



GSM



ОГЛАВЛЕНИЕ

- Теория
 - Введение
 - УМ интерфейс
 - Безопасность
- Практика
 - OsmocomBB
 - OpenBTS



ТЕОРИЯ

ВВЕДЕНИЕ



СЕТЕВОЕ ПОКРЫТИЕ

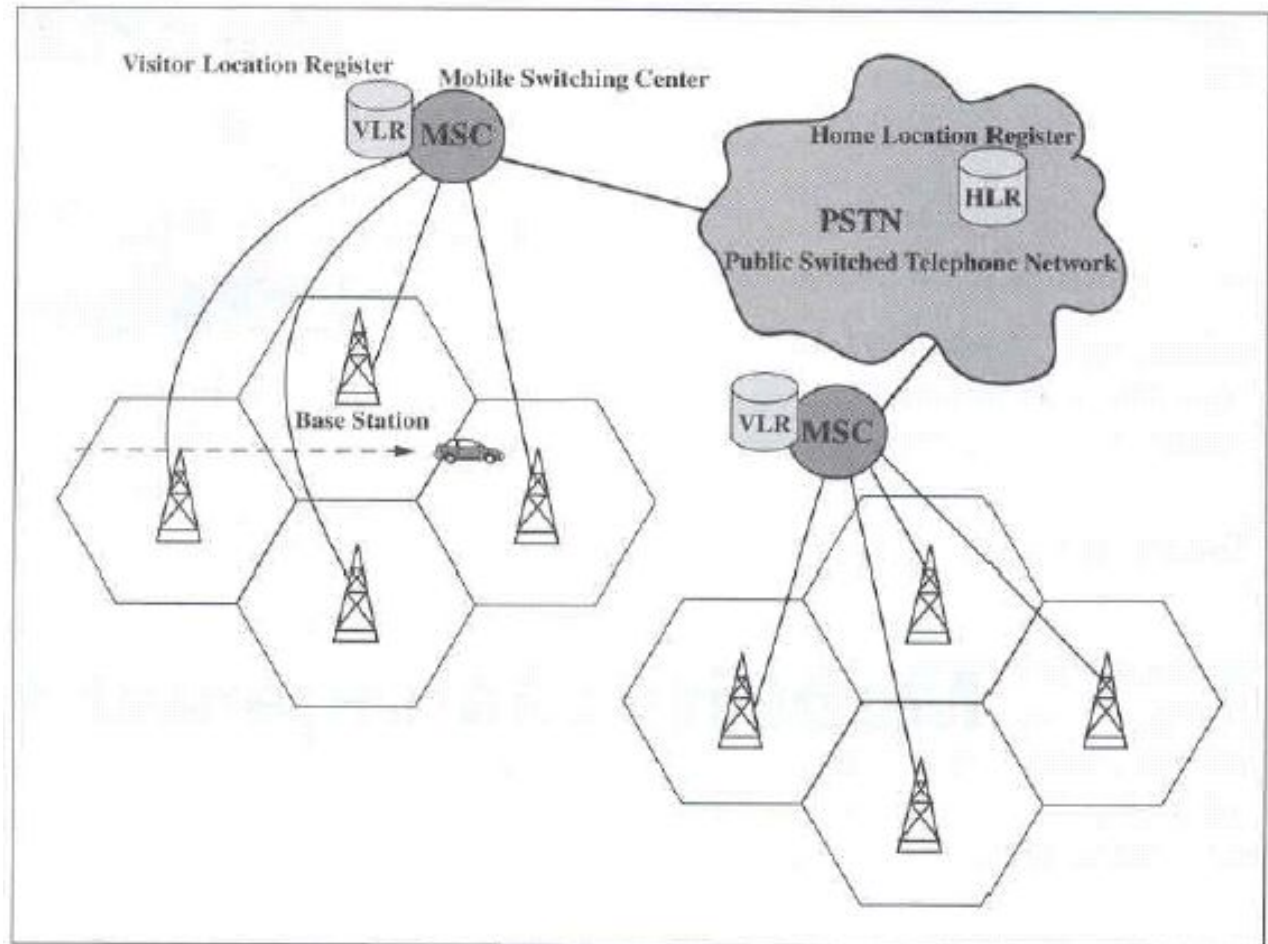
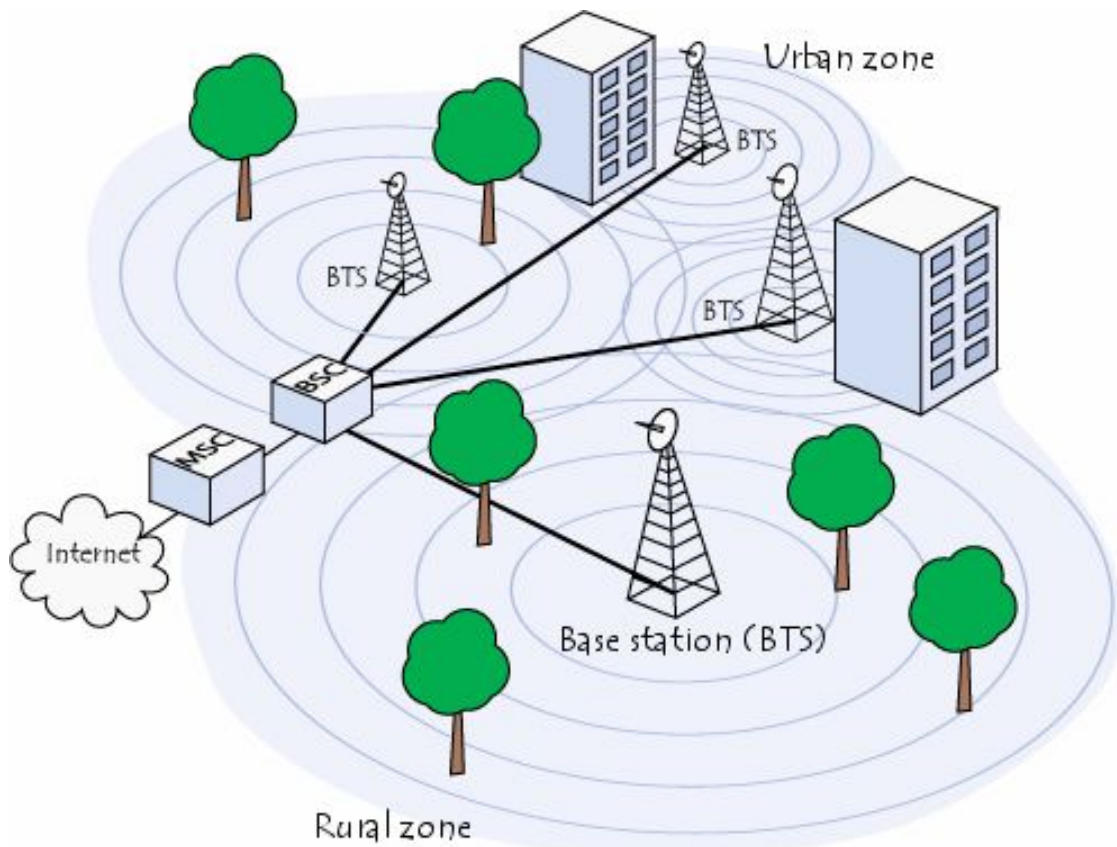
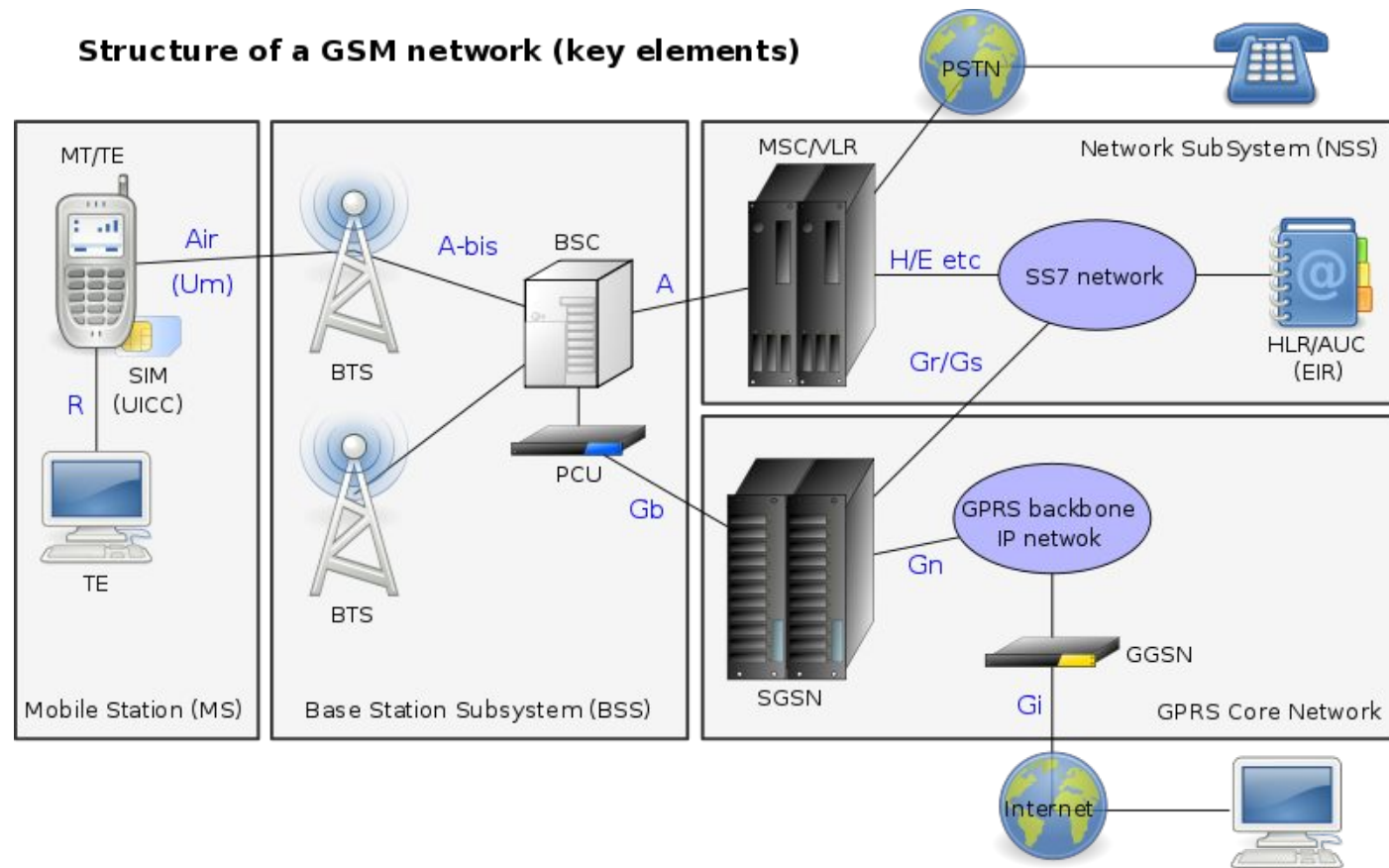


