Эссе

На тему: GSM Security and Encryption (защита и шифрование в стандарте GSM)

Студента 917 группы МФТИ
Кузнецова Дмитрия

ОБЗОР СТАНДАРТА GSM(Global System for Mobile communications)**.**

Основная цель защиты сотовой связи заключается в защите разговора и передаваемых сигналов от прослушивания, а также от телефонного мошенничества. Старые аналоговые телефонные системы, такие как: Advanced Mobile Phone System (AMPS) и Total Access Communication System (TACS), позволяли даже радиолюбителю довольно легко перехватить сообщение с сотового телефона с помощью полицейского сканера. Известен даже случай, когда был перехвачен и опубликован разговор одного из членов английской королевской семьи. Другое решение в области безопасности сотовых телекоммуникационных систем включает в себя идентификационный мандат, такой как Electronic Serial Number (ESN), который передавался в открытую в аналоговых системах. Используя более сложное оборудование, возможно получить ESN и использовать его в целях телефонного мошенничества путём “клонирования” другого сотового телефона, чтобы потом им поль-зоваться. В Соединённых Штатах Америки общий ущерб от телефонного мошенничества составил более 500 миллионов долларов только в 1993 году. Методика, по которой Мобильная Станция регистрирует своё месторасположение в системе, также уязвима против прослушивания и позволяет определять месторасположение телефона, даже когда он выключен, в доказательство этого служит известный случай полицейского преследования известного американского атлета.

Механизм обеспечения безопасности и аутентификации, заложенный в GSM делает его самым защищённым из доступных на данный момент стандартов сотовой связи. В стандарте GSM выбрана гауссовская частотная манипуляция с минимальным частотным сдвигом (GMSK). Обработка речи осуществляется в рамках принятой системы прерывистой передачи речи (DTX), которая обеспечивает включение передатчика только при наличии речевого сигнала и отключение передатчика в паузах и в конце разговора. В качестве речепреобразующего устройства выбран речевой кодек с регулярным импульсным возбуждением и линейным предикативным кодированием с долговременным предсказанием (RPE/LTR-LTP-кодек). В стандарте GSM используется узкополосный многостанционный доступ с временным разделением каналов (NB TDMA). Для перехвата и восстановления сигнала, переданного в стандарте GSM, понадобится гораздо более сложное и дорогое оборудование, нежели полицейский сканер.

Основные характеристики стандарта GSM.

Частоты передачи подвижной станциии приема базовой станции, МГц	890-915
Частоты приема подвижной станции и передачи базовой станции, МГц	935-960
Дуплексный разнос частот приема и передачи, МГц	45
Скорость передачи сообщений в радиоканале, кбит/с	270, 833
Скорость преобразования речевого кодека, кбит/с	13
Ширина полосы канала связи, кГц	200
Максимальное количество каналов связи	124
Максимальное количество каналов, организуемых в базовой станции	16-20
Вид модуляции	GMSK
Индекс модуляции	BT 0,3
Ширина полосы предмодуляционного гауссовского фильтра, кГц	81,2
Количество скачков по частоте в секунду	217
Временное разнесение в интервалах TDMA кадра (передача/прием) для подвижной станции	2
Вид речевого кодека	RPE/LTP
Максимальный радиус соты, км	до 35

Структурная схема и состав оборудования сетей связи.

