3. Функционирование сети LTE

3.1. Протоколы и процедуры

При изучении процедур, выполняемых в сети при обслуживании абонентских терминалов, целесообразно связать их с определёнными протокольными уровнями стеков протоколов сигнализации. Сигнальные протоколы взаимодействия UE с сетью LTE распределены в трех протокольных уровнях:

RRC (Radio resource Control) – управление радиоресурсом,

MM (Mobility Management) – управление мобильностью,

SM (Session management) – управление сеансом связи (рис. 3.1).

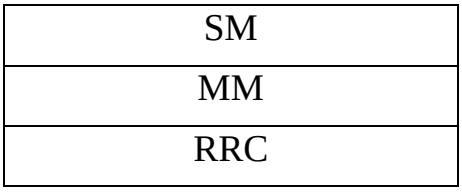

Рис.3.1. Стек сигнальных протоколов

UE и eNB обмениваются между собой сигнальными сообщениями уровня RRC. Эти команды специфицированы в [23]. Типичные примеры процедур протокола RRC – установление активного соединения между UE и eNB *RRC Connection Establishment* (см. 8.3), внутрисетевые хэндоверы.

Сигнальные сообщения более высоких уровней MM и SM имеют конечными точками UE и MME. Во многих случаях эти команды eNB пропускает прозрачно, не изменяя их содержания. Протоколами такие команды относят к сообщениям NAS (Non Access Stratum). На уровне RRC команды NAS передают в виде сигнальных сообщений *DLInformation Transfer* и *ULInformation Transfer* [23]

Протокол уровня MM обеспечивает глобальную мобильность абонентов, то-есть возможность получить обслуживание в любой точке земного шара, где развернута сеть GSM/UMTS/LTE. Этот протокол обеспечивает регистрацию абонента в MME, отслеживает его перемещения и поддерживает все процедуры безопасности. Протоколы уровня SM используют при организации услуг: создании сквозных каналов между PDN GW и UE с необходимыми качественными показателями. Команды уровня SM также относятся к классу команд NAS.

В процессе активизации мобильного терминала и при организации услуг в сети E-UTRA создают сквозные каналы (bearer). Каждый сквозной канал можно представить в виде непрерывной трубки, связывающей UE с

внешними устройствами (серверами) сети Интернет (рис. 3.2). Сквозной канал состоит из отдельных частей: EPS (Evolved Packet System) сквозного канала и его внешней части. Оператор полностью отвечает за организацию EPS сквозного канала. Параметры сквозного канала устанавливает PDN GW совместно с PCRF. Сквозной канал на радиоинтерфейсе (Radio Bearer) организует eNB, на интерфейсах S1 и S5/S8 в создании сквозного канала участвуют MME и шлюзы.

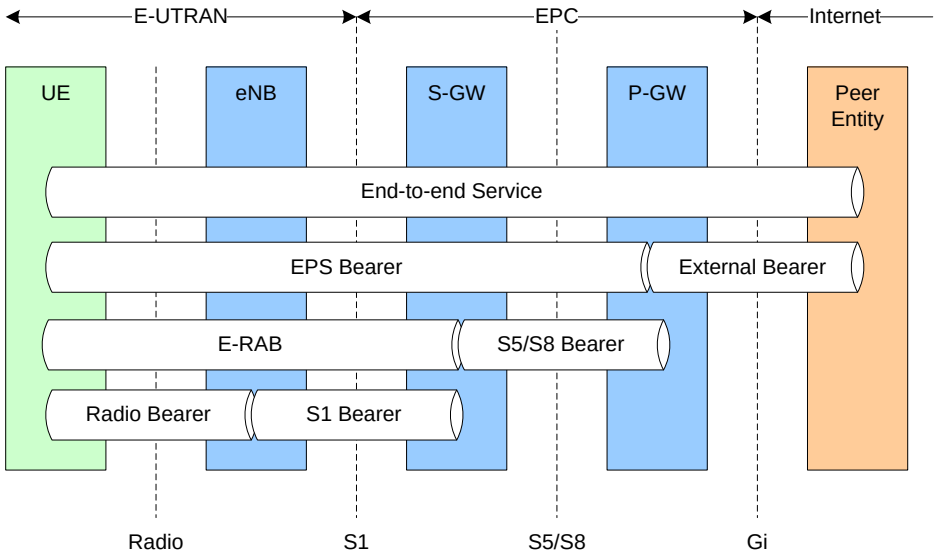

Рис. 3.2. Архитектура сквозного канала

Функционирование сетей LTE поддерживается необходимым программным обеспечением (рис. 3.3).

В подсистеме радиодоступа (E-UTRAN) eNB обеспечивает следующие функции.

Inter Cell RRM – взаимодействие между соседними узлами базовых станций с целью минимизации уровня взаимных помех (ICIC).

Radio Bearer (RB) Control – управление сквозным каналом на радиоинтерфейсе; состоит в выделении, поддержке и освобождении канального ресурса при организации сеансов связи.

Connection Mobility Control – управление мобильностью соединения; заключается в управлении радиоресурсом в отношении UE, находящихся как в состоянии CONNECTED, так и в состоянии IDLE. Речь идет об установке параметров процедур физического уровня: селекции и реселекции сот, запуске хэндоверов. Это относится также к выбору целевых eNB при хэндоверах.

Radio Admission Control – управление доступом к сети, регулирует возможность подключения UE к конкретному eNB и возможность запроса новой услуги. Эта процедура неспецифицирована и соответствующее ПО устанавливает производитель аппаратуры.

