Эссе по курсу “Защита информации”

на тему “Security in GPRS”

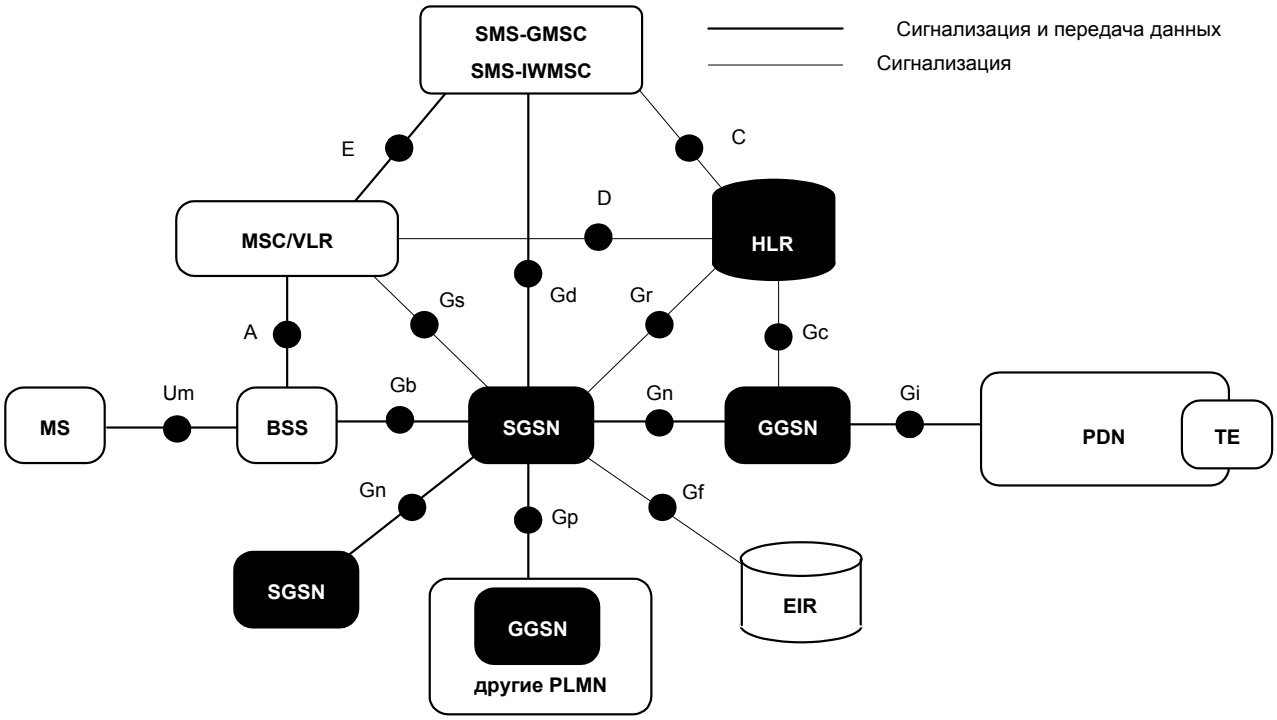
студента 911 группы Котова Ю.А.

Введение.
Можно выделить следующие фрагменты GPRS-сети, на безопасность которых необходимо обратить соответствующее внимание:

- безопасность мобильной станции
- безопасность соединения между мобильной станцией и узлом обслуживания SGSN
- безопасность данных в процессе их передачи по сети GPRS
- безопасность данных в процессе их передачи между различными операторами GPRS услуг
- безопасность данных в процессе их передачи в сети открытого доступа, например, Internet.

Об этом и пойдет речь.

Эталонная модель GPRS представлена ниже на рисунке.



Безопасность мобильной станции
Безопасность мобильного телефона (мобильной станции – MS) складывается из двух составляющих – SIM(Subscriber Identity Module) карта и сам телефон.