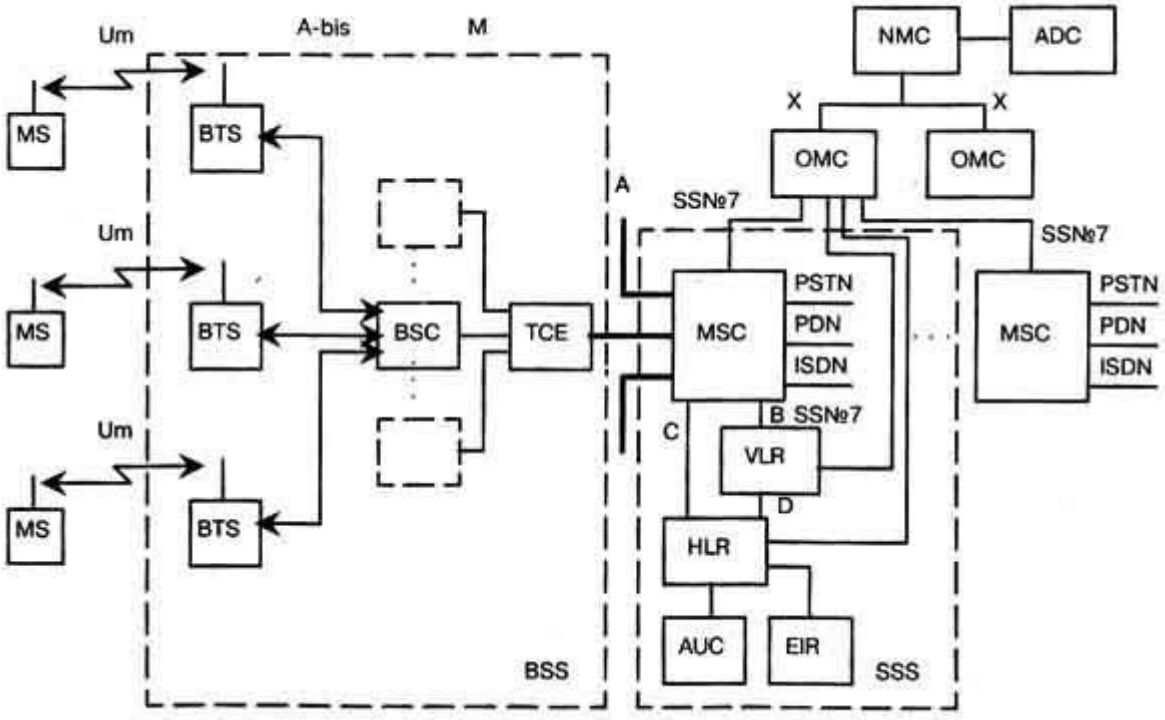


Рис. 1

На рис. 1 показано функциональное построение и интерфейсы, принятые в стандарте GSM.

- MSC (Mobile Switching Centre) - центр коммутации подвижной связи;
- BSS (Base Station System) - оборудование базовой станции;
- OMC (Operations and Maintenance Centre) - центр управления и обслуживания;
- MS (Mobile Stations) - подвижные станции.

Центр коммутации осуществляет постоянное слежение за подвижными станциями, используя регистры положения (HLR) и перемещения (VLR). MSC собирает статистические данные, необходимые для контроля работы и оптимизации сети. MSC поддерживает также процедуры безопасности, применяемые для управления доступами к радиоканалам. В HLR хранится та часть информации о местоположении какой-либо подвижной станции, которая позволяет центру коммутации доставить вызов станции. Регистр HLR содержит международный идентификационный номер подвижного абонента (IMSI). Он используется для опознавания подвижной станции в центре аутентификации (AUC). Практически HLR представляет собой справочную базу данных о постоянно прописанных в сети абонентах. В ней содержатся опознавательные номера и адреса, а также параметры подлинности абонентов, состав услуг связи, специальная информация о маршрутизации. Ведется регистрация данных о роуминге (блуждании) абонента, включая данные о временном идентификационном номере подвижного абонента (TMSI) и соответствующем VLR. К данным, содержащимся в HLR, имеют дистанционный доступ все MSC и VLR сети и, если в сети имеются несколько HLR, в базе данных содержится только одна запись об абоненте, поэтому каждый HLR представляет собой определенную часть общей базы данных сети об абонентах. Доступ к базе данных об абонентах осуществляется по номеру IMSI или MSISDN (номеру подвижного абонента в сети ISDN). К базе данных могут получить доступ MSC или VLR, относящиеся к другим сетям, в рамках обеспечения межсетевого роуминга абонентов.

Второе основное устройство, обеспечивающее контроль за передвижением подвижной станции из зоны в зону, - регистр перемещения VLR. С его помощью достигается функционирование подвижной станции за пределами зоны, контролируемой HLR. Когда в процессе перемещения подвижная станция переходит из зоны действия одного контроллера базовой станции BSC, объединяющего группу базовых станций, в зону действия другого BSC, она регистрируется новым BSC, и в VLR заносится информация о номере области связи,

которая обеспечит доставку вызовов подвижной станции. Для сохранности данных, находящихся в HLR и VLR, в случае сбоев предусмотрена защита устройств памяти этих регистров. VLR содержит такие же данные, как и HLR, однако эти данные содержатся в VLR только до тех пор, пока абонент находится в зоне, контролируемой VLR. В сети подвижной связи GSM соты группируются в географические зоны (LA), которым присваивается свой идентификационный номер (LAC). Каждый VLR содержит данные об абонентах в нескольких LA. Когда подвижный абонент перемещается из одной LA в другую, данные о его местоположении автоматически обновляются в VLR. Если старая и новая LA находятся под управлением различных VLR, то данные на старом VLR стираются после их копирования в новый VLR. Текущий адрес VLR абонента, содержащийся в HLR, также обновляется. VLR обеспечивает также присвоение номера "блуждающей" подвижной станции (MSRN). Когда подвижная станция принимает входящий вызов, VLR выбирает его MSRN и передает его на MSC, который осуществляет маршрутизацию этого вызова к базовым станциям, находящимся рядом с подвижным абонентом. VLR также распределяет номера передачи управления при передаче соединений от одного MSC к другому. Кроме того, VLR управляет распределением новых TMSI и передает их в HLR. Он также управляет процедурами установления подлинности во время обработки вызова. По решению оператора TMSI может периодически изменяться для усложнения процедуры идентификации абонентов. Доступ к базе данных VLR может обеспечиваться через IMSI, TMSI или MSRN. В целом VLR представляет собой локальную базу данных о подвижном абоненте для той зоны, где находится абонент, что позволяет исключить постоянные запросы в HLR и сократить время на обслуживание вызовов.

ОПИСАНИЕ ОРГАНИЗАЦИИ ЗАЩИТЫ В СТАНДАРТЕ GSM.

Защита GSM, и как она создавалась.