Figure 2.1 A common PCS network architecture.

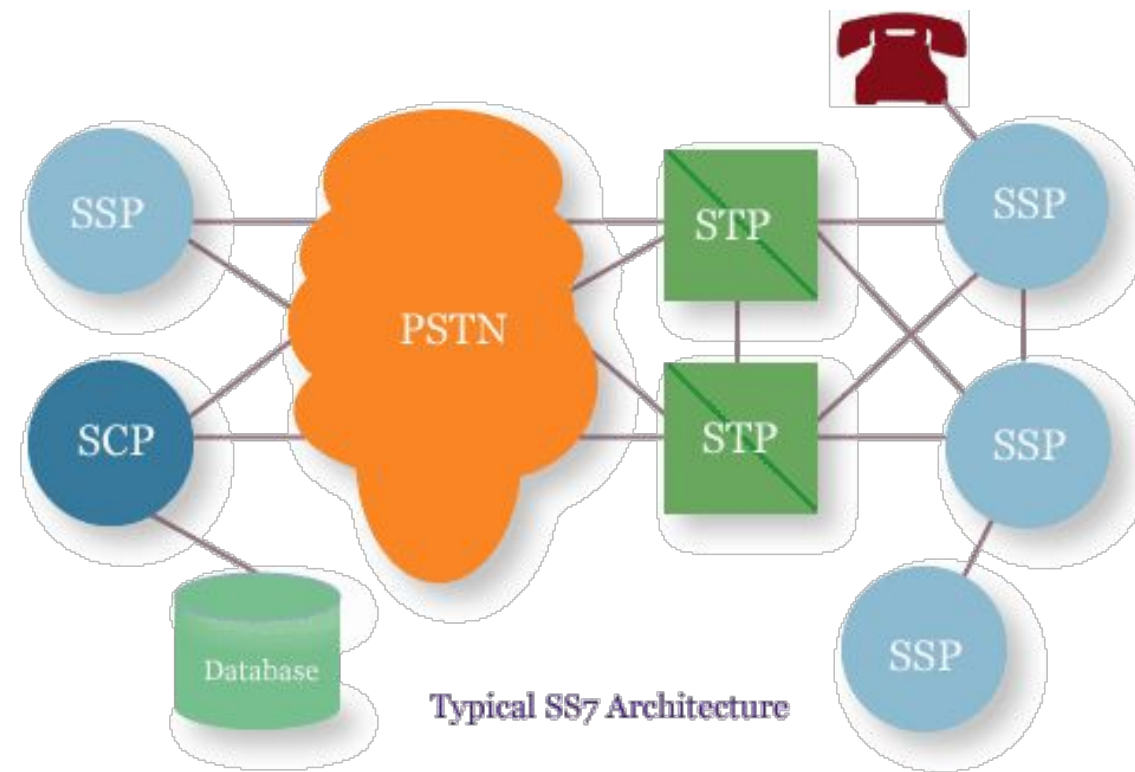
КАК ВЫГЛЯДЯТ БАЗОВЫЕ СТАНЦИИ?



ИНФРАСТРУКТУРА СЕТЕЙ GSM



OKC-7 (SS7)