SIM карта – это модуль идентификации абонента, в ней хранится информация о сервисах предоставляемых абоненту независимо от типа используемого оборудования. Она содержит

- идентификатор IMSI(International Mobile Subscriber Identity). Он состоит из 3 элементов:
  - трехразрядный код страны (Россия – 250)
  - двухразядный код сети (МТС – 01, для Билайн – 99, для СМАРТС – 07
  - десятиразрядный код абонента MSIN (Mobile Subscriber Identity Number)
- собственный индивидуальный ключ аутентификации Ki(копия его храниться в AuC (Authentication Center) связанный с регистром нахождения (Home Location Register) мобильной станции)
- алгоритм генерации ключей шифрования A8
- алгоритм аутентификации A3

- PIN код

Алгоритм A5 наряду с IMEI(International Mobile Equipment Identity) включен в состав программного обеспечения телефона и обеспечивает его защиту.

Безопасность самого телефона , обеспечивается механизмами

- Алгоритм шифрования A5
- Уникальным 14 разрядным международным идентификатором аппаратуры мобильной связи (IMEI), который однозначно идентифицирует телефон. Узнать его можно набрав на телефоне комбинацию *#06#. Если высвеченное число не совпадает с тем, что указано на задней крышке телефона, то телефон взломан. Именно такие номера хранятся в реестре EIR. Данный реестр имеет три списка IMEI
    - «белый» список , содержит идентификаторы всех разрешенных аппаратов
    - «серый» , содержит идентификаторы всех не запрещенных аппаратов, но используемых для различных целей, например, тестирования.
    - «черный», содержит идентификаторы всех запрещенных аппаратов.

Итак, IMEI , IMSI – независимы между собой. IMEI – идентифицирует мобильный терминал, а IMSI – абонента.

Безопасность соединения мобильной станции с узлом SGSN.

В процессе подключения мобильной станции, между ней и узлом SGSN происходит выбор версии используемого в дальнейшем алгоритма шифрования GPRS-A5. В сетях GPRS используются алгоритмы семейства A5 – GEA 1 и GEA2 , GEA3 (после разработки A5/3).

Безопасность данных в процессе их передачи по сети GPRS.

Все данные между узлами поддержки (SGSN, GGSN) передаются с помощью специального протокола GTP (GPRS Tunelling Protocol) , который инкапсулирует в себя любые пользовательские протоколы, например, HTTP, Telnet, FTP, и др. По умолчанию GTP-трафик не шифруется.

Безопасность в процессе взаимодействия с различными операторами GPRS услуг

Безопасность осуществляется с помощью устрйств, называемых граничными шлюзами(Border Gateway – BG) .

BG может быть использован в качестве security gateway (SG). SG это система, которая функционирует как коммутационный шлюз между внешними недоверительными системами и доверительными хостами в своей собственной подсети. Он также предоставляет безопасные сервисы для доверенных хостов, когда они общаются с внешними недоверенными системами. В случаях если такой шлюз предоставляет сервисы по поручению одного или нескольких хостов в доверенной подсети, шлюз несет ответственность за установление именно безопасного соединения. В этом случае только такой шлюз использует Authentication Header (AH) и/или ESP сервисы между шлюзами и внешними системами. Шлюз безопасности который получает датаграмму содержащую распознающую метку, от доверенного хоста, должны считать , что значение меток в рассмотрении , при создании/выборе безопасности для использования с AH между шлюзами и внешним пунктом назначения. В таких окружениях , шлюз , который получает IP пакет , содержащий IP ESP должен добавить соответсвующую аутентификацию, включая соответсвие(которое содержится в Security Association) или внешние метки , такие как IPSO(IP Security options), для расшифрованных пакетов которые они передают их доверенному хосту, которое является пунктом конечного назначения. В средах, использующих такие шлюзы они должны предоставлять основанные на IP пакетную фильтрацию неавторизованных пакетов. Этот шлюх защищает оператора от атак, связанной с подменой адреса.

Настройка такого шлюза включает в себя создание правил, разрешающих входящий/исходящий пользовательский трафик, данные биллинговой системы, аутентификацию роуминговых абонентов и т.п.

Кроме этого, межсетевой экран Firewall, если он установлен на пограничном узли или узле GGSN повышает защищенность сети оператора от возможных несанкционированных действий.