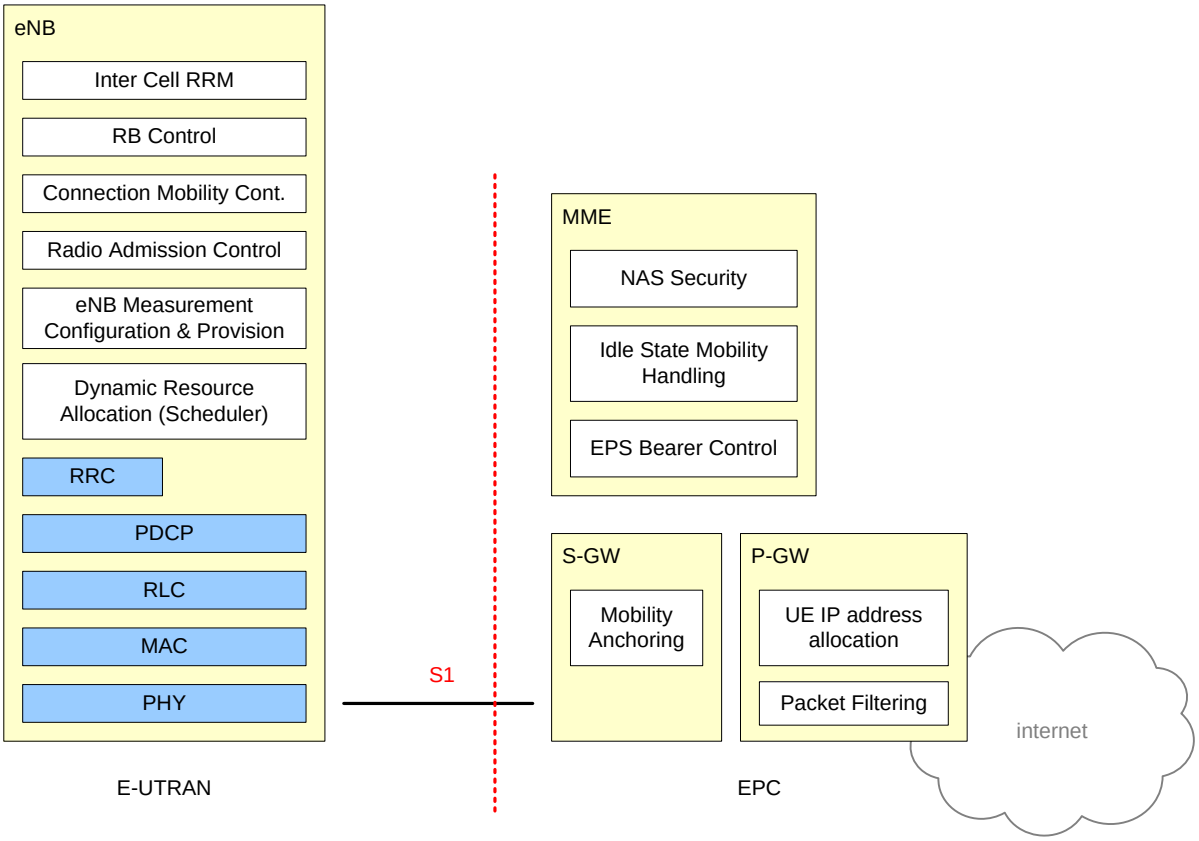

Рис. 3.3. Функциональная структура сети LTE

eNB Measurement Configuration & Provision формализует выполняемые UE измерения и представляемые ими отчеты с целью обеспечения обслуживания UE при их перемещении по сети.

Scheduler – планировщик, обеспечивает динамическое выделение канальных ресурсов для передачи пользовательского и сигнального трафика.

В ядре сети (EPC) MME поддерживает:

NAS Security – сигнализацию, необходимую для обеспечения процедур безопасности,

Idle State Mobility Handling – процедуры локализации UE, находящихся в состоянии IDLE,

EPS Bearer Control – процедуры, связанные с организацией сквозных каналов.

S-GW обеспечивает якорные функции при перемещении абонентов по сети (Mobility Anchoring).

PDN-GW назначает (активизирует) IP-адреса абонентов (UE IP Address Allocation) и распределяет информационные пакеты по сквозным каналам с соответствующими QoS (Packet Filtering).

3.2. LTE радио протокол

LTE радио протокол включает в себя 3 уровня (рис.3.4).

В плоскости управления на уровне L3 находится RRC (Radio Resource Control) протокол. Уровень L2 расщеплен на 3 подуровня:

- PDCP – Packet Data Convergence Protocol, протокол конвергенции пакетов данных;

- RLC – Radio Link Control Protocol, протокол управления радио соединением;

- MAC – Medium Access Control Protocol, протокол управления доступом к среде.

Протокол RRC представляет собой систему алгоритмов и команд, используемых для обслуживания UE на радиоинтерфейсе.

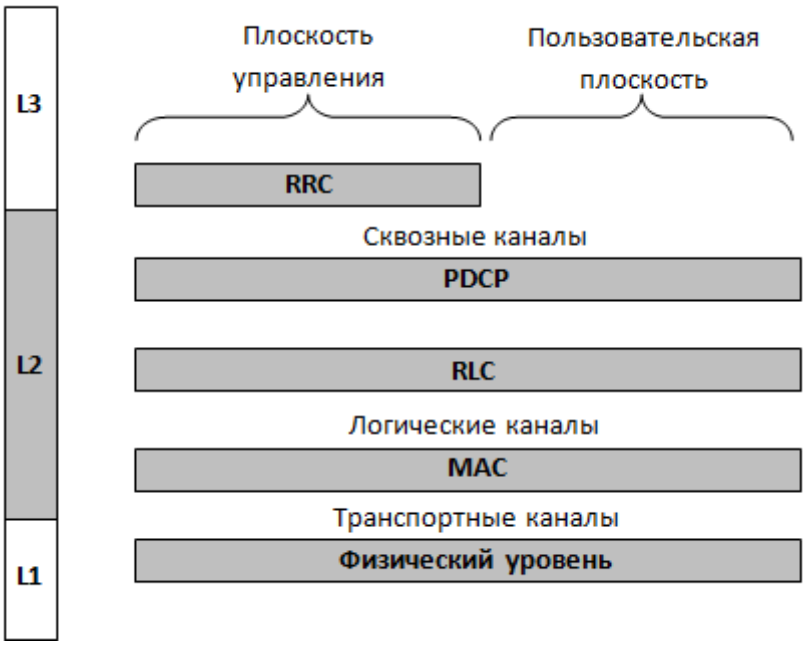

Рис.3.4. Структура радио протоколов LTE

Протокольные соединения в плоскости управления (Control Plane) в сети LTE показаны на рис.3.5. На нем, кроме радио протокола показаны сигнальные соединения по интерфейсу S1 (NAS – Non Access Stratum), организуемые поверх радио протокола, а также соединения по интерфейсу X2.

