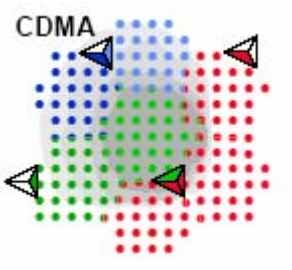


Защищенность CDMA сетей

Security of CDMA Networks

автор: **Иванова Татьяна Геннадьевна**

История CDMA

Долгое время технология CDMA применялась исключительно в военных целях. Уже после войны в течение долгого времени технология CDMA использовалась в военных системах связи как в СССР, так и в США, поскольку обладала многими ценными для таких систем преимуществами, о которых будет сказано ниже.

Чтобы понять на примитивном уровне, как работает CDMA, представьте себе комнату, в которой одновременно разговаривает друг с другом много пар людей, причем на разных языках. Каждый из них хорошо понимает своего собеседника, а все посторонние разговоры воспринимаются как некий фон и не особенно мешают разговору. Таким образом, в одном и том же радиочастотном канале одновременно передаются информационные сигналы большой группы пользователей.

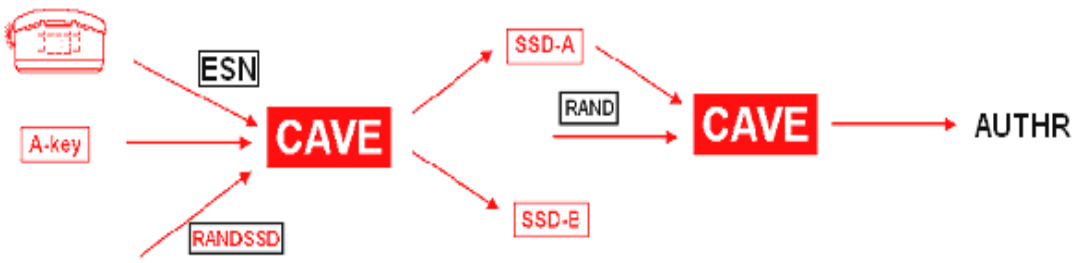
Система аутентификации

В каждом телефоне хранится два числа:
-- A-key – это 64-х битное число-ключ, которое вводится при продаже телефона и хранится в базе. Поскольку A-key не передается в эфир, его нельзя перехватить и использовать, как это делалось с серийными номерами.
-- ESN (Electronic Serial Number) – 32-битный код, присваиваемый мобильному телефону при его изготовлении и используемый для идентификации.

Итак, как же работает система аутентификации? При включении телефона станция передает ему случайное число RANDSSD. На основе A-key, ESN, MIN и RANSSD с помощью алгоритма шифрования CAVE (Cellular Authentification
and Voice Encryption) генерируется 128-битный подключ SSD (Shared Secret Data) , который состоит из двух частей SSD_A и SSD_B. SSD_A и A-key хранятся в телефоне и на станции и никогда не передаются по сети.

