1. אילו מערכות (תחנות) קיימות ברשת דור 2? מאילו ישויות מורכבות המערכות הללו ומה תפקידן?
2. מה ההבדל בין HLR ל-VLR?
3. מהו ה-AuC? מה תפקידו?
4. מדוע צריך TMSI?
5. הסבירי על TDMA, FDMA וכיצד הוא בא לידי ביטוי ב-GSM.
6. מהם אפיקי איתותים? הסבירי על SACCH, FCCH, SCH, BCCH, RACH, PCH ו-AGCH.
7. מהו ערך הTA (Time Advance)?
8. הסבירי על C1. למה צריך את החלק MAX(B,0) בביטוי?
9. כיצד המנוי מנטר עוצמות? כיצד המנוי יחליט לעבור לתא חדש?
10. מהו PLMN? מהו MCC? MNC?
11. אילו מזהים קיימים לתא סלולרי?
12. מהו SDMA? מדוע הוא בא לידי שימוש ב-GSM?
13. כיצד התא יודע לתקן הפרעות ערוץ? פרטי.
14. הסבירי על התהליכים הבאים:
    1. הדלקה של מכשיר והתחברות לרשת.
    2. הוצאת שיחה.

1.

החלקים העיקריים ברשת הם:

**MS**-Mobile Station זה אני 😊, אחראי ליצירת השיחה וניהולה גם במקרה של ניוד. הMS מחליט על עדכון מיקום לפי עוצמת הסגנל שמתקבל על ידו הוא מודיע על כך לMSC או לBSC.

**BSS (Base Station Subsystem)** מכיל את BTS וBSC.

BTS-Base Transceiver Station אליו פונה הMS דרך האוויר, ממשק שמכונה Um. מנהל את עוצמת השידור ביחד עם הנייד. הוא אחראי רק על תא סלולרי בודד. כמובן שהוא יכול לטפל במספר MS, הוא נמצא מתחת להשגחת ה BSC. BTS עושה למשל דילוג תדרים, קוד, החלטה על קצב שידור, הצפנה ומדידת עוצמות שידור בזמן שהואidle לפי התקן.

BSC base station controller נקרא גם base transceiver controller משגיח על מספר BTS, הוא נתון להשגחת הMSC. הוא לוקח את המידע שהBTS שלחו לו דרך ממשק Abis ושולח אותם בממשק A לMSC. הוא אחראי למשל על ניהול ערוצי רדיו, הצפנה וניהול handover.

**Network and switching subsystem** מכיל את הMSC, HLR וVLR.

**MSC**- משתמש בנתוני המשתמש שמאוחסנים בVLR(ראה למטה) לצורך ניהול השיחה. הוא אחראי על מספר BSC. הוא אחראי על ניתוב, חיוב המשתמש ושירותים מיוחדים כדוגמת SMS ו FAX.

BSC/MSC מחליטים על התא שמקבל את העוצמה החזקה ביותר אליו תעבור השיחה במקרה של handover.

MSSC- Mobile Services Switching Center אליו פונים הMS והBSC דרך ממשק שמכונה A. הMSSC וה BSC מדברים כבר במונחים של בקרה של שיחה בפרוטוקולי

SCCP Signaling Connection and Control Part

MTP- Message Transfer Part

הMSSC והMS מדברים על ניהול הנייד MM mobility management למשל בקשת אימות ובקשת עדכון מיקום. בנוסף הם מדברים על ניהול השיחה CM call management הודעה על עומסים, הודעה שהשיחה נענתה, נותקה ושחרור משאבים.

2.

רכיב הHLR פירושו Home Location Register הוא למעשה database מרכזי שמכיל מידע סטטי על משתמשים כגון מספר טלפון, פרטי חיוב, השירות עבורו הם שילמו וכו'. בנוסף הוא שומר מידע דינמי על מיקום המשתמשים האחרונים באזורו. הHLR אחראי לעיתים על מספר VLR כאשר הם בתורם אחראים על LA location areas שונים. ה HLR יודע עבור כל מכשיר באיזה VLR שמורים הפרטים שלו.

לעומתו רכיב הVLR הוא רכיב cache בעל זכרון קטן יותר ומהיר יותר שאחראי לעיתים אף על שטח קטן יותר. הוא מכיל חלק מזכרון הHLR, כגון מידע על המשתמשים הנוכחים בMSC המשויך לאותו VLR. הVLR אחראי על מספר LA location areas כאשר לכל משתמש רשום באיזה LA הוא נמצא.

3.