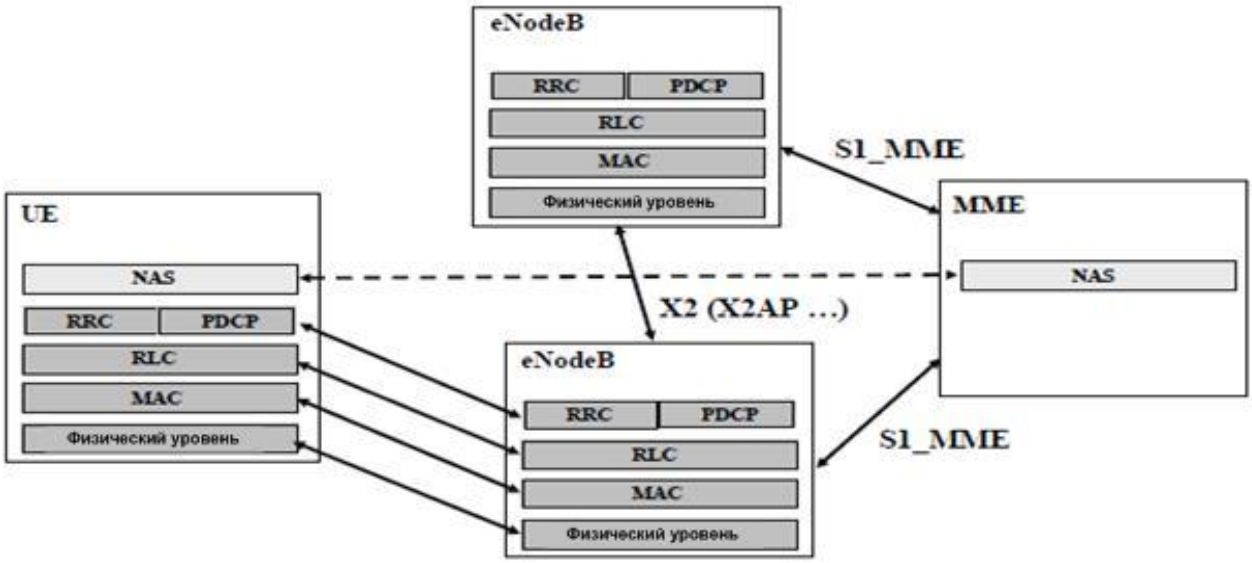

Рис.3.5. Протоколы сигнальной плоскости в архитектуре LTE

Взаимодействие протоколов при передаче пакетов трафика в пользовательской плоскости (User Plane) показано на рис. 3.6 [16]. Буферы дейтаграмм и блоков, передаваемых по радиоинтерфейсу, размещены в обслуживающем абонента eNB. Физический уровень обеспечивает 2 варианта повторной передачи (CC – Chase Combining или IR – Incremental Redundancy) непосредственно на радиоинтерфейсе. При неприеме блоков работает механизм их повторной передачи на уровне RLC. Наконец, повторную передачу дейтаграмм (файлов) обеспечивает уровень TCP.

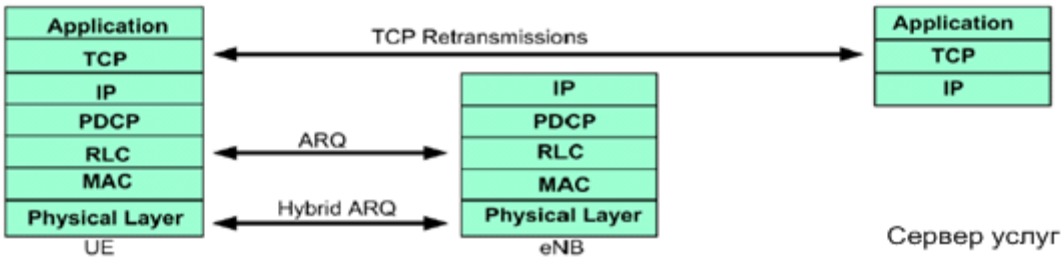

Рис.3.6. Протоколы доставки пакетов трафика в LTE

Рассмотрим функции, выполняемые различными подуровнями L2 радиоинтерфейса. На ***протокольном уровне PDCP*** обрабатывают данные более высоких уровней: SDU (Service Data Units) – дейтаграммы трафика и сигнальные сообщения. При этом осуществляют:

- сжатие (и, соответственно, восстановление) IP-заголовков, используя протокол ROHC (Robust Header Compression), разработанный IETF и применяемый с сетях UMTS,

- шифрацию и дешифрацию SDU трафика и сигнализации (в UMTS это делают на уровнях RLC или MAC),

- защиту (проверку) целостности сигнальных сообщений (в UMTS это осуществляют на уровне RLC).

Последовательность производимых операций показана на рис. 3.7.

Кроме указанных функций, уровень PDCP обеспечивает передачу данных без потерь при хэндоверах и обрывах связи.

