Московский физико-технический институт

БЕЗОПАСНОСТЬ СВЯЗИ В ТРАНКИНГОВЫХ СИСТЕМАХ СТАНДАРТА TETRA

Птушкин Д.А.

011 гр.

БЕЗОПАСНОСТЬ СВЯЗИ В ТРАНКИНГОВЫХ СИСТЕМАХ СТАНДАРТА TETRA

В настоящее время немыслимо представить мир без современных средств связи. Чем больше развиваются беспроводные технологии, тем больше приходится обращать внимание на безопасность передачи данных, прибегать к шифрованию с целью сохранения конфиденциальности. Существует много различных стандартов связи, в каждом из которых защита передаваемой информации реализована по-своему. Выбор остается за потребителем.

Одной из «прогрессирующих» систем на современном рынке связи является система TETRA, что означает Terrestrial Trunked Radio (до 1997 года аббревиатура расшифровывалась как Trans-European Trunked Radio). Она была разработана Европейским институтом телекоммуникационных стандартов ETSI (European Telecommunication Standards Institute).

Система TETRA сочетает в себе функциональность сотового мобильного телефона и радиостанции. Она позволяет строить разветвленные сети связи с высоким уровнем предоставляемых услуг на больших территориях, с возможностью группового соединения абонентов. Поэтому TETRA стала популярной среди различных служб общественной безопасности.

Основным конкурентом для TETRA выступает обычная сотовая связь. Однако простое сравнение характеристик говорит о том, что транкинговая система, в отличии от обычных сотовых сетей, - это система *профессиональной* радиосвязи. Остановимся на некоторых отличительных особенностях системы TETRA (полное сравнение можно найти здесь: http://ra3apw.by.ru/tetra/vscel.html):

- малое время установления связи (300 мс против нескольких секунд в GSM)
- возможность группового вызова
- возможность работы без инфраструктуры (возможна связь абонентов «напрямую», т.е. без участия базовой станции)
- размер зоны обслуживания одной базовой станцией достигает нескольких десятков километров (против нескольких километров в GSM)
- повышенная защищенность каналов связи

Есть также ряд услуг, которые присущи только стандарту TETRA, а именно:

- вызов, санкционированный диспетчером (оператором базовой станции)
- предоставление сервиса в определенной зоне обслуживания (например, возможность *выборочного* прослушивания линий, в то время как в сетях GSM отключение режима шифрования голоса касается *всех* абонентов)
- динамическое создание групп абонентов
- приоритетный вызов с разъединением абонентов с меньшим приоритетом
- дистанционный мониторинг окружающей обстановки
- мониторинг вызовов между другими абонентами
- приоритетный доступ к радиоресурсам с разъединением абонентов с меньшим приоритетом
- присоединение к групповому вызову после его установления

Кроме того, TETRA – это стандарт, которому, как и другим стандартам цифровой связи, свойственно предоставление такой услуги, как передача данных: режим коротких сообщений SDS, возможность реализации IP over TETRA (благодаря коммутации пакетов или каналов) и, следовательно, возможность использования всего богатства сервисов стека протоколов TCP/IP (e-mail, HTTP, FTP, WAP и т.д.), причем скорость передачи в TETRA значительно превосходит соответствующие значения в сетях аналоговой транкинговой связи.

Преимуществом TETRA для потребителей является не только современная технология с большим потенциалом возможностей, но и то, что TETRA – открытый стандарт. На современном рынке представлено оборудование TETRA ведущих мировых производителей систем связи.

Существует три режима функционирования систем TETRA:

- режим транкинговой связи
- режим связи с открытым каналом
- режим непосредственной связи

В режиме транкинговой связи обслуживаемая территория охватывается зонами действия базовых станций. Этот режим напоминает работу сотовых сетей.

В режиме с открытым каналом у абонентов есть возможность использовать так называемый *групповой вызов* и устанавливать соединение «один абонент – несколько абонентов». В этом случае говорят, что канал «открыт» для использования группой абонентов.