В принципе, по своему замыслу, цифровая система мобильной связи GSM вполне могла бы быть чрезвычайно защищенной. В основе ее лежит свод документов под названием "Меморандум о понимании стандарта GSM" или MoU Groupe Special Mobile standard. Этот Меморандум был подготовлен на излете Холодной войны по инициативе ведущих телекоммуникационных компаний Западной Европы. Разрабатывал техническую документацию GSM Европейский институт стандартов по телекоммуникациям (ETSI), а в создании схемы безопасности, в целом призванной защитить новую систему от перехвата, прослушивания и мошенничества, активное участие приняли спецслужбы стран НАТО.

Основу системы безопасности GSM составляют три секретных алгоритма (официально не раскрытые и поныне, сообщаемые лишь тем, кому это требуется по необходимости - поставщикам оборудования, операторам связи и т.д.):

A3 - алгоритм аутентификации, защищающий телефон от клонирования;

A8 - алгоритм генерации криптоключа, по сути дела однонаправленная функция, которая берет фрагмент выхода от A3 и превращает его в сеансовый ключ для A5;

A5 - собственно алгоритм шифрования оцифрованной речи для обеспечения конфиденциальности переговоров. В GSM используются две основные разновидности алгоритма: A5/1 - "сильная" версия шифра для избранных стран и A5/2 - ослабленная для всех остальных (для России).

Мобильные станции (телефоны) снабжены смарт-картой, содержащей A3 и A8, а в самом телефоне имеется ASIC-чип с алгоритмом A5. Базовые станции также снабжены ASIC-чипом с A5 и "центром аутенитификации", использующим алгоритмы A3-A8 для идентификации мобильного абонента и генерации сеансового ключа.

Вся эта архитектура при надлежащем исполнении и качественных алгоритмах призвана гарантировать надежную аутентификацию пользователя, обеспечивая защиту мобильных станций от клонирования и прочих методов мошенничества, а также качественное шифрование конфиденциальных переговоров. Собственно говоря, именно это и декларируется компаниями, успешно занимающимися разворачиванием GSM по всему миру и уже охватившими услугами удобной связи, по разным подсчетам, от 210 до 250 миллионов человек на планете.

Но реальность такова, что спецслужбы, занятые защитой правительственных коммуникаций, одновременно вовлечены и в деятельность противоположного рода: перехват и дешифрование коммуникаций в разведывательных целях. По этой причине, как свидетельствуют очевидцы, вокруг степени защиты GSM бушевали немалые страсти, поскольку спецслужбы стран НАТО имели довольно разные точки зрения на этот счет. Германия настаивала на сильных алгоритмах, поскольку имела самую длинную границу с коммунистическим блоком, другие же страны склонялись к ослабленному варианту. В конце концов, в качестве основы криптосхемы для A5 была избрана французская разработка.

Реализация A3-A8 (или COMP128).

```
typedef unsigned char Byte;

#include <stdio.h>
/* #define TEST */

/*
 * rand[0..15]: the challenge from the base station
 * key[0..15]: the SIM's A3/A8 long-term key Ki
 * simoutput[0..11]: what you'd get back if you fed rand and key to a real
 * SIM.
 *
 *   The GSM spec states that simoutput[0..3] is SRES,
 *   and simoutput[4..11] is Kc (the A5 session key).
 *   Note that Kc is bits 74..127 of the COMP128 output, followed by 10
 *   zeros.
 *   In other words, A5 is keyed with only 54 bits of entropy. This
 *   represents a deliberate weakening of the key used for voice privacy
 *   by a factor of over 1000.
 */

void A3A8(/* in */ Byte rand[16], /* in */ Byte key[16],
        /* out */ Byte simoutput[12]);

/* The compression tables. */
static const Byte table_0[512] = {
       102,177,186,162,  2,156,112, 75, 55, 25,  8, 12,251,193,246,188,
       109,213,151, 53, 42, 79,191,115,233,242,164,223,209,148,108,161,
       252, 37,244, 47, 64,211,  6,237,185,160,139,113, 76,138, 59, 70,
        67, 26, 13,157, 63,179,221, 30,214, 36,166, 69,152,124,207,116,
       247,194, 41, 84, 71,  1, 49, 14, 95, 35,169, 21, 96, 78,215,225,
       182,243, 28, 92,201,118,  4, 74,248,128, 17, 11,146,132,245, 48,
       149, 90,120, 39, 87,230,106,232,175, 19,126,190,202,141,137,176,
       250, 27,101, 40,219,227, 58, 20, 51,178, 98,216,140, 22, 32,121,
        61,103,203, 72, 29,110, 85,212,180,204,150,183, 15, 66,172,196,
        56,197,158,  0,100, 45,153,  7,144,222,163,167, 60,135,210,231,
       174,165, 38,249,224, 34,220,229,217,208,241, 68,206,189,125,255,
       239, 54,168, 89,123,122, 73,145,117,234,143, 99,129,200,192, 82,
       104,170,136,235, 93, 81,205,173,236, 94,105, 52, 46,228,198,  5,
        57,254, 97,155,142,133,199,171,187, 50, 65,181,127,107,147,226,
       184,218,131, 33, 77, 86, 31, 44, 88, 62,238, 18, 24, 43,154, 23,
        80,159,134,111,  9,114,  3, 91, 16,130, 83, 10,195,240,253,119,
       177,102,162,186,156,  2, 75,112, 25, 55, 12,  8,193,251,188,246,
       213,109, 53,151, 79, 42,115,191,242,233,223,164,148,209,161,108,
        37,252, 47,244,211, 64,237,  6,160,185,113,139,138, 76, 70, 59,
        26, 67,157, 13,179, 63, 30,221, 36,214, 69,166,124,152,116,207,
       194,247, 84, 41,  1, 71, 14, 49, 35, 95, 21,169, 78, 96,225,215,
       243,182, 92, 28,118,201, 74,  4,128,248, 11, 17,132,146, 48,245,
```