На ***уровне RLC*** осуществляют:

- сегментацию SDU на PDU (Protocol Data Unit) для передачи и объединение пакетов при приеме в требуемой последовательности,

- коррекцию ошибок при передаче, используя повторную передачу (ARQ),

- устранение ошибок в передаче пакетов, вызванных ошибками сигнализации.

Возможны 3 режима обработки пакетов на уровне RLC в зависимости от характера передаваемой информации:

- прозрачный (transparent mode) – пакеты не обрабатывают на уровне RLC,

- передача без подтверждения (unacknowledged mode),

- передача с подтверждением (acknowledged mode).

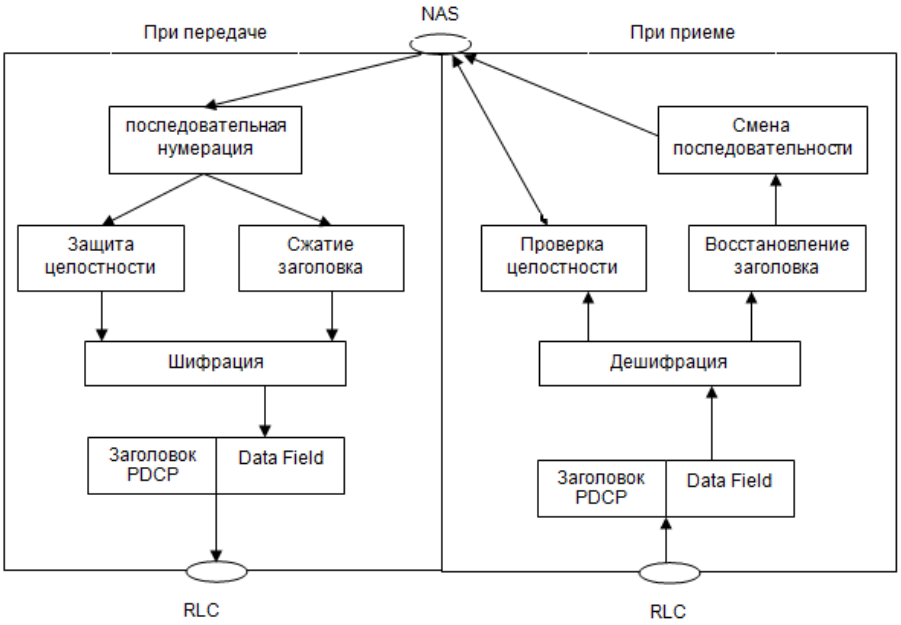

Рис.3.7. Операции, выполняемые на уровне PDCP

На ***уровне MAC*** происходит размещение и мультиплексирование пакетов логических каналов в транспортных каналах с последующей их передачей по физическим каналам. Уровень MAC осуществляет:

- управление выделением канального ресурса с учетом приоритетов разных UE и разных каналов трафика одного UE, т.е. выполняют задачи планирования передач,

- выбор транспортных форматов передач,

- управление повторными передачами непринятых пакетов через HARQ,

- организацию процедур доступа UE к сети и периодической синхронизации UE,

- измерения: объема передаваемого трафика, загрузки канала, состояния буферов передачи UE, относительной мощности передачи UE и ряд других,

- организацию режима сна/прерывистого приема (DRX) абонентских станций.

Протокольные уровни MAC и RLC тесно связаны между собой. В зависимости от характеристик канала связи и загрузки сети MAC выбирает оптимальный формат передачи (модуляцию, скорость избыточного кодирования, объем блока), на основе которого RLC устанавливает размер PDU. MAC уведомляет RLC о начале передачи по конкретному соединению и о числе PDU, которые RLC должен выставить в данный момент. При неприеме PDU MAC сообщает RLC о необходимости повторной передачи.

Работой уровня MAC непосредственно руководит планировщик, алгоритмы работы которого и ПО являются know-how производителя аппаратуры.

Сигнальный протокол RRC обеспечивает следующие функции и процедуры:

- передачу системной информации по радиоинтерфейсу,

- пейджинг,

- установление, поддержку и разрыв соединения по протоколу RRC между UE и e-UTRAN,

- выполнение задач безопасности, в том числе управление ключами шифрации и целостности [4],

- организацию части сквозного канала на радиоинтерфейсе,

- хэндоверы,

- селекцию сот при перемещении UE,

- передачу сигнализации NAS между UE и ядром сети,

- исправление системных ошибок между UE и ядром сети,

- поддержку самоконфигурации и самооптимизации сети.

3.3. Безопасность в сетях LTE

Безопасность в сетях E-UTRA (LTE) основана на тех же принципах, что и в сетях UTRA (UMTS):

- взаимная аутентификация абонента и сети,

- шифрация сообщений в радиоканале,

- защита целостности передаваемых сообщений,

- защита абонентов.

Защита абонента состоит в том, что его в процессе обслуживания закрывают временными номерами (идентификаторами) M-TMSI, S-RNTI и C-RNTI.

В дополнение к этому в сетях LTE приняты меры по безопасности внутрисетевых соединений (они представляют собой туннели). На интерфейсах S1 и X2 передаваемые пакеты можно шифровать, используя IPsec ESP. Подвергают шифрации и сообщения в сигнальных плоскостях этих интерфейсов.

При каждом подключении или активизации UE в сети сеть запускает процедуру аутентификации и соглашения о ключах AKA (Authentication and Key Agreement) [57], [58]. Цель процедуры состоит во взаимной аутентификации абонента и сети и выработки промежуточного ключа K_{ASME}[1].