Authentication Center (AUC)

הAUC נמצא בתוך (באופן רעיוני לא באמת בתוך משהו פיזי כנראה בתוך הMSC) הOSS Operation Subsytem הוא מייצר את פרמטרי האימות עבור הVLR שמעוניין לבדוק את הפנייה שהגיע אליו. בנוסף הוא מאמת משתמשים ניידים ומייצר פרמטרים להצפנת מידע המשתמש באוויר.

תפקידו לוודא שהאדם שלפנינו הוא מי שטוען שהוא. זו בדיקה שהMSC מבצע כדי לוודא שאכן החשבון ששמור אצלו במערכות הוא מקושר לאדם הפונה. הבדיקה נעשית כדי למנוע מצב שאדם שלא שילם ישתמש בשירות או שאדם יחייב אדם אחר וכדומה. בנוסף הוא מסייע בהצפנת המידע מה שעוזר לדאוג שאדם בדרך לא יקלוט את השידור ויפענח את המידע.

4

TMSI Temporary Mobile Subscriber Identity הוא מזהה זמני של השיחה במקום IMSI, היתרון שלו הוא פרטיות, לא כל הרשת יודעת מי אני אלא רק הBSC ששוחחתי איתו. בנוסף הTMSI משתנה בכל עדכון מיקום LUP location update כך שיש אנונימיות מסוימת אפילו בין מיקומים שונים.

5.

TDMA הוא Time Division Multiple Access גישה מרובת משתמשים לאותו משאב בזמנים שונים. אנו נותנים לכל משתמש Time Slot בו הוא ניגש למשאב בזמן אחר אנו נותנים לאדם אחר. במידה ואדם מבקש גישה מרובה למשאב אנו מחלקים את בקשתו לחתיכות וכל פעם נותנים לו חתיכה אחת. היתרון הוא שאם יש אדם שצורך גישה מרובה אנו יכולים להפסיק אותו באמצע כרצוננו. אם הוא היה מקבל גישה עד שהוא מסיים הוא יכל לחסום לנו את המשאב זמן רב, ואם היינו עוצרים אותו יכול להיות שכל מה שהוא שלח ירד לטמיון.

FDMA פירושו Frequency Division Multiple Access, גישה מרובת משתמשים בתדרים שונים. אנשים שונים משדרים בתדרים שונים. בGSM יש חלוקה של המידע לframes וכל frame מחולק אף הוא לbursts קצרים שאורכם כ500 micro sec. אנשים שונים יכולים לשדר במרחק בזמן של מילי שניות אחד מהשני, על אף ששיחה ממוצעת ארוכה מכך בהרבה. בנוסף השידור נעשה על פני 124 ערוצים שונים ולכן אף באותו פרק זמן ניתן לשדר בתדרים שונים.

6.

ניתן לשלוח בנוסף למידע כגון SMS ושיחות טלפון, גם מידע על הערוץ והקשר כדי לסייע לשידור תקין.

הערוץ SACCH שפירושו slow associated control channel, מיועד לשידור הודעות שמקושרות לערוץ מידע. למשל הודעות על עוצמת השידורים בערוץ המידע.

הערוץ FCCH שפירושו Frequency Correction Channel, מיועד לשיפור הקליטה במכשיר הנייד על ידי קליברציה. בנוסף משתמשים בו לזיהוי התחלה של multi frame.

הערוץ SCH שפירושו Synchronization Channel, מיועד לסנכרון זמן הקליטה במכשיר הנייד.

הערוץ BCCH שפירושו broadcast control channel, מיועד לשידור זהויות התאים הסמוכים (BTS). הודעות לגבי ערוצי בקרה נפוצים, השירות הזמין בתאים וכדומה.

הערוץ RACH שפירושו random access channel, מיועד למכשיר הנייד עבור בקשות לחיבורים מסוימים. למשל במידה והנייד רוצה גישה זמנית לערוץ כלשהו, הוא יכול לבקש גישה לRACH.

הערוץ PCH שפירושו Paging Channel, מיועד להודיע לניידים שאינם משתמשים כרגע בערוץ כלשהו על שיחה נכנסת או SMS.

הערוץ AGCH שפירושו access grant channel, מיועד להודיע לניידים על ערוץ זמני בו הם יכולים להשתמש לצורך בקרה.

7.

TA Time Advance מכונה גם Time Alignment הוא משמש בשביל למדוד כמה זמן delay יש בין הMS לBTS מידע זה משודר במהלך השיחה דרך Slow Associated Control Channel (SACCH).