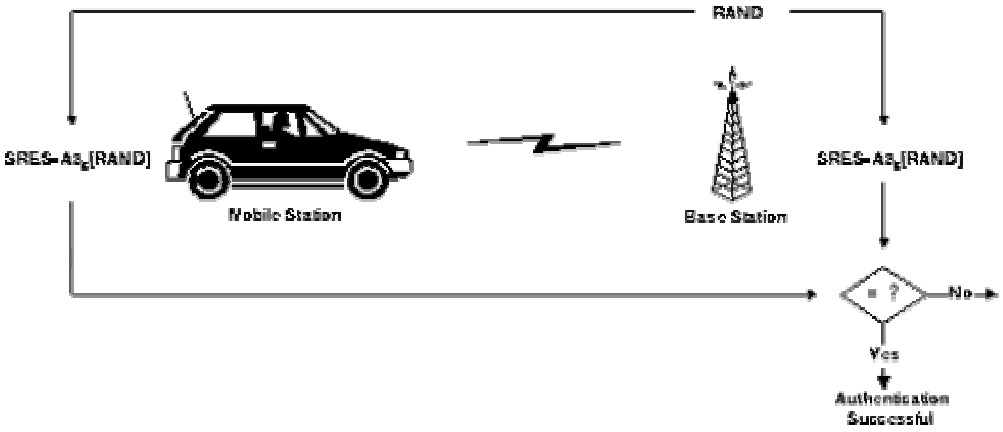
```
    90,149, 39,120,230, 87,232,106, 19,175,190,126,141,202,176,137,
    27,250, 40,101,227,219, 20, 58,178, 51,216, 98, 22,140,121, 32,
   103, 61, 72,203,110, 29,212, 85,204,180,183,150, 66, 15,196,172,
   197, 56,  0,158, 45,100,  7,153,222,144,167,163,135, 60,231,210,
   165,174,249, 38, 34,224,229,220,208,217, 68,241,189,206,255,125,
    54,239, 89,168,122,123,145, 73,234,117, 99,143,200,129, 82,192,
   170,104,235,136, 81, 93,173,205, 94,236, 52,105,228, 46,  5,198,
   254, 57,155, 97,133,142,171,199, 50,187,181, 65,107,127,226,147,
   218,184, 33,131, 86, 77, 44, 31, 62, 88, 18,238, 43, 24, 23,154,
   159, 80,111,134,114,  9, 91,  3,130, 16, 10, 83,240,195,119,253
}, table_1[256] = {
    19, 11, 80,114, 43,  1, 69, 94, 39, 18,127,117, 97,  3, 85, 43,
    27,124, 70, 83, 47, 71, 63, 10, 47, 89, 79,  4, 14, 59, 11,  5,
    35,107,103, 68, 21, 86, 36, 91, 85,126, 32, 50,109, 94,120,  6,
    53, 79, 28, 45, 99, 95, 41, 34, 88, 68, 93, 55,110,125,105, 20,
    90, 80, 76, 96, 23, 60, 89, 64,121, 56, 14, 74,101,  8, 19, 78,
    76, 66,104, 46,111, 50, 32,  3, 39,  0, 58, 25, 92, 22, 18, 51,
    57, 65,119,116, 22,109,  7, 86, 59, 93, 62,110, 78, 99, 77, 67,
    12,113, 87, 98,102,  5, 88, 33, 38, 56, 23,  8, 75, 45, 13, 75,
    95, 63, 28, 49,123,120, 20,112, 44, 30, 15, 98,106,  2,103, 29,
    82,107, 42,124, 24, 30, 41, 16,108,100,117, 40, 73, 40,  7,114,
    82,115, 36,112, 12,102,100, 84, 92, 48, 72, 97,  9, 54, 55, 74,
   113,123, 17, 26, 53, 58,  4,  9, 69,122, 21,118, 42, 60, 27, 73,
   118,125, 34, 15, 65,115, 84, 64, 62, 81, 70,  1, 24,111,121, 83,
   104, 81, 49,127, 48,105, 31, 10,  6, 91, 87, 37, 16, 54,116,126,
    31, 38, 13,  0, 72,106, 77, 61, 26, 67, 46, 29, 96, 37, 61, 52,
   101, 17, 44,108, 71, 52, 66, 57, 33, 51, 25, 90,  2,119,122, 35
}, table_2[128] = {
    52, 50, 44,  6, 21, 49, 41, 59, 39, 51, 25, 32, 51, 47, 52, 43,
    37,  4, 40, 34, 61, 12, 28,  4, 58, 23,  8, 15, 12, 22,  9, 18,
    55, 10, 33, 35, 50,  1, 43,  3, 57, 13, 62, 14,  7, 42, 44, 59,
    62, 57, 27,  6,  8, 31, 26, 54, 41, 22, 45, 20, 39,  3, 16, 56,
    48,  2, 21, 28, 36, 42, 60, 33, 34, 18,  0, 11, 24, 10, 17, 61,
    29, 14, 45, 26, 55, 46, 11, 17, 54, 46,  9, 24, 30, 60, 32,  0,
    20, 38,  2, 30, 58, 35,  1, 16, 56, 40, 23, 48, 13, 19, 19, 27,
    31, 53, 47, 38, 63, 15, 49,  5, 37, 53, 25, 36, 63, 29,  5,  7
}, table_3[64] = {
     1,  5, 29,  6, 25,  1, 18, 23, 17, 19,  0,  9, 24, 25,  6, 31,
    28, 20, 24, 30,  4, 27,  3, 13, 15, 16, 14, 18,  4,  3,  8,  9,
    20,  0, 12, 26, 21,  8, 28,  2, 29,  2, 15,  7, 11, 22, 14, 10,
    17, 21, 12, 30, 26, 27, 16, 31, 11,  7, 13, 23, 10,  5, 22, 19
}, table_4[32] = {
    15, 12, 10,  4,  1, 14, 11,  7,  5,  0, 14,  7,  1,  2, 13,  8,
    10,  3,  4,  9,  6,  0,  3,  2,  5,  6,  8,  9, 11, 13, 15, 12
}, *table[5] = { table_0, table_1, table_2, table_3, table_4 };

/*
```

```
 * The relevant bits are in Part I, Section 20 (pages 66--67).
 *
 * Note: There are three typos in the spec (discovered by
 * reverse-engineering).
 * First, "z = (2 * x[n] + x[n]) mod 2^(9-j)" should clearly read
 * "z = (2 * x[m] + x[n]) mod 2^(9-j)".
 * Second, the "k" loop in the "Form bits from bytes" section is severely
 * botched: the k index should run only from 0 to 3, and clearly the range
 * on "the (8-k)th bit of byte j" is also off (should be 0..7, not 1..8,
