korištenja CPU-a. Pored toga, koristi se dinamičko upravljanje snagom, DPC (engl. *Dynamic Power Control*) koji je za PUSCH SNR = 15, te za PUCCH SNR = 10.

Nakon svake aktivnosti dolazi do pokretanja tajmera, koji je u ovom slučaju 10000 ms. Ukoliko ne postoji nikakva aktivnost do isteka vremena šalje se *RRC Connection Release*. Pored navedenog RRC može definirati poželjne kriptografske algoritme za zaštitu sadržaja.

2.2. Opis protokola iz *4g-enb.conf*

Kao što je u prethodnom poglavlju već navedeno, mogući slojevi su: PHY, MAC, RLC, PDCP, RRC, NAS, S1AP, X2AP, GTPU i "svi". Postoji opcija "*all*" kojom se označava da se vrši adresiranje svih navedenih slojeva u isto vrijeme.
Ipak, samo neki od njih su definisani unutar skripte *4g-enb.conf*, i to:

- MAC (engl. *Medium Access Control*)
- RRC (engl. *Radio Resource Control*)
- NAS (engl. *Non-access stratum*)
- S1AP (engl. *S1 Application Protocol*)
- X2AP (engl. *X2 Application Protocol*

U nastavku će svaki od navedenih protokola biti opisan.

2.2.1. MAC - *Medium Access Control*

Protokol postoji i u UE (korisnik) i eNodeB (bazna stanica). Dio je LTE zračnog sučelja kontrolne i korisničke ravni. U samoj skripti izvršena je MAC konfiguracija. Kako je već navedeno ovaj sloj se bavi ispravljanjem grešaka korištenjem HARQ mehanizma. U konfiguracijskoj datoteci je definisan maksimalan broj HARQ transmisija za *uplink* i *downlink*, i on iznosi 5.

2.2.2. RRC - *Radio Resource Control*

Bavi se signalizacijom između korisnika (UE) i bazne stanice (eNodeB) preko LTE-Uu sučelja. U samoj skripti izvršena je RRC konfiguracija. Maksimalna veličina je postavljena na sljedeći način *rrc.maxsize=1*, te je postavljeno i *rrc.level=debug*. Pored

toga, za PUSCH kanal kojim mobilni uređaj šalj kontrolne informacije putem ovog protokola postavljen je RRC zahtjev za uspostavljanje konekcije kao *pusch_ msg3_ mcs: 0*. Na *uplink*-u je također definisan preferirani kriptografski algotram, gdje je EEA0 (engl. *EPS Encrypting Algorithm* uvijek posljednji koji se bira. Isto je urađeno i za algoritam održavanja integriteta sadržaja, gdje se EIA0 uvijek posljednji bira. Razlog ovome je što 0 na kraju predstavlja nepostojanje algoritma za kriptovanje ili očuvanje integriteta. Prekid RRC konekcije vrši se nakon isteka tajmera, koji je postavljen na 10000 ms.

2.2.3. NAS - Non-Access Stratum

Sastoji se od seta EPS (engl. *Evolved Packet System*) protokola, i to EMM (engl. *EPS Mobility Management*) i ESM (engl. *EPS Session Management*). Bavi se slanjem signalizacijskih poruka između UE (korisnika) i MME (engl. *Mobility Management Entity*) koji je dio jezgrene mreže. U samoj skripti izvršena je NAS konfiguracija. Maksimalna veličina je postavljena na sljedeći način *nas.maxsize=1*, te je postavljeno i *nas.level=debug*.

2.2.4. S1AP - S1 Application Protocol

Aplikacijski protokol koji omogućava signalizacijeu između E-UTRAN i evolviranog paketskog jezgra EPC (engl. *Evolved Packet Core*). Ima sljedeće funkcije [9]:

- E-RAB menadžment funkcije
- Funkcije za transport konteksta
- Indikacijske funkcije o mogućostima UE-a
- Mobilnost
- Upravljanje S1 interfejsom
- Transport NAS signalizacije
- Obavještavanje o lokaciji

U samoj skripti izvršena je S1AP konfiguracija. Maksimalna veličina je postavljena na sljedeći način *s1ap.maxsize=1*, te je postavljeno i *s1ap.level=debug*. Pored toga, definisana je adresa MME-a za korištenje S1AP protokola ito kao 127.0.1.100, dok u slučaju da se MME pokreće na drugačijem *host*-u ova adresa mora biti modifikovana.