Безопасность в процессе взаимодействия с Internet.
Основные механизмы безопасности реализованы на узле GGSN , в состав которого входит межсетевой экран, который определяет тип входящего GPRS- трафика. Его задача также защитить мобильную станцию от атак внешних хакеров. Для этого используется трансляция адресов (network address translation). Все остальные механизмы защиты , это например, аутентификация при помощи серверов RADIUS , защита трафика с помощью IPSec и др.

Связь через сеть передачи общего пользования(PDN) , где соединение состоит в связи через третью информационную сеть. Это соединение имеет отлично от предыдущих, потому что оно больше не использует интерфейс Gp. Gi интерфейс определяет соединение между GPRS backbone и PDN(рисунок в начале). Соединение двух GPRS backbon\ов (the GPRS Backbone это сеть реализованная путем соединения GSN, управляемых одним оператором) через PDN – можно представить в виде соединения двух различных GPRS backbon\ов к единственной PDN. Этот случай рассматривается ниже.

Процесс подключения мобильной станции.
Упрощенно процесс подключения абонента, желающего воспользоваться услугами GPRS выглядит так:

1) MS посылает запрос на получение доступа к сети, который содержит ряд параметров(IMSI и др).
2) Узел SGSN получив такой запрос, проверяет наличие аутентифицирующей данного абонента информациив своей базе. Если такая информация то SGSN посылает запрос в реестр HLR , который возвращает аутентификационный триплет.
3) Полученное случайное число передается на мобильную станцию, которая на его основе вырабатывает ключ шифрования и ключ аутентификации. Так как индивидуальные ключи , хранящиеся в реестре HLR и на мобильной станции совпадают , то и ключи штфрования и аутентификации также должны совпадать.
4) После идентификации абонента осуществляется идентификация оборудования, которое посылает на SGSN идентификатор IMEI. Узел SGSN в свою очередь проводит проверкуд данного оборудования по реестру EIR.
5) После аутентификации абонента и оборудования происходит процедура определения местоположения абонента. (используются реестры HLR и VLR), после этого происходит завершение процедуры подключения MS к GPRS. Если MS не смогла пройти аутентификацию , то SGSN посылает на нее сообщение Attach Reject.

Ключи и триплеты.
Когда соединение устанавливается с мобильной станцией (MS), Serving GPRS Support Node (SGSN) информирует и берет во владение Аутентификационную процедуру. SGSN запрашивает IMSI и использует его для определения регистра нахождения станции. SGSN передает IMSI и свой собственный регистр HLR (Home Location Register), это информирует сеть о текущем положении MS, когда соединение осуществляется с ним. Если HLR получает ее, подписчик IMSI обращается к аутентификационному Центру и запрашивает ключ шифрования Ki. Этот ключ используется вместе со случайным числом в качестве параметра в алгоритме A3 для распознавания подписи или подписания ответа.