Процедуру аутентификации запускает MME, посылая в HSS соответствующий запрос. В ответ HSS направляет в MME вектор аутентификации (рис.3.8):

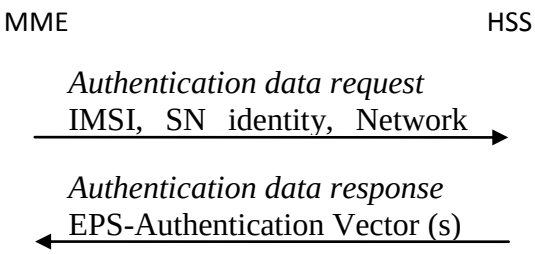

Рис.3.8. Начало процедуры AKA

На рис.3.8 SN (Serving Network) identity – идентификатор обслуживающей сети (24 бита), состоящий из MCC и MNC (кода страны и кода опе-

[1] ASME – Access Security Management Entity.

ратора). Тип сети (Network Type) – E-UTRA. Из HSS обслуживающая сеть (MME) получает вектор аутентификации EPS (Evolved Packet System). Вектор аутентификации в HSS генерируют в два этапа. На первом этапе используют алгоритм, принятый в UMTS (рис.3.9).

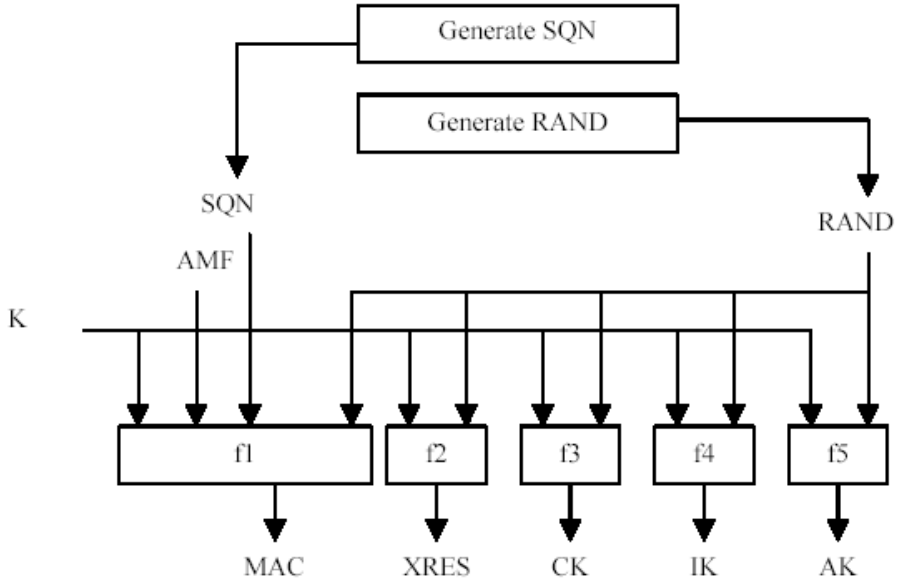

Рис.3.9. Исходный алгоритм генерации вектора аутентификации

Криптографический алгоритм (рис.3.9) реализован с помощью однонаправленных функций. Это значит, что прямой результат получают путем простых вычислений, но не существует эффективного алгоритма для получения обратного результата. В самом алгоритме использованы 5 однонаправленных функций: f1, f2, f3, f4 и f5. Исходными параметрами являются случайное число RAND <128бит>, Master Key K абонента <128бит> и порядковый номер процедуры Sequence Number SQN. Счетчик SQN меняет свое значение при каждой генерации вектора аутентификации. Аналогичный счетчик SQN работает в USIM. Это позволяет всякий раз получать новый вектор аутентификации и делает невозможным повторение уже использованного вектора.

Кроме трех исходных величин: SQN, RAND и K, в алгоритме f1 участвует поле управления аутентификацией Authentication Management Field AMF, в алгоритмах f2 – f5 исходные параметры – RAND и K. На выходах соответствующих функций получают Message Authentication Code (MAC) <64 бита>, XRES – eXpected Response, результат работы алгоритма аутентификации <32 – 128 бит>, ключ шифрации CK, ключ целостности IK и промежуточный ключ Anonymity Key AK <64 бита>.

Второй этап генерации вектора аутентификации зависит от типа сети обслуживания. Поле AMF содержит специальный бит (separation bit), определяющий тип сети: если он равен 0, то это сеть GERAN/UMTS. В этом случае вектор аутентификации состоит из чисел RAND, XRES, ключей CK, IK и числа AUTN представляющего собой запись в строку трех параметров: SQN ⊕ AK, AMF и MAC.

При обслуживании абонента сетью E-UTRA ключи CK и IK в открытом виде в ядро сети не передают. HSS генерирует K_{ASME} с помощью алгоритма KDF (Key Derivation Function), для которого исходными параметрами являются CK и IK, а также идентификатор обслуживающей сети и SQN⊕AK. Вектор аутентификации содержит RAND, XRES, AUTN и K_{ASME}, на основе которого происходит генерация ключей шифрации и целостности, используемых в соответствующих алгоритмах.

Мобильная станция получает из ядра сети три параметра: RAND, AUTN и KSI_{ASME} (рис.3.10). KSI – Key Set Identifier, индикатор установленного ключа, однозначно связанный с K_{ASME} в мобильной станции.

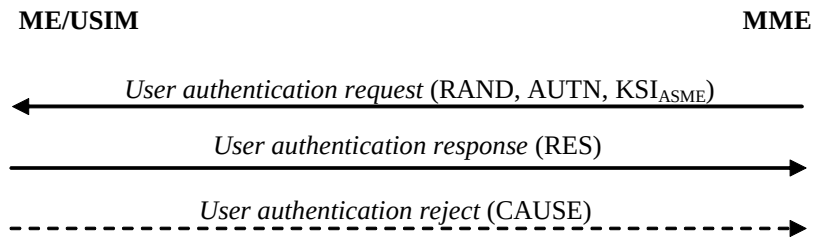

Рис.3.10. Завершение процедуры аутентификации

Используя RAND и AUTN, USIM на основе алгоритмов безопасности, тождественных хранящимся в HSS, производит вычисление MAC, XRES, CK и IK (рис.3.12).