2.2.5. X2AP - X2 Application Protocol

Aplikacijski protokol koji se koristi da uspostavi mobilnost korisnika unutar E-UTRAN-a i omogućava sljedeće funkcije [10]:

- Upravljanje mobilnošću
- Upravljanje teretom
- Izvještavanje o generalnim greškama
- Resetovanje X2
- *Update* eNodeB-a

U samoj skripti izvršena je X2AP konfiguracija. Maksimalna veličina je postavljena na sljedeći način *x2ap.maxsize=1*, te je postavljeno i *x2ap.level=debug*.

3. Proces povezivanja

3.1. Analiza procesa povezivanja i raskida konekcije u 4G mrežu, te procesa prenosa podataka

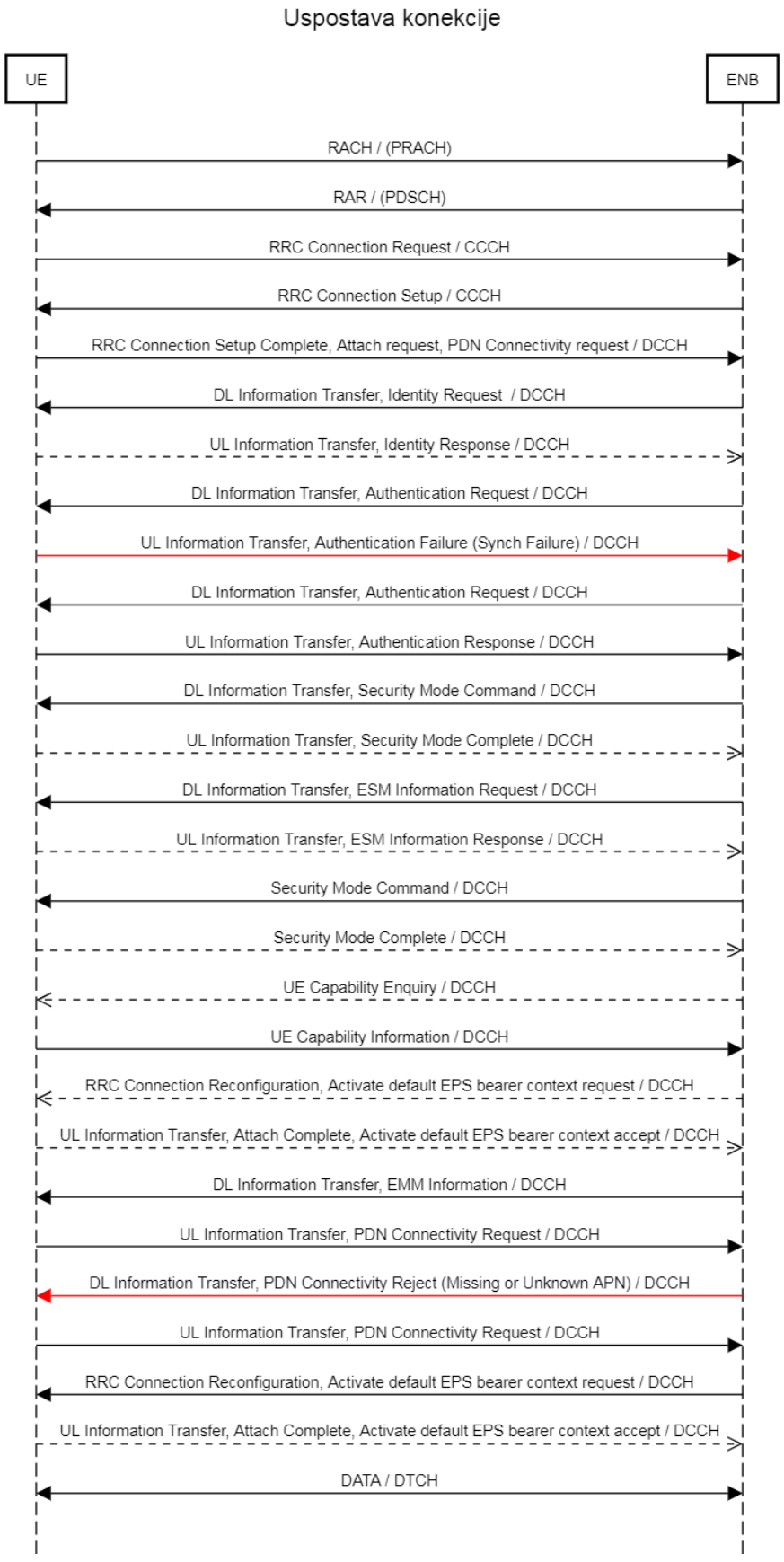
Prilikom analize saobraćaja, razmatran je snimak saobraćaja pod nazivom *4g-enb.pcap*. Prije same analize povezivanja uređaja na mrežu, prikazaćemo dijagram poruka sačinjen na osnovu priloženog pcap file-a.