כדי למנוע חפיפה בין MS שונים, בכל burst ישנו זמן שבו אין שידור הוא מכונה guard time. זמן הguard time הוא מאוד קצר, כי הרשת מבקרת באופן פעיל את יתרון הזמנים של המכשיר הנייד. בקרה זו של הרשת מכונה timing advance control. הבקרה מתחילה כאשר הנייד מבקש ערוץ דרך RACH בקשה זו נמצאת בburst שכמעט כולו guard time. הBTS מקבל את הבקשה ומעביר אותה לBSC עם ערך TA שנדרש עבור נייד זה. הBSC עונה לנייד עם מספר הSDCCH ועם ערך TA. הBTS במהלך השידור מודד את הדיליי ומודיע במידת הצורך לBSC שבתורו מורה לנייד לשנות את הדיליי שלו דרך הודעה בSACCH.

8.

C1 הוא חיבור על כרטיס הסים שמשמש להספקת מתח. הBS base station מורה לMS מה עוצמת השידור הדרושה. ישנם 16 רמות כל אחת במרווח שווה משכנותיה של 2dB. כמובן שבמידה ויש בקשה לעוצמה שלילית (לא בdB), צריך להפסיק לשדר. ולכן עוצמת השידור היא למעשה max(B,0).

9. בזמן שהנייד לא משדר או קולט, הוא מודד את עוצמת השידור של התא שלו ושל התאים הסמוכים. הוא עושה זאת גם בזמן שיחה פעילה שכן לא בכל השיחה יש שידורים, למשל כאשר הVAD voice activity detection מזהה שאין שיחה אזי הנייד לא משדר. התא שלו (BTS) מודיע לו דרך BCCH את תדרי השידור של התאים השכנים ולכן הנייד יכול למדוד את עוצמתם.

ערך עוצמת השידור מכונה received signal strength indication RSSI, וכאשר הRSSI של תא שכן חזק יותר מהRSSI של התא שמשרת את הנייד בערך שיכול להקבע על ידי מפעיל הרשת, הנייד בוחר את התא החזק וקורא את הBCCH. אם התאים שייכים לאיזורים אחרים, LAC שונים, אזי הנייד צריך לעדכן את מיקומו ולא רק לשנות את התא. הנייד פונה לMSC לאחר אימות מול הVLR לצורך מעבר לתא החדש.

10.

PLMN- Public Land Mobile Network זוהי רשת התקשורת שאחראית על עשרות MSCs.

MCC Mobile Country Code זהו קוד שאורכו עד 3 ספרות שמזהה את המדינה של הנייד. קוד זה יכול לשמש לצורך ניתוב, שכן אם אני רואה קוד של איטליה, אזי אני יכול לכוון את השיחה לMSC באיטליה.

MNC- Mobile Network Code זהו קוד שמזהה את הרשת הסלולרית. קוד זה מזהה את החברה דרכה אני משתמש ברשת הסלולרית, למשל בישראל יש קוד שונה לחברות כגון סלקום, אורנג, וכו'.

11.

לתא סלולרי יש מזהה יחודי שנקרא cell ID. בנוסף יש לו מזהה הנוגע למיקומו LAC location area code אבל מזהה זה אינו בהכרח ייחודי, שכן יכולים להיות תאים שונים עם אותו LAC.

12.

SDMA-space division multiple access, גישה של מספר אנשים לאותו משאב במקומים שונים במרחב. בGSM קיים שימוש בSDMA שכן תאים באזורים שונים במרחב יכולים לשדר באותו זמן ותדר, אם הם רחוקים, כך שאין הפרעה לשידור של אחד מהם.

13.

ראשית כל בכל burst שאורכו כ500 מיקרו שניות יש אות שידור ידוע שעוזר לשערך את פרמטרי הערוץ. אך עדיין כמובן שישנן שגיאות.

ישנם מספר מרכיבים שעוזרים לתיקון ובדיקת השגיאות.

כל 260 ביטי שמע, מחולקים ל3 מחלקות. המחלקה הראשונה מכילה את 50 הביטים הכי חשובים, שמכילים את עיקר המידע והמקדמים הראשונים לשחזור אות השמע. הם מוגנים על ידי קוד CRC cyclic redundancy code, כך שאם חלה בהם טעות קטנה, כל 260 הביטים נזרקים. נציין שהבדיקה לא יכולה לוודא שאכן לא חלה בהם טעות, ברמה המתמטית בודקים שהחלוקה של המידע בפולינום ידוע שווה ל3 ביטי מידע שמייצגים את השארית. יכול להיות שבסיכוי מסוים חלה טעות במידע אך הCRC יצא תקין.