Режим непосредственной связи обеспечивает установление соединения между абонентами «напрямую», без передачи сигналов через базовые приемо-передающие станции.

Анализ способов распределения каналов связи показывает, что TETRA может использовать два вида мультиплексирования цифровых потоков: узкополосный TDMA и FDMA (time/frequency division multiplexing). В первом случае резервируется выделенный частотный канал, в котором «полезная» информация и информация управления передаются *по очереди* (технология тайм-слотирования). Один частотный канал разбивается на четыре временных, по одному из которых передаётся служебная информация. В случае FDMA используются несколько частотных каналов, один из которых отводится для передачи служебной информации *одновременно* с полезной информацией, передающейся по другим частотным каналам.

Основной причиной, по которой стандарт TETRA стал популярен среди правоохранительных органов, является повышенная безопасность связи.

Стандартом обеспечивается два уровня безопасности:

- стандартный уровень, использующий шифрование радиоинтерфейса (аналогично системе сотовой связи GSM)
- высокий уровень, использующий сквозное шифрование (от источника до получателя)

Защита радиоинтерфейса включает в себя механизмы аутентификации абонента и инфраструктуры, а также обеспечение конфиденциальности трафика, которая

достигается за счет потока псевдоимен и специфицированного шифрования информации. А возможность переключения информационных каналов и каналов управления во время сеанса связи обеспечивает дополнительную защиту.

Определенным группам абонентов может потребоваться более высокий уровень конфиденциальности. Для этого применяется режим *сквозного шифрования*, который обеспечивает защиту данных в любой точке линии связи между абонентами. Причем TETRA не привязывается к какому-то определенному алгоритму, задавая только интерфейс для сквозного шифрования, а ответственность за использование того или иного способа защиты (одного из 4-х, предложенных данной технологией) «ложится на плечи» абонента.

Сквозное шифрование – шифрование на верхних уровнях модели OSI. При таком подходе нет необходимости расшифровывать сообщение в каждом узле сети, чтобы извлечь из кода маршрутную информацию, т.к. она передается в открытом виде. Это положительным образом сказывается на быстродействии сети, однако существенно ухудшается защищенность трафика. Как отправитель, так и получатель должны обладать одинаковым набором ключей. Существуют более надежные методы шифрования (например, *канальное,* при котором каждый узел «знает» ключи только своих соседей, или *комбинированное* – сквозное + канальное), но в TETRA они не применяются из-за своей «медлительности».

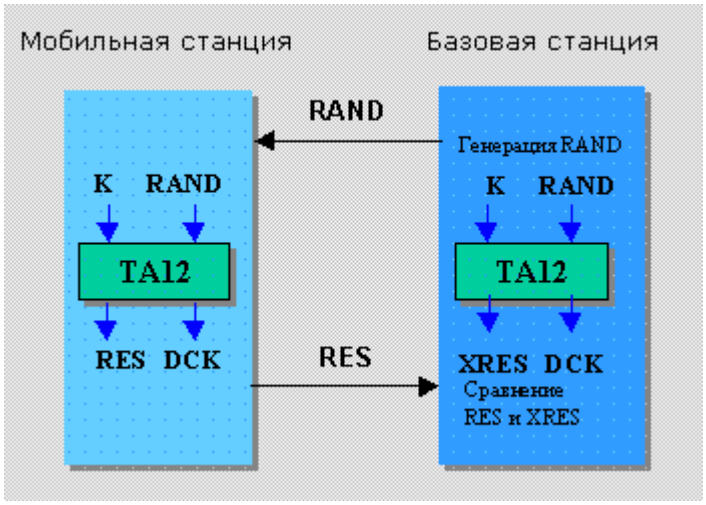
Для обеспечения конфиденциальности информации стандарт определяет следующие механизмы:

- аутентификация абонентов
- шифрование передаваемой информации
- обеспечение скрытности номера абонента

Для обмена данными станции используют единый пароль, который может быть фиксированным, а может зависеть от передаваемых данных. Этот пароль передается отправителем в теле сообщения, затем извлекается из принятого сообщения получателем, сравнивается с оригинальным паролем и на основе сравнения выносится решение: принимать сообщение (отправитель санкционированный) либо отвергать.