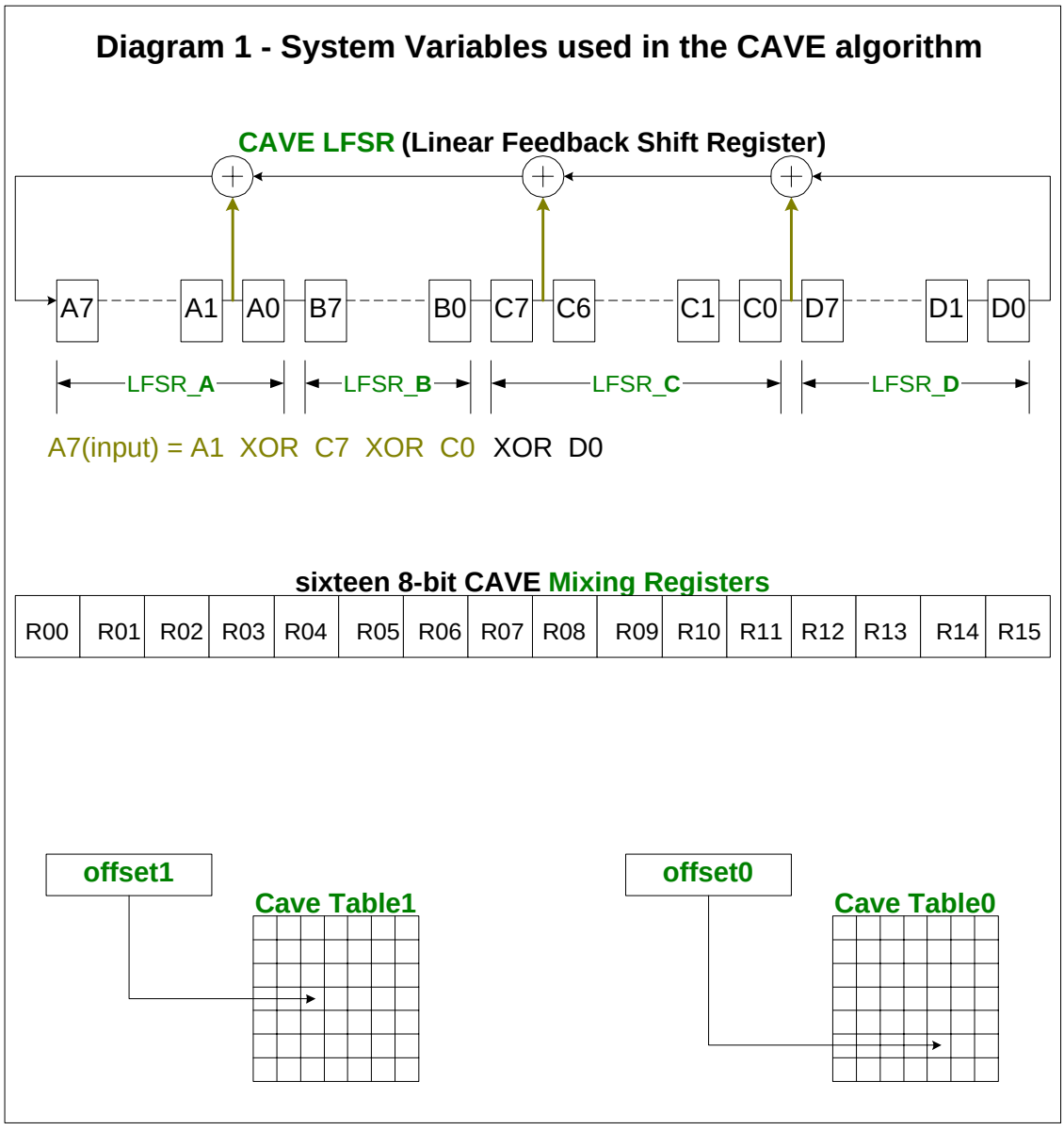
Периодически (примерно один раз в неделю) станция посылает сотовому телефону сообщения о генерации нового временного ключа, SSD_A, при получении этого сообщения (SSD_UPDATE) телефон рассчитывает новый временный ключ SSD_A, используя A-KEY, ESN, MIN, и случайное число со станции. Таким образом, сам ключ аутентификации (SSD_A) является временным и периодически меняется, и становится бессмысленным "клонирование" трубок, а также нахождение SSD_A методом последовательного перебора, поскольку после первого же изменения ключа работать дальше будет только один телефон с новым ключом

С частотой раз в 20 минут базовая станция генерирует 128-битное случайное число RAND и передают его широковещательно. Потом мобильное устройство на основе SSD_A и RAND с помощью алгоритма CAVE генерирует 18-битную цифровую подпись AUTH_SIGNATURE, которая передается по сети на станцию и там сравнивается с независимо подсчитанным числом, вычисленным на базовой станции. Если они не совпадают, то аутентификация считается неудачной, и пользователю отказывают в соединении.



Алгоритм шифрования CAVE

CAVE – это программно-совместимая нелинейная смешивающая функция. Она состоит из трех компонентов:
-- 32-битный LFSR (Linear-Feedback Shift Register)
-- шестнадцать 8-битных смешивающих регистров
-- таблица преобразования, состоящая из 256 элементов



Алгоритм шифрования состоит из трех этапов:

1) Начальная загрузка данных в регистры A,B,C,D, R00-R15
2) Операция смешивания в 4 или 8 раундов при помощи CAVE table и операций с регистрами A,B,C,D
3) Вывод данных