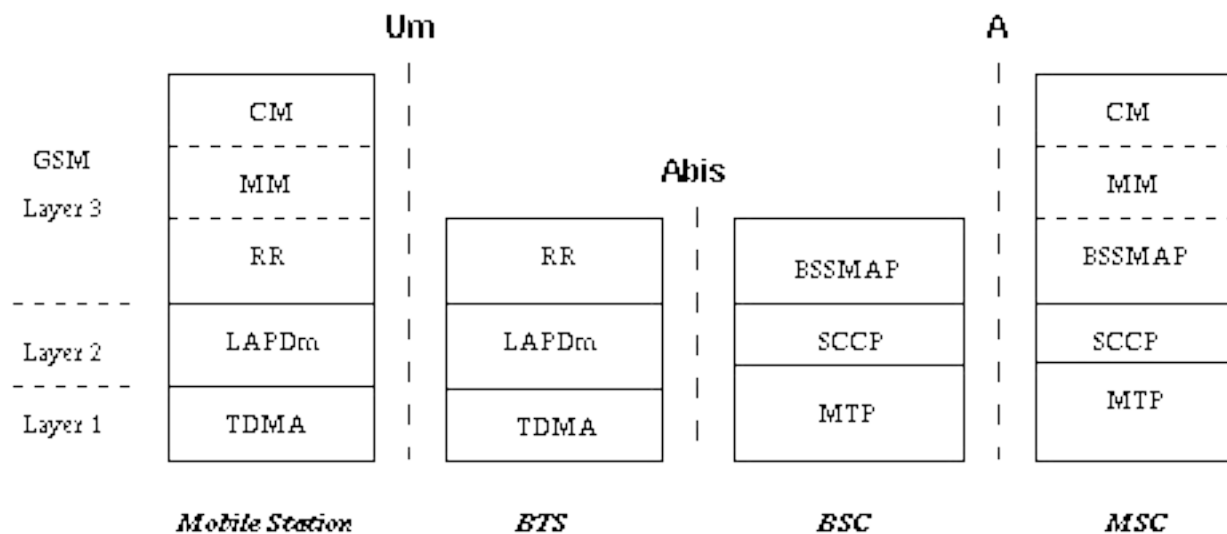
ТЕОРИЯ

УМ ИНТЕРФЕЙС



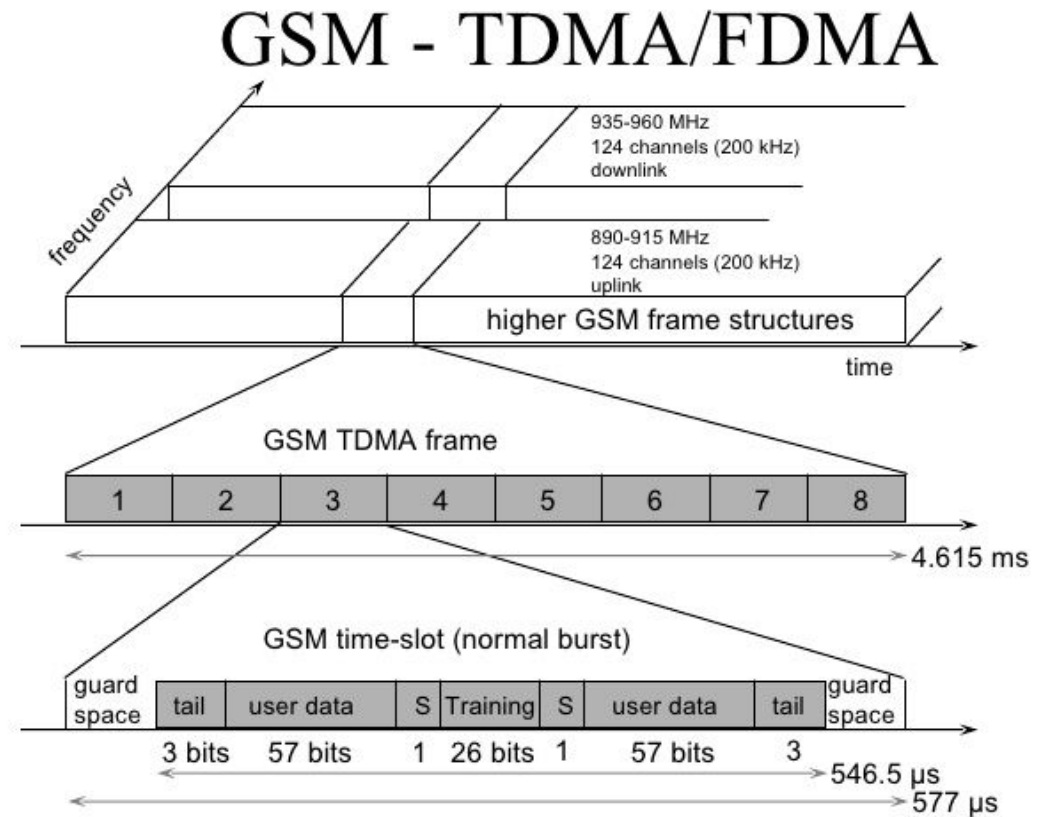
СТЕК ПРОТОКОЛА

- Layer 3
 - Сетевой уровень
 - GSM 04.{ 07, 08, 10, 11 }
- Layer 2
 - Канальный уровень
 - GSM 04.06
- Layer 1
 - Физический уровень
 - Описывает взаимодействие устройств в радиоэфире
 - GSM 05.xx



ФИЗИЧЕСКИЕ КАНАЛЫ РАЗДЕЛЕНИЕ МНОЖЕСТВЕННОГО ДОСТУПА

- FDMA
 - Frequency Division Multiple Access
- TDMA
 - Time Division Multiple Access