В ответе *Res* (рис.3.10) UE передает в MME вычисленное RES, которое должно совпасть с XRES, полученным из HSS. Так сеть аутентифицирует абонента. Вычислив XMAC, UE сравнивает его с MAC, полученным ею в AUTN. При успешной аутентификации абонентом сети (MAC = XMAC) UE сообщает об этом в ответе *Res*. Если аутентификация сети не удалась (MAC ≠ XMAC), то UE направляет в MME ответ *CAUSE*, где указывает причину неудачи аутентификации.

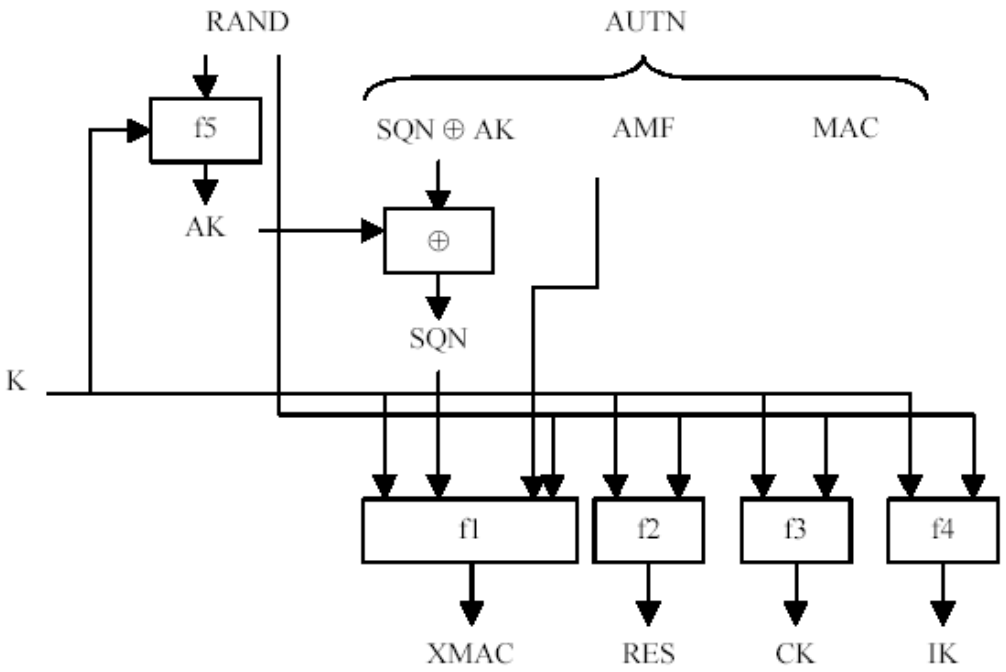

Рис.3.12. Процедура аутентификации в USIM

Далее MME, eNB и UE производят генерацию ключей, используемых для шифрации и проверки целостности получаемых сообщений. Иерархия ключей в E-UTRA приведена на рис.3.13.

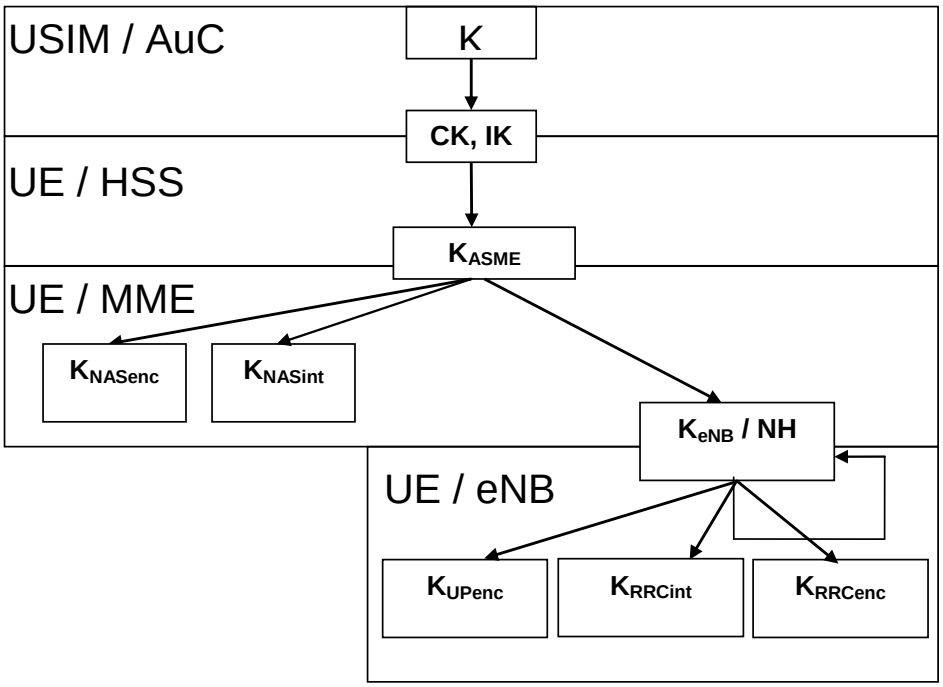

Рис.3.13. Иерархия ключей в E-UTRA

Исходным ключом для всей цепочки является K_{ASME} <256 бит>. Защиту при передаче в радиоканале обеспечивают для сигнального трафика (Control Plane) и для пользовательских пакетов (User Plane). При этом все сообщения сигнализации разделяют на сквозные сигнальные сообщения между UE и MME протоколов MM и SM (NAS – Non Access Stratum) и сигнальные сообщения между eNB протокола RRC (AS – Access Stratum). Для шифрации и защиты целостности согласно [58] можно использовать разные базовые алгоритмы:

- UEA2 (UMTS Encryption Algorithm 2) и UIA2 (UMTS Integrity Algorithm 2), разработанные для стандартов 3G,

- AES (Advanced Encryption Standard).