 * to be consistent with the subsequent section).
 * Third, SRES is taken from the first 8 nibbles of x.
 */

void A3A8(/* in */ Byte rand[16], /* in */ Byte key[16],
        /* out */ Byte simoutput[12])
{
        Byte x[32], bit[128];
        int i, j, k, l, m, n, y, z, next_bit;

        /* ( Load RAND into last 16 bytes of input ) */
        for (i=16; i<32; i++)
                x[i] = rand[i-16];

        /* ( Loop eight times ) */
        for (i=1; i<9; i++) {
                /* ( Load key into first 16 bytes of input ) */
                for (j=0; j<16; j++)
                        x[j] = key[j];
                /* ( Perform substitutions ) */
                for (j=0; j<5; j++)
                        for (k=0; k<(1<<j); k++)
                                for (l=0; l<(1<<(4-j)); l++) {
                                        m = l + k*(1<<(5-j));
                                        n = m + (1<<(4-j));
                                        y = (x[m]+2*x[n]) % (1<<(9-j));
                                        z = (2*x[m]+x[n]) % (1<<(9-j));
                                        x[m] = table[j][y];
                                        x[n] = table[j][z];
                                }
                /* ( Form bits from bytes ) */
                for (j=0; j<32; j++)
                        for (k=0; k<4; k++)
                                bit[4*j+k] = (x[j]>>(3-k)) & 1;
                /* ( Permutation but not on the last loop ) */
                if (i < 8)
                        for (j=0; j<16; j++) {
                                x[j+16] = 0;
```

```
                        for (k=0; k<8; k++) {
                                next_bit = ((8*j + k)*17) % 128;
                                x[j+16] |= bit[next_bit] << (7-k);
                        }
                }
        }

        /*
         * ( At this stage the vector x[] consists of 32 nibbles.
         *   The first 8 of these are taken as the output SRES. )
         */

        for (i=0; i<4; i++)
                simoutput[i] = (x[2*i]<<4) | x[2*i+1];
        for (i=0; i<6; i++)
                simoutput[4+i] = (x[2*i+18]<<6) | (x[2*i+18+1]<<2)
                                | (x[2*i+18+2]>>2);
        simoutput[4+6] = (x[2*6+18]<<6) | (x[2*6+18+1]<<2);
        simoutput[4+7] = 0;
}


#ifdef TEST
int hextoint(char x)
{
        x = toupper(x);
        if (x >= 'A' && x <= 'F')
                return x-'A'+10;
        else if (x >= '0' && x <= '9')
                return x-'0';
        fprintf(stderr, "bad input.\n");
        exit(1);
}

int main(int argc, char **argv)
{
        Byte key[16], rand[16], simoutput[12];
        int i;

        if (argc != 3 || strlen(argv[1]) != 34 || strlen(argv[2]) != 34
                        || strncmp(argv[1], "0x", 2) != 0
                        || strncmp(argv[2], "0x", 2) != 0) {
                fprintf(stderr, "Usage: %s 0x<key> 0x<rand>\n", argv[0]);
                exit(1);
        }

        for (i=0; i<16; i++)
```

```
            key[i] = (hextoint(argv[1][2*i+2])<<4)
                    | hextoint(argv[1][2*i+3]);
    for (i=0; i<16; i++)
            rand[i] = (hextoint(argv[2][2*i+2])<<4)
                    | hextoint(argv[2][2*i+3]);
    A3A8(key, rand, simoutput);
    printf("simoutput: ");
    for (i=0; i<12; i++)
            printf("%02X", simoutput[i]);
    printf("\n");
    return 0;
}
#endif
```