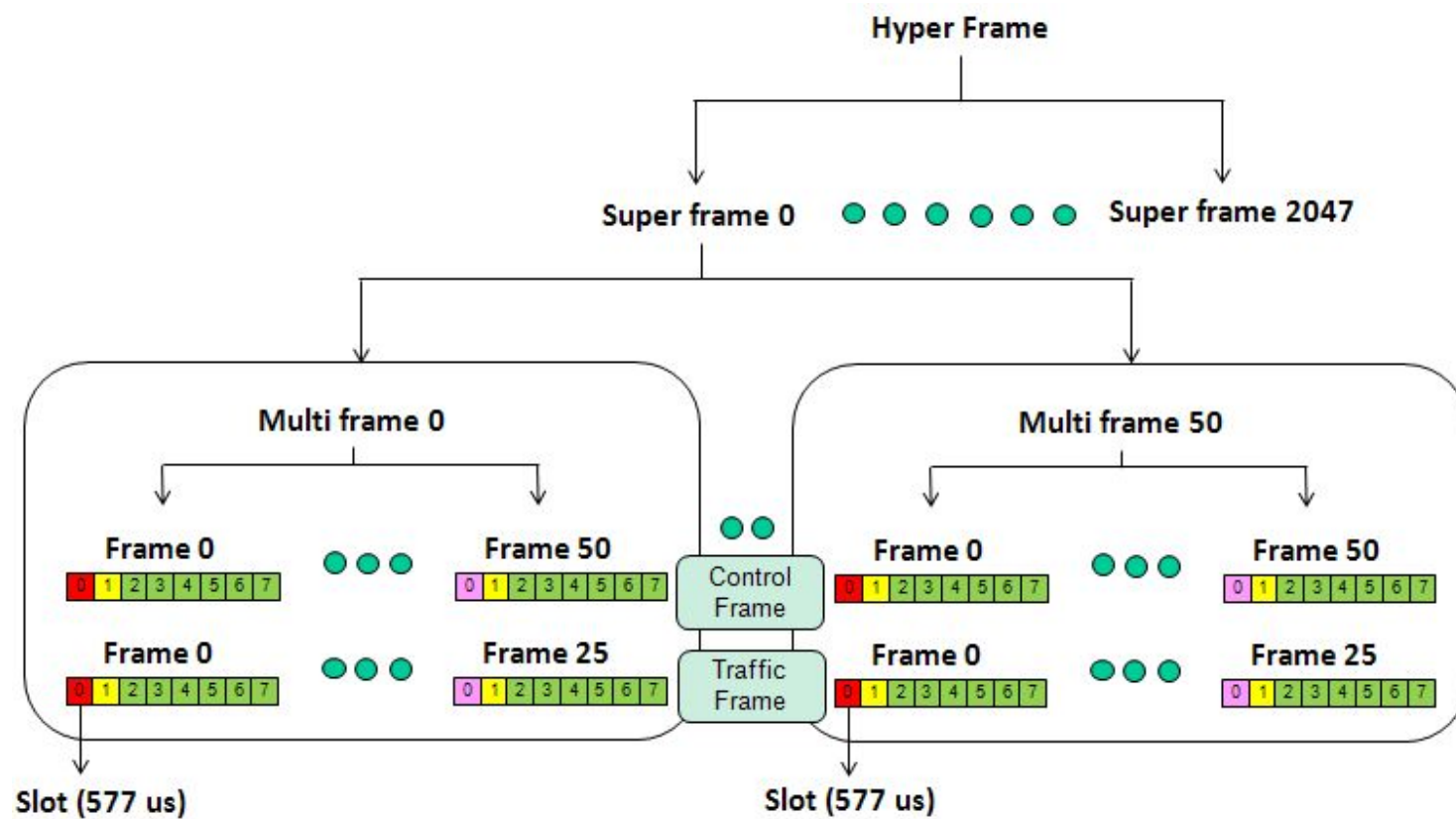


FDMA

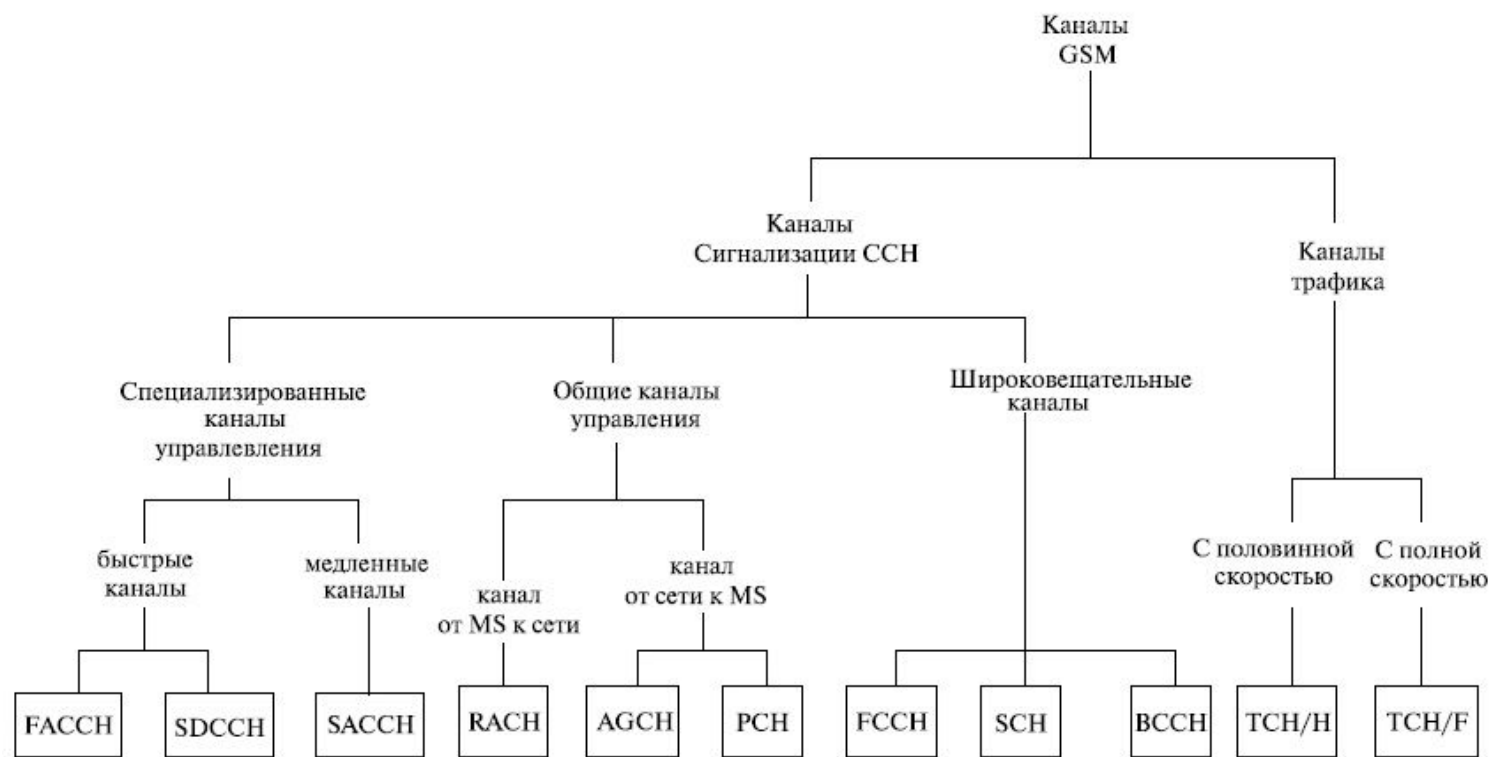
- Несколько диапазонов
 - GSM-850, E-GSM-900, DCS-1800, PCS-1900
- Frequency Division Duplex
 - Downlink
 - Uplink
- ARFCN
 - Определяет частоту UL/DL

System	Band	Uplink	Downlink	Channel Number
GSM 400	450	450.4 - 457.6	460.4 - 467.6	259 - 293
GSM 400	480	478.8 - 486.0	488.8 - 496.0	306 - 340
GSM 850	850	824.0 - 849.0	869.0 - 894.0	128 - 251
GSM 900 (P-GSM)	900	890.0 - 915.0	935.0 - 960.0	1 - 124
GSM 900 (E-GSM)	900	880.0 - 915.0	925.0 - 960.0	975 - 1023, (0, 1-124)
GSM-R (R-GSM)	900	876.0 - 915.0	921.0 - 960.0	955 - 973, (0, 1-124, 975 - 1023)
DCS 1800	1800	1710.0 - 1785.0	1805.0 - 1880.0	512 - 885
PCS 1900	1900	1850.0 - 1910.0	1930.0 - 1990.0	512 - 810