S lijeve strane imamo naznačenu poruku koja se razmjenjuje između korisničkog terminala i bazne stanice, dok sa desne strane imamo logički kanal na kojem se prenosi ta poruka. Crvenom linijom su označene *failure* poruke, dok su isprekidanom linijom označene ACK poruke. Kao što možemo vidjeti na slici iznad, jedino se za poruke RACH i RAR, naznačeni kanali nalaze u zagradi iz razloga što za navedene poruke ne postoji logički kanali. NA RACH transportnom kanalu se, putem PRACH fizičkog kanala prenosi poruka za slučajni pristup baznoj stanici, kako bi se uspostavila konekcija. Na navedenu poruku se odgovara *RAR (Random Access Response)*, koja se prenosi na PDSCH fizičkom kanalu.

Nakon uspostavljanja konekcije, ostatak toka uspostave se prenosi preko CCCH i DCCH logičkih kanala. Iz razloga što se ovi kanali mapiraju na DLSCH i ULSCH transportne kanale (u ovisnosti od smjera komunikacije), te na PDSCH i PUSCH fizičke kanale, na dijagramu nisu naznačeni transportni i fizički kanali. CCCH (engl. *Common Control Channel*) se koristi za prenos kontrolnih informacija između korisničkog terminala i mreže, u slučaju kada ne postoji uspostavljena RRC konekcija, dok se u suprotnom koristi DCCH (engl. *Dedicated Control Channel*). Za prenos podataka koristi se DTCH (engl. *Dedicated Traffic Channel*).

Nakon prijave na mrežu šalje se *RRC (Radio Resource Control) Connection Request* poruka, te kao odgovor od bazne stanice dobija *RRC Connection Setup* poruka. Navedenom razmjenom se vrši dodjela radio resursa korisničkom terminalu, dodjela radio nosioca, te se uspostavljaju i ostali logički kanali potrebni za nastavak komunikacije. Time se konfiguriše korisnička i kontrolna ravan u skladu sa uslovima u mreži, te se definiraju parametri kao što su modulacija, dužina resursnog bloka, da li se radi u potvrdnom modu i slično (u našem slučaju 16-QAM, 1 i potvrdni mod).

Dalje terminal šalje *RRC Connection Setup Complete, Attach Request, PDN connectivity request* poruku, kako bi se uspostavio default-ni EPS (engl. *Evolved Packet switched System*) nosioc, te kako bi se naposljetko mogao ostvariti protok informacija između terminala i *Public Data Network*. U navedenoj poruci se dostavljaju razni podaci kao što su podržani algoritmi za šifriranje, provjeru integriteta, mogućnosti za korištenje



Slika 3.1: Dijagram poruka na zračnom sučelju pri uspostavi konekcije u 4G mreži

kodeka, mogućnosti mobilne stanice kao i mreže. Dalje bazna stanica šalje *Identity Request*, čime od terminala traži specifične identifikacijske informacije (IMSI, IMEI), te joj korisnički terminal odgovara Identity Response porukom (IMSI-262010000000002).