Механизм аутентификации.



Для исключения несанкционированного использования ресурсов системы связи вводятся механизмы аутентификации - удостоверения подлинности абонента. Центр аутентификации состоит из нескольких блоков и формирует ключи и алгоритмы аутентификации. С его помощью проверяются полномочия абонента и осуществляется его доступ к сети связи. AUC принимает решения о параметрах процесса аутентификации и определяет ключи шифрования абонентских станций на основе базы данных, сосредоточенной в регистре идентификации оборудования (EIR - Equipment Identification Register). Каждый подвижный абонент на время пользования системой связи получает стандартный модуль подлинности абонента (SIM), который содержит: международный идентификационный номер (IMSI), свой индивидуальный ключ аутентификации (Ki), алгоритм аутентификации (A3). С помощью записанной в SIM информации в результате взаимного обмена данными между подвижной станцией и сетью осуществляется полный цикл аутентификации и разрешается доступ абонента к сети. Процедура проверки сетью подлинности абонента реализуется следующим образом. Сеть передает случайный 128-битовый номер (RAND) на подвижную станцию. На ней с помощью Ki и алгоритма аутентификации A3 определяется значение 32-битового отклика (SRES), т.е.

SRES = Ki * [RAND]

Подвижная станция посылает вычисленное значение SRES в сеть, которая сверяет значение принятого SRES со значением SRES, вычисленным сетью. Если оба значения совпадают, подвижная станция приступает к передаче сообщений. В противном случае связь прерывается, и индикатор подвижной станции показывает, что опознавание не состоялось. Для обеспечения секретности вычисление SRES происходит в рамках SIM. Несекретная информация (например, Ki) не подвергается обработке в модуле SIM.

Структура TDMA кадров и формирование сигналов.

В результате анализа различных вариантов построения цифровых сотовых систем подвижной связи (ССПС) в стандарте GSM принят многостанционный доступ с временным разделением каналов (TDMA). Общая структура временных кадров показана на рис**.** 2. Длина периода последовательности в этой структуре, которая называется гиперкадром, равна Тг = 3 ч 28 мин 53 с 760 мс (12533,76 с). Гиперкадр делится на 2048 суперкадров, каждый из которых имеет длительность Те = 12533,76/2048 = 6,12 с.

Суперкадр состоит из мультикадров. Для организации различных каналов связи и управления в стандарте GSM используются два вида мультикадров:

1) 26-позиционные TDMA кадры мультикадра;
2) 51-позиционные TDMA кадры мультикадра.

Суперкадр может содержать в себе 51 мультикадр первого типа или 26 миультикадров второго типа. Длительности мультикадров соответственно:

1) **Тм= 6120/51 = 120 мс**
2) **Тм = 6120/26 = 235,385 мс (3060/13 мс)**

Длительность каждого TDMA кадра

Тк = 120/26 = 235,385/51 = 4,615 мс (60/13 мс)

В периоде последовательности каждый TDMA кадр имеет свой порядковый номер (NF) от О до NFmax, где

NFmax = (26x51x2048) -1 = 2715647

Таким образом, гиперкадр состоит из 2715647 TDMA кадров. Необходимость такого большого периода гиперкадра объясняется требованиями применяемого процесса криптографической защиты, в котором номер кадра NF используется как входной параметр. TDMA кадр делится на восемь временных позиций с периодом

То = 60/13:8 = 576,9 мкс (15/26 мс)

Каждая временная позиция обозначается TN с номером от 0 до 7. Физический смысл временных позиций, которые иначе называются окнами, - время, в течение которого осуществляется модуляция несущей цифровым информационным потоком, соответствующим речевому сообщению или данным.

Цифровой информационный поток представляет собой последовательность пакетов, размещаемых в этих временных интервалах (окнах). Пакеты формируются немного короче, чем интервалы, их длительность составляет 0,546 мс, что необходимо для приема сообщения при наличии временной дисперсии в канале распространения.

Информационное сообщение передается по радиоканалу со скоростью 270,833 кбит/с. Это означает, что временной интервал TDMA кадра содержит 156,25 бит.
Длительность одного информационного бита 576,9 мкс/156,25 = 3,69 мкс.

Каждый временной интервал, соответствующий длительности бита, обозначается BN с номером от 0 до 155; последнему интервалу длительностью 1/4 бита присвоен номер 156.