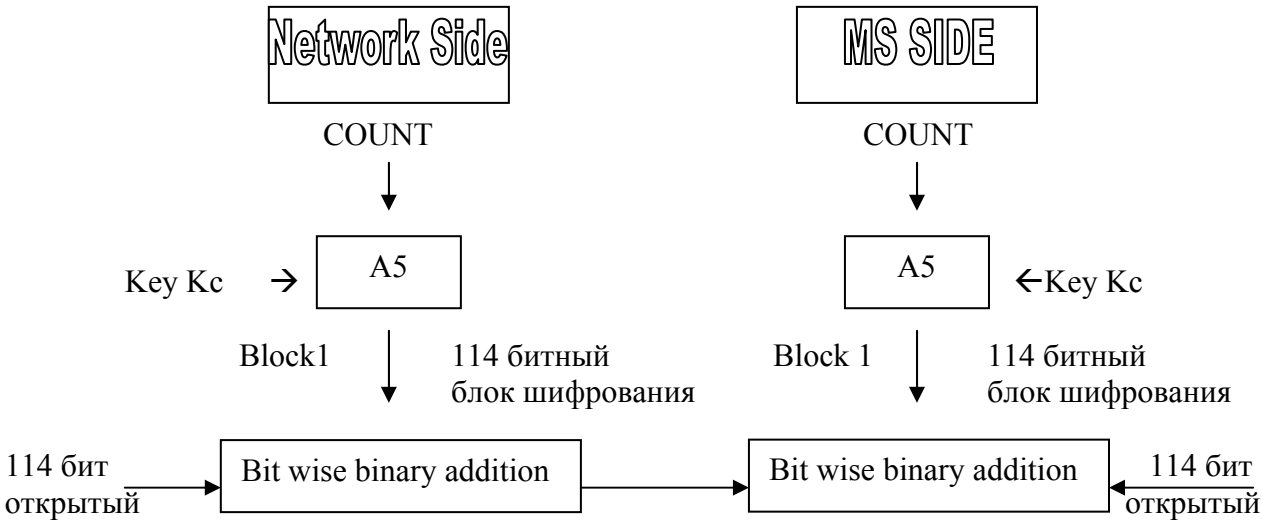
AuC похожим образом использует Ki и случайное число в качестве параметра в алгоритме A8 для вычисления ключа шифрования Kc для кодирования канала, по которому передается траффик. Случайное число, подписанный ответ и Kc составляют тройню(триплет) для мобильной станции, которые используются для дальнейшего шифрования. Так как каждый триплет используется только один раз и аутентификационный центр считает несколько триплетов и посылает их в HLR и в SGSN , где находиться мобильная станция. Когда SGSN доиспользует все свои триплеты он запрашивает у HLR новый набор.

Характеристики различных алгоритмов.

Три алгоритма определено:

- Алгоритм A3 – Аутентификационный алгоритм. Его цель – предоставить аутентификацию мобильного подписчика. A3 вычисляет ожидаемый ответ SRES от случайного вызова RAND посланного сетью. Для этих вычислений, A3 использует аутентификационный ключ Ki. На стороне абонента A3 содержит содержится в Sim карте. В сети он поддерживается в аутентификационном центре, который является подразделением HLR. Два входных параметра имеют следующий формат.
  - Длина ключа - 128 бит
  - Длина RAND - 128 бит
- Алгоритм A5 – алгоритм шифрования / дешифрования. Этот алгоритм используется как в мобильной станции там и SGSN. Шифрование происходит перед модуляцией и после интерливинга. Во время TDMA используемых в системе, полезная информация разделяется на блоки по 114 бит. Затем каждый блок вставляется в нормальный пакет (burst) и передается. Для шифрования алгоритм A5 каждые 4.615 мс (время прохождения фрейма) производится последовательность из 114 битов шифрования/дешифрования, называемых блоками(BLOCK). Дешифрование : A5 производит последовательность из 114 битов и первый бит добавляется к шифротексту (кодированному сообщению) и так далее. Для каждого слота, расшифровка просходит на стороне мобильной станции с первым блоком (BLOCK1) и шифрование при помощи второго блока (BLOCK2). Аналогично, на стороне сети BLOCK1 используется для шифрования, а второй BLOCK2 для дешифрования. Тем самым, A5 должен производить дважды 114 бит каждые 4.615 мс.

Шифрование начинается, когда приходит подтверждение соответсвия от MS, используя синхронизацию, которая была выбрана в BSC . Синхронизация тем самым гарантируется переменной открытого времени, COUNT, полученной из LLC. Таким образом, блок из 114 бит полученный A5 зависит только от LLC frame number, ключа шифрования Kc . Нижеследующий рисунок суммирует все вышесказанное .



текст Канал текст

Несколько алгоритмов шифрования будут созданы, но только один из них будет использоваться при аутентификации. Итак, 2 входных параметра (COUNT и Kc) и выходные параметры (BLOCK 1 & BLOCK 2) алгоритма A5 имеют следующий формат :

- длина Kc – 64 бит
- длина COUNT – 22 бита
- длина BLOCK1 – 114 бит
- длина BLOCK2 – 114 бит
- Алгоритм A8 – генератор ключа шифрования. На стороне MS, он содержится в SIM карте. В сети он располагается наряду с протоколом A3. Два входных параметра (RAND & Ki) и выходной параметр (Kc) A8 соответсвуют следующему формату
  - Длина Ki – 128 бит
  - Длина RAND – 128 бит
  - Длина Kc – 64 бита.