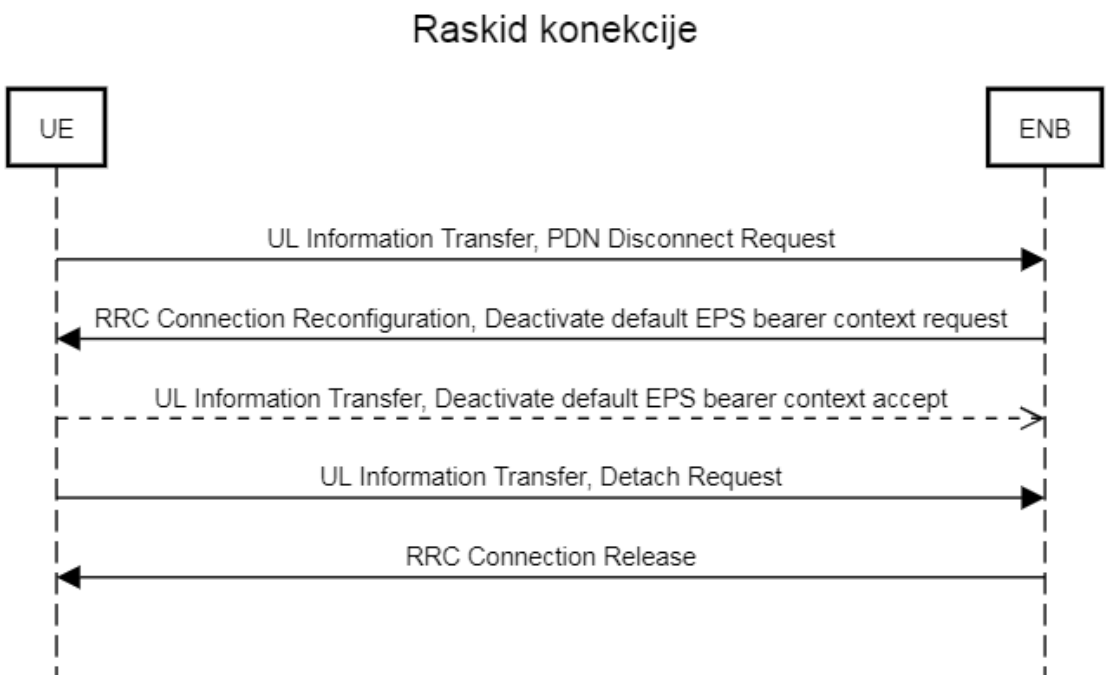
Komunikacija se nastavlja *Authentication Request* porukom, kako bi se izvršila uzajamna autentikacija između mreže i korisnika, te dogovorili ključevi za šifriranje. Međutim, dolazi do nemogućnosti autentikacije iz razloga što je SQN vrijednost (jedna od korištenih za kreiranje ključa) izvan opsega dozvoljenih vrijednosti, te se pokreće novi proces autentikacije koji biva uspješno okončan.

Bazna stanica šalje *Security Command (Information Transfer)* kako bi se uspostavila AS sigurnost za siguran prenos RRC poruka u kontrolnoj ravni te IP paketa u korisničkoj ravni korištenjem AS ključeva. Dalje bazna stanica šalje ESM Information Request, kako bi od terminala dobila informacije o APN (engl. *Access Point Name* – u našem slučaju internet), te informacije o opcijama konfiguracije protokola (npr. adresa primarnog DNS servera – 0.0.0.0). Sljedećom *Security Mode* komandom se uspostavlja algoritam za šifriranje (EEA) te algoritam za provjeru integriteta (EIA).

Nadalje se šalje *UE Capability Enquiry* poruka, kako bi se dobili podaci o podržanim opsezima, parametrima, konfiguracijama od strane korisničkog terminala. Navedeno je potrebno iz razloga što postoji Release-ova koje pokriva LTE te s napretkom mreže, potrebno je omogućiti i podršku za uređaje koji ne podržavaju nove funkcionalnosti. Terminal odgovara *UE Capability Information* porukom, koja sadrži podatke kao što su podržani release (14 u našem slučaju), *ue-Category (4)*, lista podržanih opsega, načina rada (half-duplex, full duplex) te raznih drugih mogućnosti (inter-frequency handover).

Sljedeća poruka jeste od strane mreže prema terminalu, koja sadrži EMM informacije, kao što je ime mreže (Amarisoft Network), te vremenska zona i lokalno vrijeme. Nakon toga dolazi novi *PDN Connectivity Request* sa nepostojećim APN imenom (hos), koji upravo iz tog razloga biva odbijen. Novi zahtjev sa APN imenom IMS (engl. *IP Multimedia Subsystem*), biva prihvaćen te se vrši rekonfiguracija RRC konekcije, porukom *RRC Connection Reconfiguration*, nakon čega se vrši aktivacija default EPS nosioca. Rekonfiguraciju je bilo potrebno obaviti iz razloga što su potrebne određene vrijednosti za razmjenu multimedije te se može vidjeti da je unutar poruke definisana brzina od 8 kbps te veličina *bucketa* od 100 ms. Ovime je uspješno okončan proces povezivanja uređaja na mrežu

Prikaz raskida konekcije je dat na sljedećoj slici.