Для сигнальных сообщений NAS ключи шифрации K_{NASenc} и целостности K_{NASint} получают по схеме рис.3.14. Входными параметрами являются K_{ASME}, тип алгоритма (в данном случае *NAS-enc-alg* или *NAS-int-alg*) и идентификаторы базовых алгоритмов (UEA2, UIA2) или AES. На выходах генераторов ключей KDF (Key Derivation Function) соответствующие ключи имеют длину 256 бит. У каждого ключа усекают 128 старших бит (Trunc); в результате получают рабочие ключи длиной 128 бит. Эти процедуры выполняют параллельно в UE и MME.

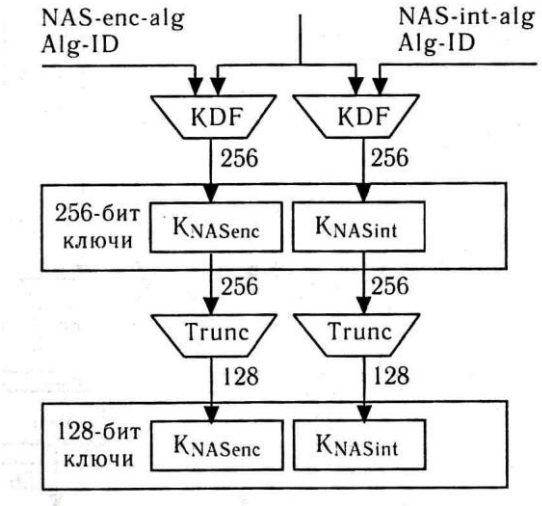

Рис.3.14. Генерирование ключей шифрации и целостности для NAS сигнализации

Сигнальные сообщения протокола RRC (AS) также шифруют и обеспечивают их целостность. Пакеты трафика только шифруют. Эти операции производят в обслуживающей eNB и UE. Схема получения ключей шифрации и целостности (рис.3.15) для AS и UP трафика отличается от схемы рис.3.14 тем, что исходным параметром здесь служит вторичный промежу-

точный ключ K_{eNB} <256 бит>. Этот ключ генерируют, также используя KDF, где входными параметрами являются: K_{ASME}, счетчик сигнальных сообщений NAS вверх, прежнее значение K_{eNB}, идентификатор соты и номер частотного канала в направлении вверх. Таким образом, при каждой периодической локализации UE происходит изменение K_{eNB}.

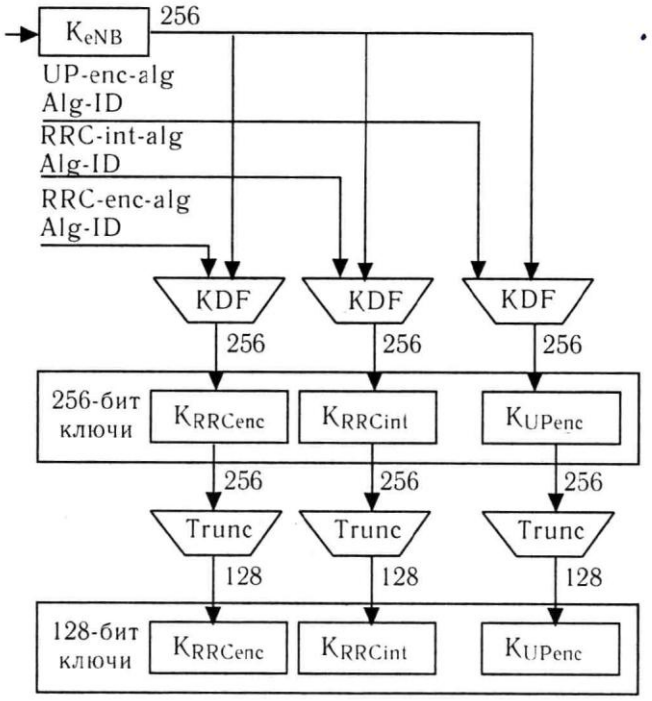

Рис.3.15. Генерирование ключей для AS сигнализации и пакетов трафика UP

K_{eNB} меняется и при хэндовере; при этом в алгоритме генерации нового K_{eNB} можно использовать дополнительный параметр NH (Next Hop), фактически счетчик числа базовых станций, по цепочке обслуживающих абонента. Все реализуемые процедуры безопасности в сети E-UTRAN проиллюстрированы рис. 3.16.

Алгоритм шифрации и дешифрации сообщений представлен на рис. 3.17. Исходными параметрами в нем являются: шифрующий ключ *KEY* <128 бит>, счетчик пакетов (блоков) *COUNT* <32 бита>, идентификатор сквозного канала *BEARER* <5 бит>, указатель направления передачи *DIRECTION* <1 бит> и длина шифрующего ключа *LENGTH*. В соответствии с выбранным алгоритмом шифрации *EEA (EPS Encryption Algorithm)* вырабатывается шифрующее число *KEYSTREAM BLOCK*, которое при передаче складывают по модулю два с шифруемым исходным текстом блока *PLAINTEXT BLOCK*. При дешифрации на приемном конце повторно совершают ту же операцию.