Аутентификация абонента – это способ опознавания его подлинности с целью обеспечения защиты ресурсов сети от несанкционированного доступа.

Для выполнения процедуры аутентификации абонент получает так называемый электронный модуль подлинности (проще говоря, SIM-карту), в котором записан уникальный ключ и алгоритм аутентификации. С помощью этой информации базовая станция решает, допустить абонента к ресурсам сети или нет. Ниже приведен рисунок, изображающий обобщенный цикл аутентификации в системе TETRA.



Обобщенная процедура аутентификации в стандарте TETRA

Базовая станция (БС) посылает случайное число RAND на мобильную станцию. Получив это число, мобильная станция преобразует его с помощью стандартного криптографического алгоритма TA12, используя индивидуальный ключ идентификации абонента К, и формирует отклик - число RES, которое затем отправляет обратно на БС.

БС аналогичным способом вычисляет отклик XRES и сравнивает его с полученным значением RES. Если числа совпадают, то процедура аутентификации завершается и мобильная станция получает доступ к ресурсам сети. Если же значение RES не совпадает с ожидаемым значением (XRES), то индикатор мобильной станции информирует о сбое аутентификации, и связь прерывается.

Следует отметить, что на основе случайного числа RAND кроме значения RES формируется так называемый *выделенный ключ шифра* DCK (Derived Cipher Key) – индивидуальный ключ идентификации абонента, который в дальнейшем может применяться для ведения связи в режиме сквозного шифрования.

Этот же алгоритм может использоваться для аутентификации сети абонентом, которая обычно имеет место при регистрации его в определенной зоне сети. Данная процедура также может вызываться в любое другое время после регистрации.

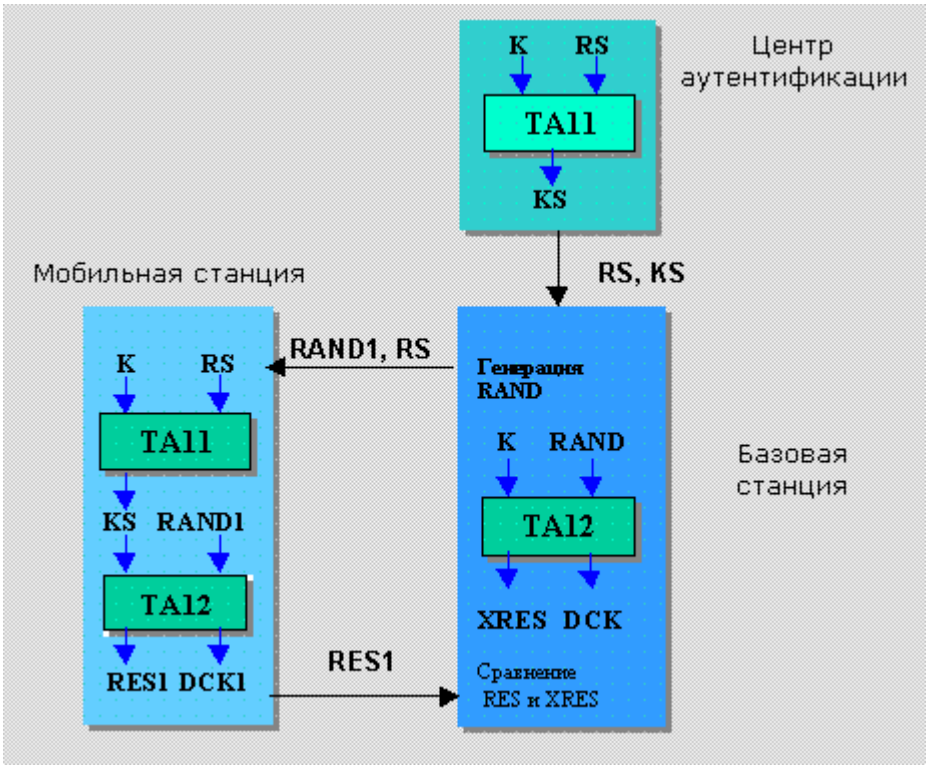
Такой подход к аутентификации абонента или сети обладает существенным недостатком. Здесь предполагается, что базовая станция «знает» все возможные ключи своих абонентов, т.е. эти ключи должны храниться на каждой БС в каком-либо виде. Поэтому есть вероятность того, что злоумышленник, получив доступ к ключам одной из БС, сможет безнаказанно пользоваться ресурсами сети. Чтобы исключить такую ситуацию, в стандарте TETRA применяется иерархическая система ключей, в которой одни ключи защищаются другими. При этом процесс аутентификации аналогичен изображенному на рисунке ниже, где вместо ключа К используется так называемый сеансовый ключ KS, который вычисляется на основе ключа К и некоторого случайного кода RS. Распределением ключей KS по базовым станциям занимается Центр аутентификации, надежно защищенный от вероятных попыток его взлома.