CAVE Table

hi/lo	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	D9	23	5F	E6	CA	68	97	B0	7B	F2	0C	34	11	A5	8D	4E
1	0A	46	77	8D	10	9F	5E	62	F1	34	EC	A5	C9	B3	D8	2B
2	59	47	E3	D2	FF	AE	64	CA	15	8B	7D	38	21	BC	96	00
3	49	56	23	15	97	E4	CB	6F	F2	70	3C	88	BA	D1	0D	AE
4	E2	38	BA	44	9F	83	5D	1C	DE	AB	C7	65	F1	76	09	20
5	86	BD	0A	F1	3C	A7	29	93	CB	45	5F	E8	10	74	62	DE
6	B8	77	80	D1	12	26	AC	6D	E9	CF	F3	54	3A	0B	95	4E
7	B1	30	A4	96	F8	57	49	8E	05	1F	62	7C	C3	2B	DA	ED
8	BB	86	0D	7A	97	13	6C	4E	51	30	E5	F2	2F	D8	C4	A9
9	91	76	F0	17	43	38	29	84	A2	DB	EF	65	5E	CA	0D	BC
A	E7	FA	D8	81	6F	00	14	42	25	7C	5D	C9	9E	B6	33	AB
B	5A	6F	9B	D9	FE	71	44	C5	37	A2	88	2D	00	B6	13	EC
C	4E	96	A8	5A	B5	D7	C3	8D	3F	F2	EC	04	60	71	1B	29
D	04	79	E3	C7	1B	66	81	4A	25	9D	DC	5F	3E	B0	F8	A2
E	91	34	F6	5C	67	89	73	05	22	AA	CB	EE	BF	18	D0	4D
F	F5	36	AE	01	2F	94	C3	49	8B	BD	58	12	E0	77	6C	DA

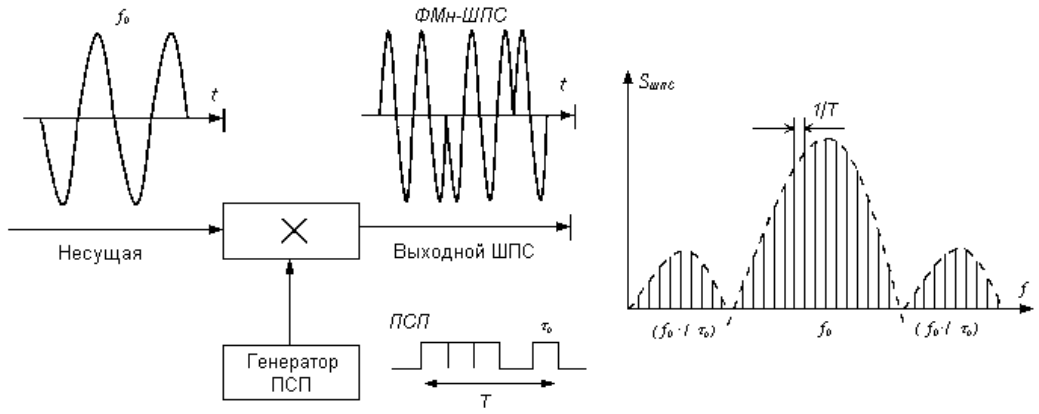
Кодовое разделение пользователей

Как уже было сказано, в стандарте CDMA несколько пар пользователей работают в одном и том же диапазоне частот. Для разделения пользователей используется код Уолша. Он формируется из строк матрицы вида:

$$W_L = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}$$

Особенность этой матрицы состоит в том, что каждая ее строка ортогональна любой другой или строке, полученной с помощью операции логического отрицания. В стандарте CDMA матрица состоит из 64 строк. Для выделения сигнала на выходе приемника применяется цифровой фильтр. При ортогональных сигналах фильтр можно настроить таким образом, что на его выходе всегда будет логический «0», за исключением случаев, когда принимается сигнал, на который он настроен. Таким образом, при соединении пользователей им обоим передается один и тот же код Уолша, который позволяет говорить на «одном и том же языке».