המחלקה השניה מכילה 132 ביטים, ביטים אלו מצורפים ל53 הביטים מהחלק הקודם ליצירת 185 ביטי מידע. ביטי מידע אלו נכנסים לתוך מקודד קונבולוציה שמטרתו היא תיקון שגיאות בצד המקבל. עומק הקוד הוא 5, כלומר כל ביט לאחר הקידוד תלוי ב4 ביטים שלפניו. הקוד מכפיל את אורך המידע המקורי כלומר 185\*2=370 ביטים. לצורך שיפור הקוד, אנו מעוניינים שכל מילת הקוד תסתיים בקידוד האפס, מכיוון שכל ביט תלוי ב4 ביטים לפניו, נוסיף עוד 4 ביטי מידע, וסה"כ 8 ביטי מידע לאחר קידוד. בינתיים 378 ביטים.

המחלקה השלישית מכילה 78 ביטים שעוברים ללא הגנה משגיאות, ולכן שגיאה בהם לא תתוקן או תזוהה. בסה"כ 456 ביטים.

ביטים אלו מחולקים ל4 פרצים bursts, בכל אחד 114 ביטים. נציין שמעקרון הTDMA כל burst כנראה ישודר בframe משלו, אלא אם כן לא יהיה צורך.

עדיין ישנה בעייתיות, מה יקרה אם יהיו הרבה שגיאות בburst מסוים באזור מסוים? אלגוריתם Viterbi שמשמש להפקת מידע משידורים שקודדו בקודי קונבולוציה, לא עובד טוב עם שגיאות במיקום מסוים. ולכן יש צורך לפזר את ביטי המידע על פני יותר פריימים, למעשה 8, ולבצע פרמוטציות ביניהם, כך שלאחר ביטול הפרמוטציות,interleaver, אם יהיו שגיאות בנקודה מסוימת, השגיאות יתפזרו על פני כל המידע וניתן יהיה לתקנם.

14.

**הדלקה של מכשיר והתחברות לרשת.**

מדליקים את המכשיר😊. דבר ראשון אולי יהיה צריך ססמה PIN לסים. המכשיר סורק את התדרים עד למציאת רשת. בעזרת המידע מהערוץ שנמצא, base channel, הMS בודק האם מיקומו השתנה, במידה וכן הוא מתחיל בתהליך הרשמה ברשת😊.

הIMSI מחולץ מהSIM ונשלח לBSC לבקשת ערוץ. הBSC מסתכל בMNC וMCC ופונה לBTS להפעלת ערוץ במידה והוא מאשר, הBTS מודיע לMS. הMS פונה לMSC לעדכון מיקום, הMSC בודק את אימות המנוי בעזרת הAUC וה VLR.

הAUC בודק את פרטי המנוי בעזרת תגובה על אתגר, למשל בקשה מהמנוי להצפין משהו רנדומלי בעזרת המפתח הסודי.

לאחר מכן הMSC מחליט על TMSI חדש ומעדכן את המיקום והTMSI בVLR ובHLR, והBSC משחרר את הערוץ.

לאחר מכן הMSC יכול לעזור למנוי לפי מה שכתוב בHLR של הרשת הביתית של המנוי. למשל אם הMSC רואה שיש message waiting flag דלוק בVLR, אזי הוא פונה לSMSC ואומר לו לנסות לשלוח שוב את הודעת הSMS.

**הוצאת שיחה.**

**Mobile Originated call establishment**

הIMSI מחולץ מהSIM ונשלח לBSC לבקשת ערוץ. הBSC מסתכל בMNC וMCC ופונה לBTS להפעלת ערוץ במידה והוא מאשר, הBTS מודיע לMS. הMS מבקש ליצור שיחה מהMSC, הMSC בודק את אימות המנוי בעזרת הAUC וה VLR. הMSC שולח בקשת אימות ולאחר תגובה של הMS, הוא שולח לMS את פקודת ההצפנה, הMS עונה והAUC בודק זאת.

הMS שולח הודעה של המספר שאליו הוא רוצה לחייג. השיחה נשלחת למקבל בעזרת הMSC שמנווט את השיחה ברשת. הMSC מקצה ערוץ TCH traffic channel לצורך השיחה וMS מאשר. מודיעים לMS אם המיועד עסוק או לא. מודיעים לMS במידה והמיועד ענה. הMS מאשר וכעת הם יכולים לשוחח ביניהם.