Алгоритм аутентификации с использованием сеансовых ключей

Центр аутентификации генерирует некоторую случайную последовательность RS. Затем, используя код RS, индивидуальный ключ K аутентификации абонента и криптографический алгоритм TA 11, он формирует сеансовый ключ KS. Далее, пара значений (KS, RS) передается на базовую станцию.

Базовая станция генерирует случайное число RAND1 и передает его на мобильную станцию вместе со случайным числом RS.

Мобильная станция восстанавливает сеансовый ключ KS по паре значений (RS, K). Следующим шагом вычисляется значение отклика RES1 по алгоритму TA 12 с использованием пары (KS, RAND1). Также формируется выделенный ключ шифра DCK1. Затем код RES1 передается на базовую станцию и сравнивается с ожидаемым числом XRES1, которое вычисляет сама БС аналогичным способом (TA 12). Завершение аутентификации происходит при условии совпадения RES1 и XRES1. В противном случае абонент получает отказ в обслуживании.



Процедура аутентификации мобильных абонентов с использованием сеансовых ключей

Так же, как и ранее, процесс аутентификации сети абонентом происходит аналогично. Отличие лишь в том, что вместо алгоритмов TA 11 и TA 12 используются сертифицированные алгоритмы TA 21 и TA 22.

Отличительной чертой стандарта TETRA является высокая защищенность связи. Это достигается благодаря широким возможностям по разграничению доступа к передаваемой информации. Сквозное шифрование, которое может быть активизировано после успешного завершения аутентификации, включает четыре алгоритма (TEA1 – TEA4). Они различаются степенью защиты речи и данных. Необходимость такого разделения алгоритмов вытекает из существования нескольких групп абонентов, у каждой из которых индивидуальные требования к безопасности связи. К тому же использование лучшей защищенности может существенно отразиться на скорости передачи данных.

В случае шифрования речи потери скорости несущественны. Речь представляет собой низкоскоростной поток данных, поэтому возможно применение сложных алгоритмов с повышенной криптостойкостью, не ухудшающих качество восстановленного сигнала. Такие преобразования обеспечивают почти полную защиту радиопереговоров от прослушивания.

Аналогичная схема применяется для шифрования данных. Отличие лишь в том, что степень безопасности выбирается пользователем – ему самому приходится искать компромисс между скоростью передачи данных и криптостойкостью. (см. Табл.)