Для передачи информации по каналам связи и управления, подстройки несущих частот, обеспечения временной синхронизации и доступа к каналу связи в структуре TDMA кадра используются пять видов временных интервалов (окон):

NB используется для передачи информации по каналам связи и управления, за исключением канала доступа RACH. Он состоит из 114 бит зашифрованного сообщения и включает защитный интервал (GP) в 8,25 бит длительностью 30,46 мкс. Информационный блок 114 бит разбит на два самостоятельных блока по 57 бит, разделенных между собой обучающей последовательностью в 26 бит, которая используется для установки эквалайзера в приемнике в соответствии с характеристиками канала связи в данный момент времени. В состав NB включены два контрольных бита (Steeling Flag), которые служат признаком того, содержит ли передаваемая группа речевую информацию или информацию сигнализации. В последнем случае информационный канал (Traffic Channel) "украден" для обеспечения сигнализации.

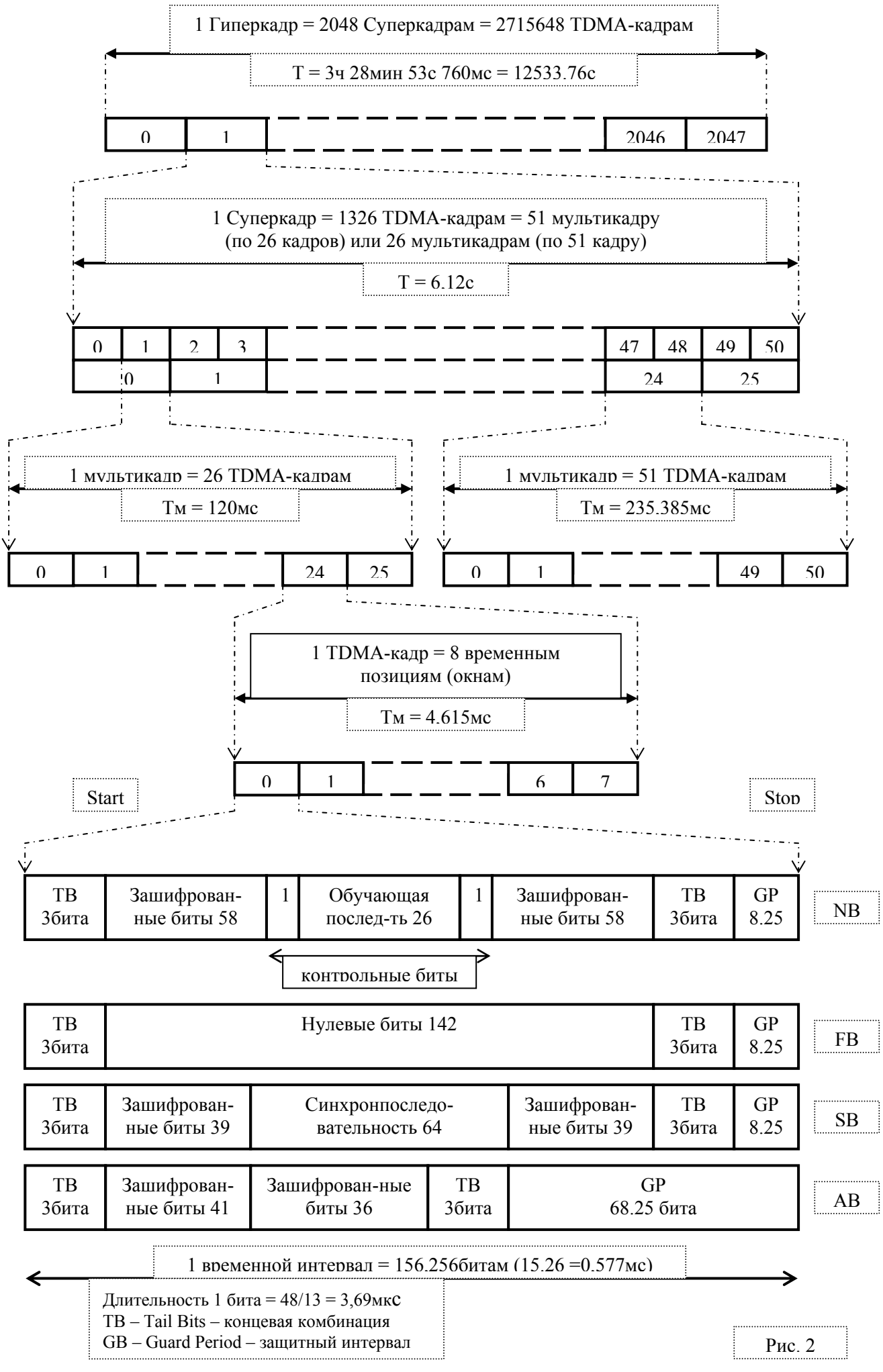

1 Гиперкадр = 2048 Суперкадрам = 2715648 TDMA-кадрам
T = 3ч 28мин 53с 760мс = 12533.76с
0
1
2046
2047
1 Суперкадр = 1326 TDMA-кадрам = 51 мультикадру
(по 26 кадров) или 26 мультикадрам (по 51 кадру)
T = 6.12с
0
1
2
3
47
48
49
50
0
1
24
25
1 мультикадр = 26 TDMA-кадрам
Тм = 120мс
1 мультикадр = 51 TDMA-кадрам
Тм = 235.385мс
0
1
24
25
0
1
49
50
1 TDMA-кадр = 8 временным
позициям (окнам)
Тм = 4.615мс
0
1
6
7
Start
Stop
ТВ
3бита
Зашифрован-
ные биты 58
1
Обучающая
послед-ть 26
1
Зашифрован-
ные биты 58
ТВ
3бита
GP
8.25
NB
контрольные биты
ТВ
3бита
Нулевые биты 142
ТВ
3бита
GP
8.25
FB
ТВ
3бита
Зашифрован-
ные биты 39
Синхронпоследо-
вательность 64
Зашифрован-
ные биты 39
ТВ
3бита
GP
8.25
SB
ТВ
3бита
Зашифрован-
ные биты 41
Зашифрован-ные
биты 36
ТВ
3бита
GP
68.25 бита
AB
1 временной интервал = 156.256битам (15.26 =0.577мс)
Длительность 1 бита = 48/13 = 3,69мкс
ТВ – Tail Bits – концевая комбинация
GB – Guard Period – защитный интервал

Рис. 2

Между двумя группами зашифрованных бит в составе NB находится обучающая последовательность из 26 бит, известная в приемнике. С помощью этой последовательности обеспечивается:

- оценка частоты появления ошибок в двоичных разрядах по результатам сравнения принятой и эталонной последовательностей. В процессе сравнения вычисляется параметр RXQUAL, принятый для оценки качества связи. Конечно, речь идет только об оценке связи, а не о точных измерениях, так как проверяется только часть передаваемой информации. Параметр RXQUAL используется при вхождении в связь, при выполнении процедуры "эстафетной передачи" (Handover) и при оценке зоны покрытия радиосвязью;

- оценка импульсной характеристики радиоканала на интервале передачи NB для последующей коррекции тракта приема сигнала за счет использования адаптивного эквалайзера в тракте приема;

-определение задержек распространения сигнала между базовой и подвижной станциями для оценки дальности связи. Эта информация необходима для того, чтобы пакеты данных от разных подвижных станций не накладывались при приеме на базовой станции. Поэтому удаленные на большее расстояние подвижные станции должны передавать свои пакеты раньше станций, находящихся в непосредственной близости от базовой станции. FB предназначен для синхронизации по частоте подвижной станции.