Slika 3.2: Dijagram poruka na zračnom sučelju pri raskidu konekcije u 4G mreži

Korisnički terminal šalje poruku *PDN Disconnect Request*, nakon čega se šalje poruka za deaktivaciju EPS nosioca, što mobilna stanica prihvata. Kroz zahtjev za odspajanje se vrši kombinirano odspajanje EPS nosioca i isključivanje IMSI, što znači da se mobilna stanica gasi. Navedeno je također očigledno iz poruka nakon *RRC Connection Release* kojom se potpuno raskida veza, a koje se prenose samo u downlink smjeru (dodatno nakon svake poruke slijedi retransmisija). Ovime je okončan proces raskida konekcije u 4G mreži.

Pri dvosmjernoj razmjeni podataka između korisnika i mreže, pored prenosa na downlinku i uplinku, postoje još i *short BSR* i *long BSR* poruke, koje predstavljaju *Buffer Status Report*, odnosno kontrolni element koji prikazuje količinu podataka u korisničkom terminalu koja je spremna za slanje, kako bi mreža mogla osigurati minimalne resurse za prenos tih podataka.

Također, jedna od poruka, pored navedenih te padding podataka, a koja se javlja u samoj komunikaciji, jeste *CS Domain not available*. Ona se javlja u slučaju da MME ne može poslužiti zahtjev korisničkog terminala iz razloga što CS domena nije dostupna te SMS nije podržan u MME.

Bibliografija

[1] C. Cox, *An Introduction to LTE: LTE, LTE-Advanced, SAE and 4G Mobile Communications, 2nd Edition.* John Wiley & Sons, 2014, ch. "6: Architecture of the LTE Air Interface".

[2] 3GPP TS 36.321 v11.6.0. 3rd Generation Partnership Project; Technical Specification Group Radio Access Network; Evolved Universal Terrestrial Radio Access (E-UTRA); Medium Access Control (MAC) protocol specification (Release 11) [Na internetu]. (2015) Dostupno: http://www.arib.or.jp/english/html/overview/doc/STD-T104v4_20/5_Appendix/Rel11/36/36321-b60.pdf [pristupano: 15.1.2021.].

[3] Prodevelopertutorial.com. "LTE MAC: Understanding MAC PDU" [Na internetu]. (2020) Dostupno: https://www.prodevelopertutorial.com/lte-mac-understanding-mac-pdu/ [pristupano: 15.1.2021.].

[4] ETSI TS 136 322 v12.3.0. LTE; Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Link Control (RLC) protocol specification (3GPP TS 36.322 version 12.3.0 Release 12) [Na internetu]. (2015) Dostupno: https://www.etsi.org/deliver/etsi_ts/136300_136399/136322/12.03.00_60/ts_136322v120300p.pdf [pristupano: 18.1.2021.].

[5] ETSI TS 136 323 V14.3.0. LTE; Evolved Universal Terrestrial Radio Access (E-UTRA); Packet Data Convergence Protocol (PDCP) protocol specification (3GPP TS 36.323 version 14.3.0 Release 14) [Na internetu]. (2017) Dostupno: https://www.etsi.org/deliver/etsi_ts/136300_136399/136323/14.03.00_60/ts_136323v140300p.pdf [pristupano: 18.1.2021.].

[6] ETSI TS 136 331 V13.0.0. LTE; Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Resource Confrol (RRC) protocol specification (3GPP TS 36.331 version 13.0.0 Release 13) [Na internetu]. (2016) Dostupno: https://www.etsi.org/deliver/etsi_ts/136300_136399/136331/13.00.00_60/ts_136331v130000p.pdf [pristupano: 18.1.2021.].

[7] ETSI TS 124 301 V15.4.0. Universal Mobile Telecommunications System (UMTS); LTE; 5G; Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS); Stage 3 (3GPP TS 24.301 version 15.4.0 Release 15) [Na internetu]. (2018) Dostupno: https://www.etsi.org/deliver/etsi_ts/124300_124399/124301/15.04.00_60/ts_124301v150400p.pdf [pristupano: 16.1.2021.].

[8] Kaljić, E. (2020) - *Predavanja iz predmeta Sistemi i servisi mobilnih telekomunikacija*, Univerzitet u Sarajevu, [Na internetu]. (2020) Dostupno:

https://c2.etf.unsa.ba/course/view.php?id=229 [pristupano: 28.12.2020.].

[9] S1 Application Protocol (S1AP) [Na internetu]. (2020) Dostupno: http://4g5gworld.com/specification/s1-application-protocol-s1ap [pristupano: 20.1.2021.].

[10] X2 Application Protocol (X2AP) [Na internetu]. (2020) Dostupno: http://4g5gworld.com/specification/x2-application-protocol-x2ap [pristupano: 20.1.2021.].