Зависимость скорости передачи данных (Кбит/с) от степени защищенности канала

Уровень защиты	Число используемых тайм-слотов			
	1	2	3	4
Без защиты	7,2	14,4	21,6	28,8
Низкий	4,8	9,6	14,4	19,2
Высокий	2,4	4,8	7,2	9,6

При работе с низким уровнем защиты в TETRA применяется поточное шифрование, при котором генерируется псевдослучайная последовательность (зависящая от ключа DCK) и складывается побитно с потоком данных. Зная DCK и IV (Initial Vector), принимающая сторона может сгенерировать такую же псевдослучайную последовательность, прибавить к принятому сообщению и восстановить исходный «текст». Преимуществом такого подхода является отсутствие накопления ошибок в канале с помехами. Т.е. ошибка приема одного бита зашифрованного сообщения дает только один ошибочный бит расшифрованного текста и не приводит к нескольким ошибкам.

Для защиты радиоинтерфейса используются следующие виды ключей:

- *Выделенные ключи (DCK - Derived Cipher Key)* служат для организации point-to-point соединений. Их применение возможно только после успешной аутентификации.
- *Статические ключи (SCK – Static Cipher Key)* - несколько заданных величин (до 32), которые загружаются в мобильную станцию, причем эти величины известны сети. SCK применяются для ограниченной защиты сигналов сигнализации в системах, которые функционируют без явной аутентификации.
- *Групповые ключи (CCK – Common Cipher Key)* используются для шифрования информации при групповом вызове.

Станции стандарта TETRA однозначно определяют своих абонентов с помощью уникальных ID. Эти номера могут меняться со временем, чтобы обеспечить защиту от несанкционированной идентификации (например, вследствие перехвата передаваемых сообщений). Механизм использования временных ID прост: после первого сеанса связи с абонентом, его ID меняется на «псевдоним» - временный ID. Такие замены могут происходить неоднократно, кроме того, все ID (как уникальные, так и временные) защищаются с помощью шифрования радиоинтерфейса.

Скрытность абонента сохраняется и при переходе из одной зоны обслуживания (зоны охвата конкретной БС) в другую, т.к. мобильная станция и БС постоянно обмениваются специальными сообщениями, содержащими в себе временный ID абонента. Разумеется, данные сообщения передаются зашифрованными.

Рассмотренные выше меры безопасности и особенности применения систем стандарта TETRA позволяют говорить о возможности широкого применения TETRA в сферах, которые невозможно представить без профессиональной радиосвязи.

ЛИТЕРАТУРА

1. Л.М. Невдяев. Мобильная связь 3-го поколения. Под ред. Ю.М. Горностаева, М.: МЦНТИ, 2000, 208 с., илл.
2. В.П. Николаев. Новые технологии GSM для сотрудников служб безопасности//“Специальная техника” № 4, 2000, 16 – 20 с.
3. А.Н. Дремов. Решительный шаг к интеграции. TETRA на пути к поколению 3G//“Технологии и средства связи”, № 2, 2001, 46 – 52 с.
4. ГОСТ Р50922-96. Защита информации. Основные термины и определения
5. А.М. Овчинников, С.В. Воробьев, С.И. Сергеев. Открытые стандарты цифровой транкинговой радиосвязи. М.: МЦНТИ, 2000, 166 с., илл.
6. А. Фильчаков. TETRA – профессиональное радио и не только//“КомпьютерПресс”, № 5, 2000
7. Овчинников А.М. TETRA – стандарт, открытый для всех//“Специальная техника” № 4, 1999 http://st.ess.ru/publications/articles/ovchinkv/ovchkv.htm
8. Вахлаков В.Р., Соколов В.В. Обеспечение безопасности связи в транкинговых системах стандарта TETRA//“Специальная техника” № 6, 2001 http://st.ess.ru/publications/6_2001/vahlakov/vahlakov.htm
9. Сайт Московской группы пакетной радиосвязи http://ra3apw.by.ru/tetra/