Все 142 бита в этом временном интервале - нулевые, что соответствует немодулированной несущей со сдвигом 1625/24 кГц выше номинального значения частоты несущей. Это необходимо для проверки работы своего передатчика и приемника при небольшом частотном разносе каналов (200 кГц), что составляет около 0,022% от номинального значения полосы частот 900 МГц.

FB содержит защитный интервал 8,25 бит так же, как и нормальный временной интервал. Повторяющиеся временные интервалы подстройки частоты (FB) образуют канал установки частоты (FCCH).

SB используется для синхронизации по времени базовой и подвижной станций. Он состоит из синхропоследовательности длительностью 64 бита, несет информацию о номере ТОМА кадра и идентификационный код базовой станции. Этот интервал передается вместе с интервалом установки частоты. Повторяющиеся интервалы синхронизации образуют так называемый канал синхронизации (SCH).

DB обеспечивает установление и тестирование канала связи. По своей структуре DB совпадает с NB (рис. 1.6) и содержит установочную последовательность длиной 26 бит. В DB отсутствуют контрольные биты и не передается никакой информации. DB лишь информирует о том, что передатчик функционирует.

AB обеспечивает разрешение доступа подвижной станции к новой базовой станции. AB передается подвижной станцией при запросе канала сигнализации. Это первый передаваемый подвижной станцией пакет, следовательно, время прохождения сигнала еще не измерено. Поэтому пакет имеет специфическую структуру.

Сначала передается концевая комбинация 8 бит, затем - последовательность синхронизации для базовой станции (41 бит), что позволяет базовой станции обеспечить правильный прием последующих 36 зашифрованных бит. Интервал содержит большой защитный интервал (68,25 бит, длительностью 252 мкс), что обеспечивает (независимо от времени прохождения сигнала) достаточное временное разнесение от пакетов других подвижных станций. Этот защитный интервал соответствует двойному значению наибольшей возможной задержки сигнала в рамках одной соты и тем самым устанавливает максимально допустимые размеры соты. Особенность стандарта GSM - возможность обеспечения связью подвижных абонентов в сотах с радиусом около 35 км. Время распространения радиосигнала в прямом и обратном направлениях составляет при этом 233,3 мкс.

Литература.

- M.Mouly, M.B.Pautet. The GSM System for Mobile Communications. 1992. p.p. 702.
- Ю.А. Громаков. Сотовые системы подвижной радиосвязи. Технологии электронныхкоммуникаций. Том 48. "Эко-Трендз". Москва. 1994.
- A. Mehrotra. Cellular Radio: Analog and Digital Systems. Artech House, Boston-London. 1994. p.p. 460.
- Ю.А. Громаков. Структура TDMA кадров и формирование сигналов в стандарте GSM. "Электросвязь". N 10. 1993. с. 9-12.
- W. Heger. GSM vs. CDMA. GSM Global System for Mobile Communications. Proceedings of the GSM Promotion Seminar 1994 GSM MoU Group in Cooperation with ETSI GSM Members. 15 December 1994. p.p. 3.1-1 - 3.1-18.
- Hardcopy from anonymous 3 March 1997.