TDMA

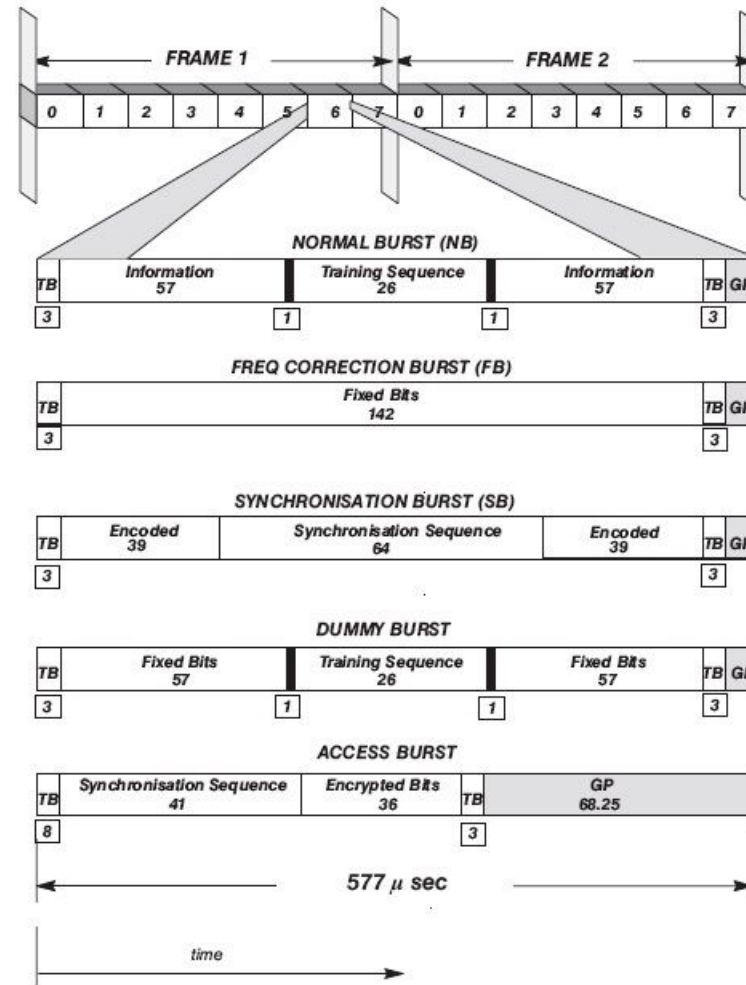


ЛОГИЧЕСКИЕ КАНАЛЫ



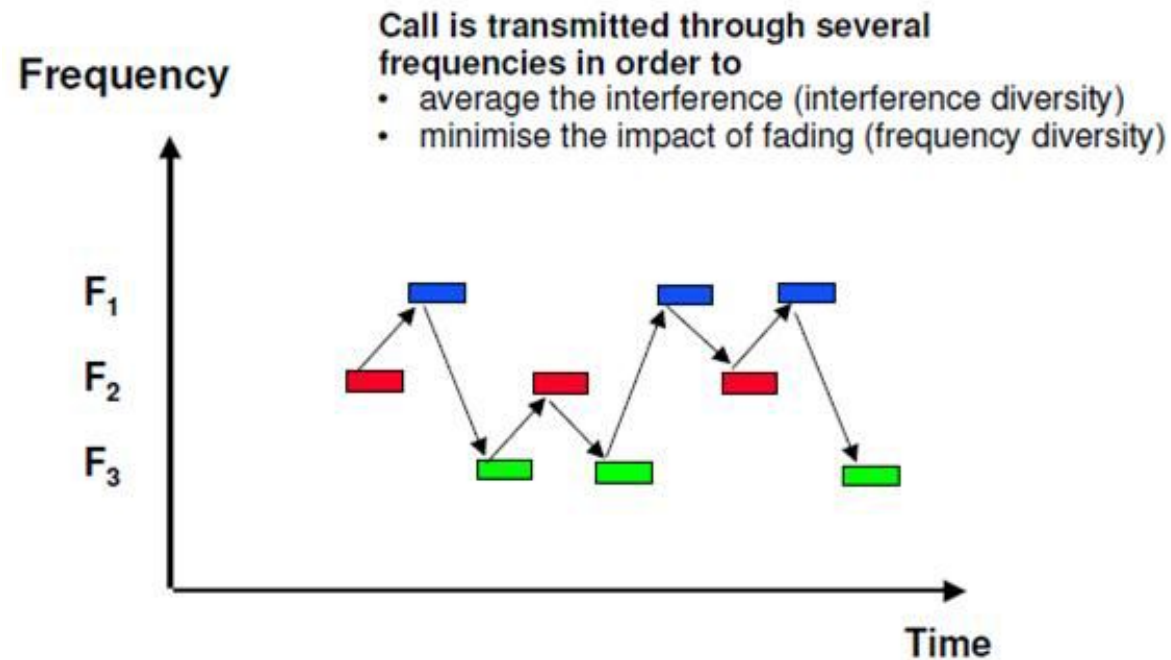
ЧТО ТАКОЕ BURST? ВИДЫ BURST

- Normal Burst
- Frequency Correction Burst
- Synchronization Burst
- Dummy Burst
- Access Burst



FREQUENCY HOPPING

- Уменьшение влияния интерференции
- Усложнение глушения сигнала
- Повышение безопасности сети