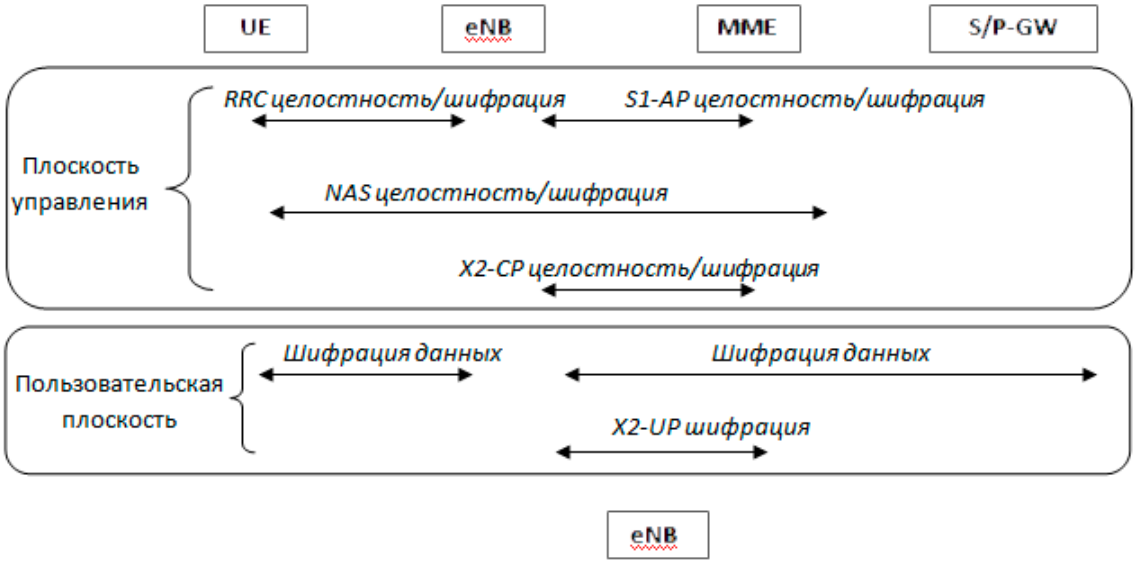

Рис.3.16. Реализуемые процедуры безопасности в сети E-UTRAN

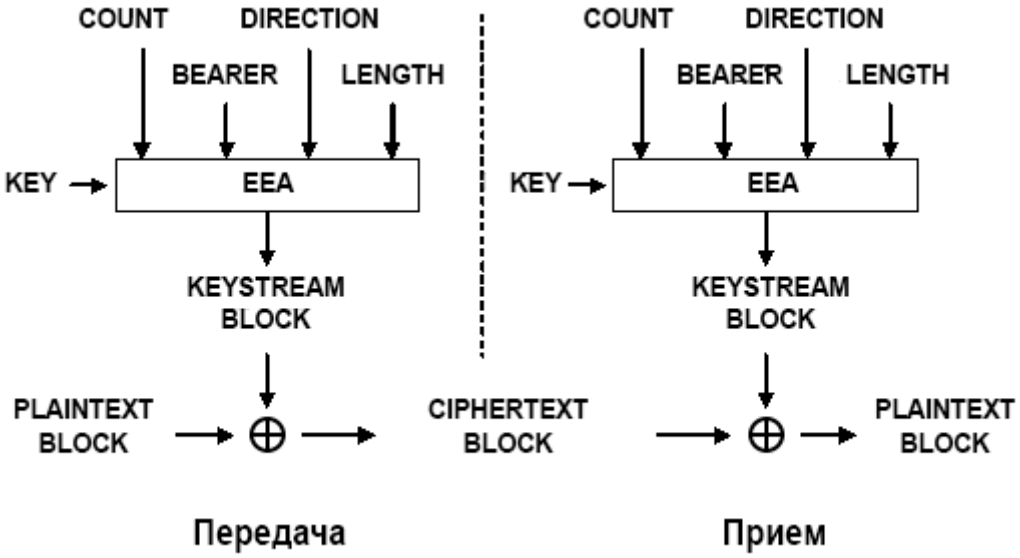

Рис.3.17. Алгоритм шифрации в E-UTRA

Процедура защиты целостности сообщения состоит в генерации “хвоста“ MAC (Message Authentication Code) <32 бита>, присоединяемого к передаваемому пакету. Алгоритм генерации MAC и проверки целостности полученного пакета путем сравнения XMAC с MAC (они должны совпасть) показан на рис. 3.18.

В алгоритме *EIA (EPS Integrity Algorithm)* использован ключ целостности *KEY* <128 бит>, счетчик сообщений *COUNT* <32 бита>, идентификатор

сквозного канала *BEARER* <5 бит>, указатель направления передачи *DIRECTION* <1 бит> и само сообщение *MESSAGE*.

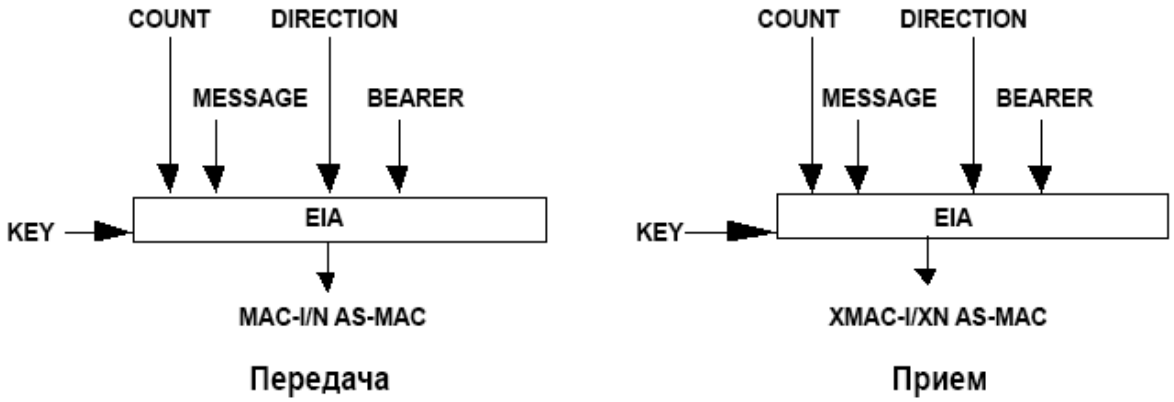

Рис.3.18. Алгоритм проверки целостности в E-UTRA