Так как индивидуальный ключ имеется не только у абонента, но и хранится в реестрах HLR и VLR, то и абонент и оборудование сети создают одинаковый ключ

Аутентификация.

HLR передает значение триплета в SGSN и значение случайного числа потом посылается мобильной станции. Вдобавок SGSN предоставляет выбор алгоритма шифрования (различные версии алгоритма A5 доступны) и синхронизацию для начала шифрования.

Мобильная станция после получения случайного числа, вычисляет другие числа для триплета (подписанный ответ и Kc), используя алгоритм A3 и A8. Подписанный ответ отсылается обратно в SGSN и сравнивается с тем который посылался HLR.

Любые дальнейшие процессы не предпринимаются перед подписанием ответа, вычисленным HLR и хранищимся в SGSN , сравненный с вычисленным в мобильнике.

Аутентификационная процедура.

1) Если SGSN не имеет первоначально хранящегося аутентификационного триплета, IMSI посылается в HLR. HLR дает Authentication Triplets, который включает RAND, SRES и Kc.
2) SGSN посылает аутентификационный запрос (RAND, Начало шифрования, алгоритм штфрования A5) . MS отвечает (SRES). Успешная аутентификация подписчика означает, что ответ совпадает с подписью в SGSN, присланной HLR.

Encoding

Если аутентификация подписчика успешная , то потом идет шифрование. Информация и сигнализация сливаются в канале между мобильными станцией и SGSN используя:

1) алгоритм шифрования A5 и синхронизацией специфицированной SGSN.
2) Ключ Kc в качестве параметра.

IP Security(коротко)

Безпасность не предоставляется в GTP(GPRS Tunnel protocol). GPRS Tunnel protocol просто способ туннелирования пакетов от источника к последней точке. Безопасность может быть предоставлена оператором между граничным шлюзом (Border Gateway) в различных GPRS сетях . Механизм отвечающий за безопасность – IP Security.

Ipv4 не предоставляет возможностей безопасностей, кроме как опционного метки безопасности. Ipv6 предоставляет ряд возможностей, в частности , Ipv6 включает свойства поддерживающие аутентификацию и защиту. Эти свойства также могут быть включены в Ipv4.

Имеются 2 заголовка, которые используются для предоставления безопасных сервисов в Ipv4 и Ipv6. Эти заголовки “IP Authentication Header (AH)” и “ IP Encapsulating Security

Payload (ESP)" заголовки. Есть несколько способов, в которых эти механизмы IP безопасности могут использоваться.

IP AH создан, чтобы предоставить интеграцию и аутентификацию без конфиденциальности к датаграмме. Недостаток конфиденциальности гарантирует что использование AH будет широко доступно , даже в расположениях где экспорт, импорт или использование шифрования для предоставления конфиденциальности используется. AH поддерживает безопасность между двумя или более хостами, между двумя или более шлюзами, хостами или шлюзами и набором костов или шлюзов. IP ESP разработан для предоставления интеграции, аутентификации, и конфиденциальности IP датаграммам. ESP поддерживает безопасность между двумя или более хостами , между хостом или шлюзом и набором хостов и/или шлюзов.

Authentication header.
Это механизм для предоставления надежной интеграции и аутентификации для IP датаграмм. Он также может зависеть от того какой криптографический алгоритм испрользуется и как происходит работа с ключами. Например, алгоритм RSA. Конфиденциальность и защита от анализа трафика не обеспечивается AH. Пользователи которые хотят обеспечить себе это, должны использовать ESP.