ТЕОРИЯ

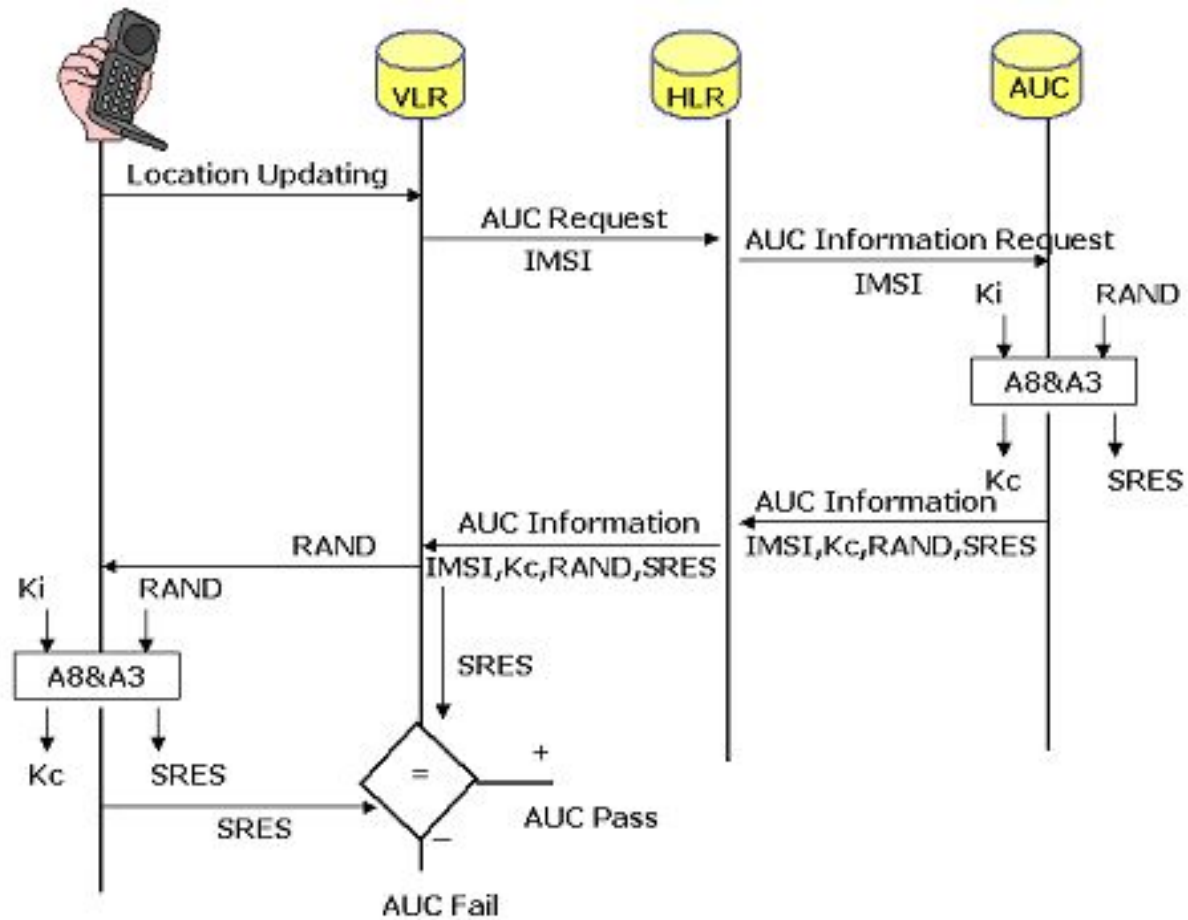
БЕЗОПАСНОСТЬ



ИДЕНТИФИКАЦИЯ АБОНЕНТОВ

- IMSI – идентификация мобильного абонента
- IMEI – идентификатор мобильного оборудования
- TMSI – временный идентификатор абонента

АУТЕНТИФИКАЦИЯ



ПРОБЛЕМЫ

- Односторонняя аутентификация □ Rogue BTS
- Ненадежное шифрование □ Kraken
- Уязвимость к атакам со стороны SS7 сети

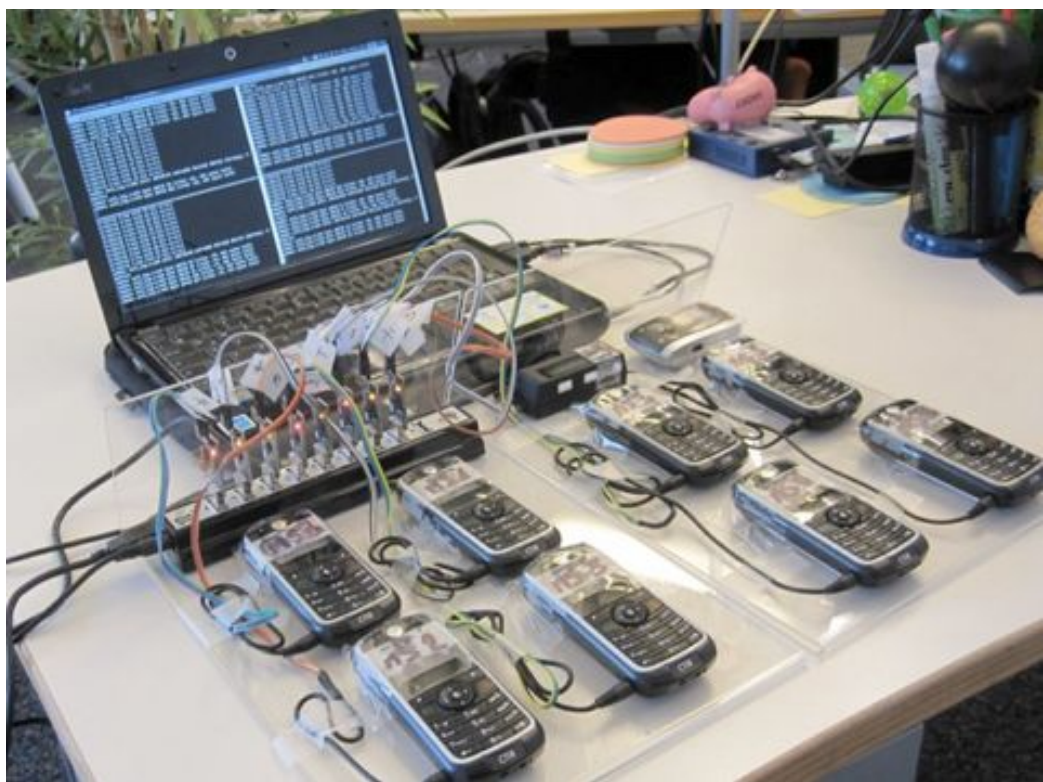


ПРАКТИКА

ОСМОСОМ-ВВ



ВВЕДЕНИЕ



BRANCHES

- master
- sylvain/burst_ind
 - Упор на сниффинг GSM
- sylvain/testing
 - Transceiver app
- jolly/testing
- jolly/emi
 - Проведение стресс-тестов
- jolly/menu
 - Хранение приложений в Flash-памяти телефона
- luca/catcher
 - Ловушка для Rogue BTS
- luca/libosmosim