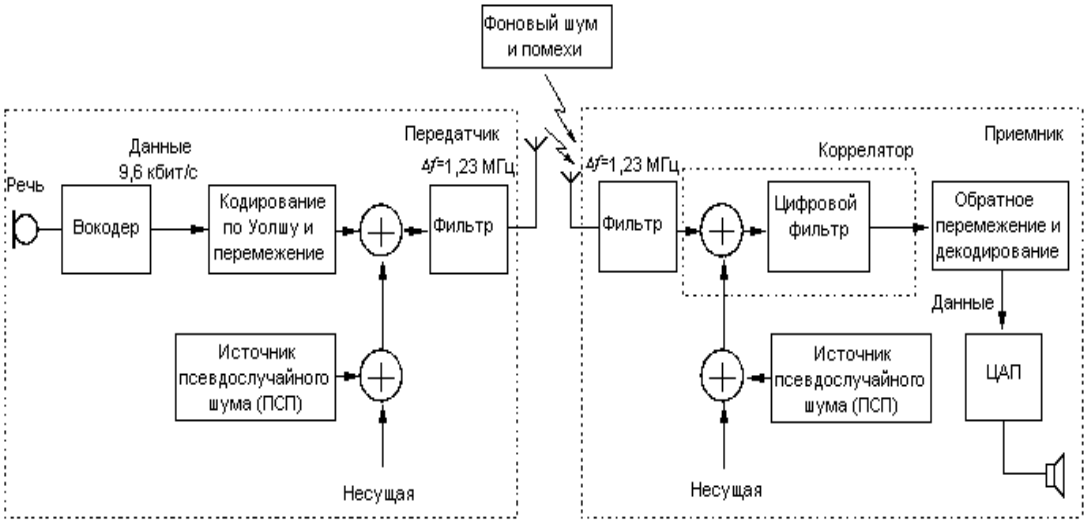
После кодирования по Уолшу информация должна быть введена в широкополосный сигнал (ШПС). Наиболее известный способ заключается в наложении информации на широкополосную модулирующую кодовую последовательность перед модуляцией несущей для получения шумоподобного широкополосного сигнала (ШШС). Узкополосный сигнал умножается на псевдослучайную последовательность (ПСП) с периодом T, состоящую из N бит длительностью t_0 каждый. В этом случае база ШПС численно равна количеству элементов ПСП.



В системах, использующих метод CDMA, изменяя синхронизацию источника псевдослучайного шума, можно использовать один и тот же участок полосы частот для работы во всех ячейках сети. Такое 100%-ное использование доступного частотного ресурса - один из основных факторов, определяющих высокую абонентскую емкость сети стандарта

CDMA и упрощающих ее организацию. Системы на базе CDMA имеют динамическую абонентскую емкость. И хотя имеется 64 кода Уолша, этот теоретический предел не достигается в реальных условиях, и абонентская емкость системы ограничивается внутрисистемной интерференцией, вызванной одновременной работой подвижных и базовых станций соседних ячеек.

Число абонентов в системе CDMA зависит от уровня взаимных помех. Согласованные фильтры базовой станции весьма чувствительны к эффекту «ближний-дальний» (far-near problem), когда мобильная станция, расположенная вблизи базовой, работает на большой мощности, создавая недопустимо высокий уровень помех при приеме других, «дальних» сигналов, что приводит к снижению пропускной способности системы в целом. Эта проблема существует у всех стандартов мобильной связи, однако наибольшие искажения сигнала возникают именно в CDMA-системах, работающих в общей полосе частот, в которых используются ортогональные шумоподобные сигналы. Если бы в этих системах отсутствовала регулировка мощности, то они существенно уступали бы по характеристикам сотовым сетям на базе TDMA. Поэтому ключевой проблемой в CDMA-системах можно считать индивидуальное управление мощностью каждой станции.



Шифрование данных в стандарте CDMA

Для шифрования данных используется подключ SSD_B. С помощью него генерируется Data-key. Голосовые данные передаются по сети после шифрования алгоритмом ORYX при использовании ключа DATA-key.

Служебные сообщения кодируются при помощи CMEA (Cellular Message Encryption Algorithm).

Недостатки и преимущества стандарта CDMA

К недостаткам стандарта CDMA можно отнести:

1) необходима система регулировки мощности для того, чтобы уровень помех от соседних мобильных станций.
2) Дорогостоящее оборудование

Преимущества стандарта CDMA:

1) в отличии от ESN A-key никогда не передается по сети. Следовательно он недоступен подслушивателям. Криптоаналитики могут обойти эту проблему только клонированием телефона. Но раз в неделю SSD_A будет обновляться и следовательно это приведет в отключению клона от сети
2) любые операции по криптоанализу дорогостоящие и доступны практически только спецслужбам

Список используемой литературы

1) *Christopher Wingert, Mullaguru Naidu* "CDMA Security OverView"
http://www.cdg.org/technology/cdma_technology/white_papers/cdma_1x_security_overview.pdf
2) Кунегин С.В. «Сотовые сети стандарта CDMA»
http://kunegin.narod.ru/ref3/mob/index.htm