AH может появиться после любого другого заголовка, который проверяется на каждом скачке и перед любым другим заголовком, который не исследуется в промежуточном хопе. Ipv4 и Ipv6 заголовки непосредственно предшествующие AH будут содержать значение 51 в своем следующем поле заголовка. Пример Ipv6

Ipv6 Header	Hop-by Hop/Routing	Authentication header	Upper Protocol

Пример Ipv4

Ipv4 Header	Authentication Header	Upper Protocol (TCP, UDP)

IP AH имеет следующий формат

0 8 16 31

Next Header	Payload length	Reserved
Security parameters index		
Authentication data(32-х битное слова)		

Аутентификационная информация поддерживаемая IP AH обычно вычисляется используя алгоритм профиля сообщения(например, MD5). Только алгоритмы, которые считаются криптографически сложными используются для IP AH. При получении пакета содержащий IP AH, получатель сначала использует Destination Address и SPI значение для определения правильного безопасного соединения. Получатель сравнивает на соответствие информационное поле и полученный информацонный пакет, и он принипается если совпадает.

Encapsulating SecurityPayload.
ESP – это механизм для предоставления интеграции и конфиденциальности для IP датаграмм. Ниже приведен зашифрованная Ipv4 датаграмма или Ipv6 пакет.

< ---------- Unencrypted ---------- > | < ---------- Encrypted ---------- >

IP Header	Other IP headers	ESP	Header	Transport-level segment

< ---------- Single partially-encrypted IP packet ---------- >

a) Transport mode

IP header	Other IP headers	ESP	Header	IP header plus transport-level segment

|< ---Completely-encrypted inner packet ---------- >|

| < ---------- Partially encrypted outer IP packet ---------- > |

б) Tunnel mode

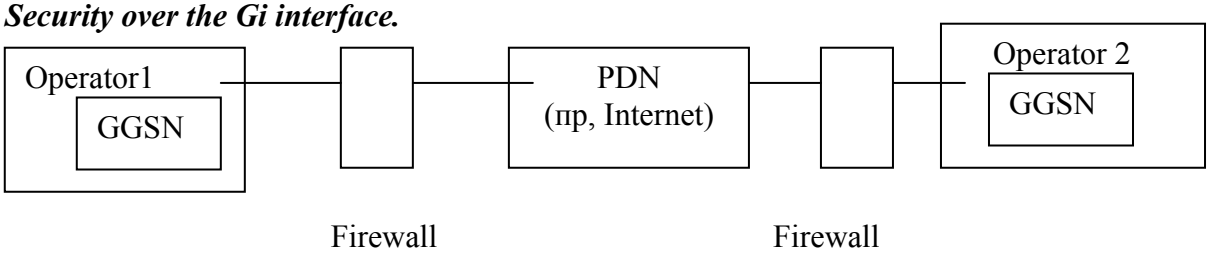
Есть два режима использования ESP.

- Туннельный режим – инкапсулирует всю IP датаграмму в ESP.
- Транспортный режим – инкапсулирует фрейм транспортного уровня (UDP, TCP) в ESP. Только в этом режиме аутентификация применятеся ко всему пакету, но только сегмент транспортного уровня защищен механизмом шифрования.

The GPRS Backbone

The GPRS Backbone это сеть реализованная путем соединения GSN, управляемых одним оператором. Путь, по которому информация посылается через эту шину был определен GPRS Tunnel Protocol (GTP). Информацией обмениваются между несколькими SGSN или между SGSN и GGSN, но в обоих случаях эти GSN принадлежат одной шине(backbone). Этот случай должен быть рассмотрен отдельно от соединения различных backbon\ов , в то время как GPRS backbone может иногда рассматриваться как доверительная подсеть.Но соединение нескольких GPRS backbone так не может рассматриваться. Способ, которым мы можем гарантировать безопасность только что рассматривался. AH & ESP основные способы предоставления безопасности. Но наиболее частая ситуация – это соединение нескольких единичных GPRS backbon\ов. Известны различные способы, которые я и рассмотрю ниже.

Security over the Gi interface.