SHOW TIME

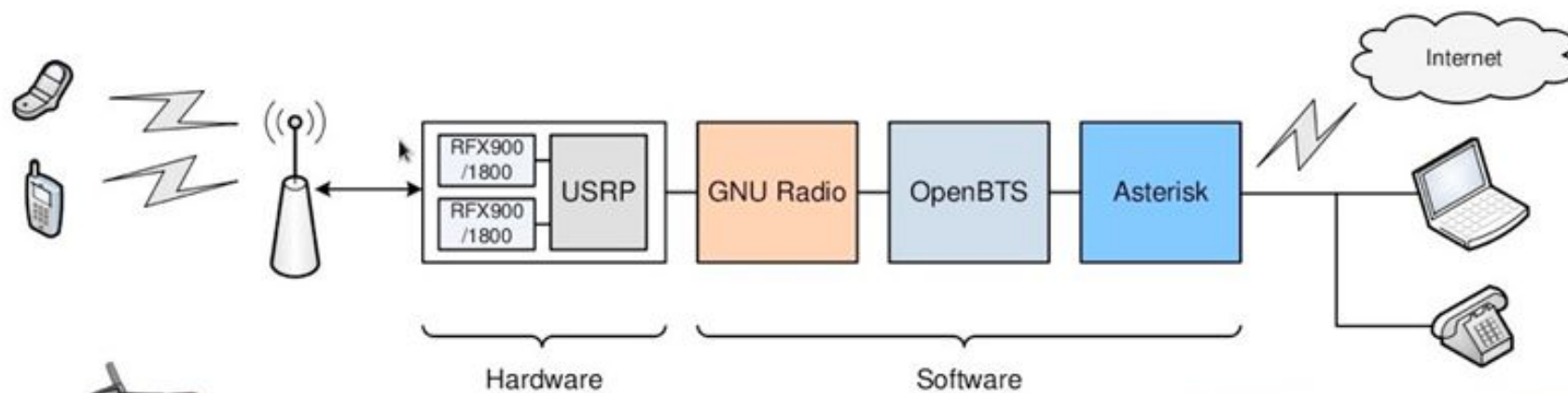


ПРАКТИКА

ROGUEBTS



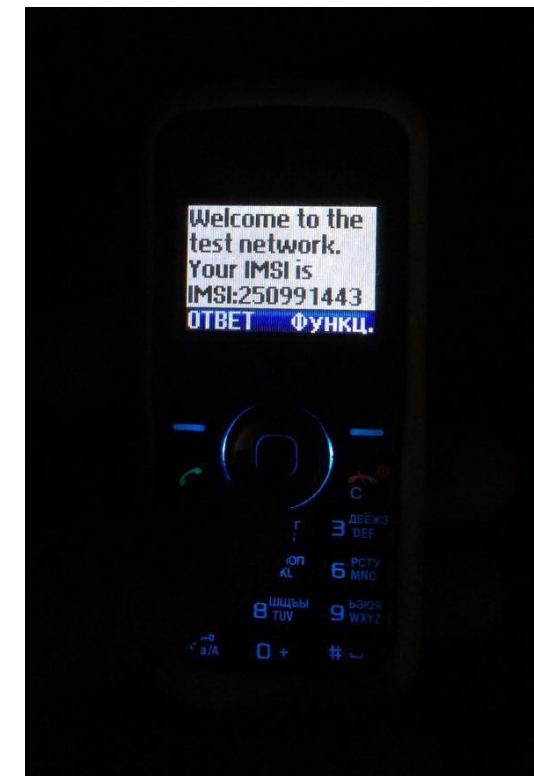
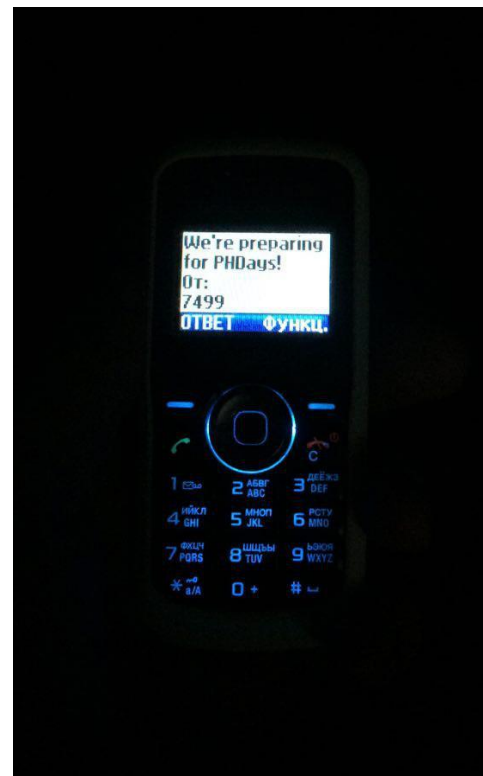
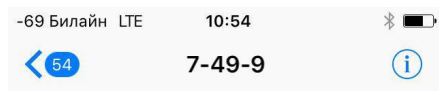
ЧТО ЭТО ТАКОЕ? ЗАЧЕМ ЭТО НУЖНО?



ЧТО ТАКОЕ SDR?



И ЧТО МЫ С ЭТИМ СМОЖЕМ СДЕЛАТЬ?



ССЫЛКИ

■ Теория

- <https://habrahabr.ru/post/268127/>
- <http://www.teletopix.org/category/gsm/>
- <http://www.sharetechnote.com/html/>
- <http://www.csie.ntpu.edu.tw/~yschen/course/95-1/>
- <http://www.ciens.ucv.ve:8080/genasig/sites/redesmov/archivos/GSM.pdf>
- http://read.pudn.com/downloads102/doc/comm/418135/DM_7_GSM_Protocol_Architecture.pdf

ССЫЛКИ

- Wikipedia

- <https://ru.wikipedia.org/wiki/GSM>
- https://en.wikipedia.org/wiki/Network_switching_subsystem
- https://en.wikipedia.org/wiki/Um_interface
- https://en.wikipedia.org/wiki/GSM_frequency_bands
- <https://ru.wikipedia.org/wiki/OKC-7>

ССЫЛКИ

- Сборник статей об атаках
 - <https://github.com/axilirator/plmn-research/tree/master/security>
- Kraken
 - <https://srlabs.de/bites/decrypting-gsm/>
- GSM fuzzing
 - https://fuzzinginfo.files.wordpress.com/2012/05/gsm_fuzzing.pdf
- Practical Cellphone Spying
 - <https://www.youtube.com/watch?v=fQSu9cBaojc>
- Easy 4G/LTE IMSI Catchers for Non-Programmers
 - <https://arxiv.org/pdf/1702.04434.pdf>

ССЫЛКИ

■ OpenBTS

- http://openbts.org/w/index.php?title=Main_Page
- <http://openbts.org/site/wp-content/uploads/2014/07/OpenBTS-4.0-Manual.pdf>
- http://openbts.org/site/wp-content/uploads/ebook/Getting_Started_with_OpenBTS_Range_Networks.pdf

■ OsmocomBB

- <http://osmocom.org/projects/baseband/wiki>
- <https://habrahabr.ru/post/260213/>