Как показано на рисунке соединение с PDN проходит через шлюз GGSN и не через BG, как это имело место для Gp. GGSN конвертирует GTP, в один из тех которые используется в PDN. BG не имеет такой функциональности , он просто передает пакеты, которые получает. Тем не менее мы можем использовать GGSN в качества безопасного шлюза. Также мы должны использовать Firewall для обеспечения безопасности. GPRS оператор должен также решить использовать другие протоколы основанные на двустороннем соглашении. Функция отражения (Screening) имеющаяся в GPRS сети и имеет три уровня. Screening – находиться за пределами стандарта GPRS , лишь скажу что поддерживаются следующие типы

- Network controlled
- Subscription controlled

Последние веяния.

Дело в том что при разработке спецификации GPRS вопросам безопасности уделялось мало внимания. Сейчас в связи с развитием GPRS возникла необходимость разрабоки новых алгоритмов безопасности. Так в 3 квартале 2002 года началась разрабока разработка новой версии алгоритма A5. Он называется A5/3 и может использоваться не только в GSM, но и в GPRS, HSCSD, EDGE сетях. Он разработан на базе алгоритма Казуми(Kasumi), который в свою очередь был разработан на базе алгоритма MISTY компании Мицубиси. На данный момент в сетях GPRS используются алгоритмы семества A5 – GEA1 и GEA2.

Некоторые элементы сети. (см. Рисунок)

Базовая станция (BSS) – принимает радиосигнал от мобильной станции и в зависимости от того что передается (голос или данные) транслирует траффик.

Узел поддержки обслуживания GPRS (SGSN – Serving GPRS support node). По своей сути он очень похож на аналогичный центр коммутации MSC в GSM и выполняет аналогичные задачи. Он отвечает за коммутацию трафика к BSS и сетевым элементам, которые устанавливают взаимосвязь с внешними PDNs. SGSN таким образом выполняте также задачи обычного маршрутизатора. С точки зрения безопасности на него возложены такие функции : аутентификация абонентов (аналогично GSM) , мониторинг активных абонентов, регистрация новых абонентов, шифроавние данных (Алгоритмы шифрования в GPRS (GEA1, GEA2, GEA3) .

Узел поддержки GPRS шлюза(GGSN – Gateway GPRS support node). Это узел маршрутизации. SGSNs и GGSN соединятются через опорную сеть IP. GGSN также участвует в процессе управления мобильностью.

Home Location Register (HLR) - это реестр собственных абонентов сети, которая хранит информацию о каждом человеке, оплатившем услуги оператора GPRS именно данной сети. В частности, HLR хранит информацию о дополнительных услугах, параметрах аутентификации, IP-адресе и т.д. Обмен данной информацией происходит между HLR и SGSN. Это по сути расширение HLR в GSM , в котором хранятся также абонентские данные, связанные с коммутацией пакетов.

Visitor Location Register (VLR) - это реестр перемещений, которая хранит информацию о каждой мобильной станции, находящейся в данный момент в зоне действия SGSN. В VLR хранится та же информация об абоненте, что и в HLR, но только до тех пор, пока абонент не покинет географическую зону, обслуживаемую этим реестром перемещений.

Equipment Identity Register (EIR) - это реестр идентификационных данных оборудования, который содержит информацию, позволяющую блокировать вызовы от украденных, мошеннических или иных неавторизованных устройств.

Узел поддержки обслуживания GPRS (SGSN – Serving GPRS support node). По своей сути он очень похож на аналогичный центр коммутации MSC в GSM и выполняет аналогичные задачи. Он отвечает за коммутацию трафика к BSS и сетевым элементам, которые устанавливают взаимосвязь с внешними PDNs. SGSN таким образом выполняте также задачи обычного маршрутизатора. С точки зрения безопасности на него возложены такие функции : аутентификация абонентов (аналогично GSM) , мониторинг активных абонентов, регистрация новых абонентов, шифроавние данных (Алгоритмы шифрования в GPRS (GEA1, GEA2, GEA3) .

Использованная литература.

1) Security over GPRS - http://www.ee.ucl.ac.uk/~lsacks/tcomsmsc/ projects/pastproj/s_piot.pdf

2) An evolved UMTS Network Domain Security architecture
http://www.telenor.no/fou/publisering/notater/N_28_2002.pdf

3) Тестирование протокола беспроводной GPRS в мире беспроводной связи.(статья, без автора)