ХАРЬКІВСКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ СЕМЕНА КУЗНЕЦЯ

ТЕХНОЛОГІЯ МЕРЕЖ МОБІЛЬНОГО ЗВ'ЯЗКУ LTE

ЛЕКЦІЯ 10

Доцент кафедри кібербезпеки та ІТ
к.т.н. Лимаренко Вячеслав Володимирович
к.т. 066-0708586 (Viber, Telegram)

Стандарт LTE

Принципи побудови і функціонування мереж LTE

За даними компанії HUAWEI Рис.1, мережі другого покоління 2G можуть забезпечити передачу даних до 114 Кбіт/с при використанні GPRS та до 472,6 Кбіт/с за технологією EDGE. Використовуючи 3G можна отримати швидкість до 21,6 Мбіт/с. У свою чергу, LTE забезпечує швидкість до 326,4 Мбіт/с від базової станції до користувача і до 172,8 Мбіт/с у зворотному напрямку

Рис.1. Рік розробки та швидкість передавання інформації в мережах різних поколінь

Принципи побудови і функціонування мереж LTE

Метою створення стандарту LTE є:
 збільшення можливостей високошвидкісних систем мобільного зв'язку;
 зменшення вартості передачі даних;
 можливість надання широкого спектру недорогих послуг.

До числа основних технологічних особливостей LTE відносяться:
 Flexible Bandwidth – гнучкий вибір полоси каналу: 1.4, 3, 5, 10, 15, 20 МГц.
 Більш широкий вибір частотного діапазону для впровадження LTE: 700, 800, 900, 1800, 2100, 2300, 2600, 3500 МГц та ін.
 OFDMA технологія радіодоступу.
 3 схеми модуляції QPSK, 16QAM, 64QAM. Вибір необхідної схеми модуляції залежно від конкретних радіоумов.
 Технологія MIMO (Multiple Input Multiple Output) – використання декількох антен для передачі даних.
 Carrier Aggregation – технологія агрегації частот для збільшення швидкості передачі даних.
 All IP архітектура і відсутність контролера

Ще одна перевага LTE — варіативність частотних діапазонів, придатних для запуску (від 800 до 2600 МГц).

Принципи побудови і функціонування мереж LTE

Однак поліпшення якісних і кількісних показників мереж нового покоління висуває й нові вимоги, пов'язані з підвищенням безпеки переданої інформації. Оскільки технологія 4G повністю заснована на протоколі IP, чи не перетворяться мобільні мережі в Інтернет з притаманними йому небезпеками і проблемами? Для відповіді на це питання необхідно знання переваг LTE. Мобільний зв'язок четвертого покоління передбачає використання цілого спектру технологій, які раніше розвивалися паралельно. Всі вони внесли свій внесок у специфікацію LTE реалізованої в двох основних варіантах технологій: з дуплексним частотним поділом LTE-FDD (Frequency Division Duplex) і часовим поділом LTE-TDD (Time Division Duplex) [1]. Опора на безліч різних технологій ускладнює пошук вразливостей в LTE, що добре з точки зору безпеки — злом радіоканалу для одних методів може спрацювати, а для інших — ні. Якщо в 3G голосовий трафік і дані передавалися по двом різним мережам, то в мережах 4G весь трафік проходить через єдину архітектуру EPC (Evolved Packet Core) за протоколом IP. Ось чому в компанії Cisco вважають, що всі загрози безпеки інформації, що передається, пов'язані саме з протоколом IP.

З фізичної точки зору в мережах LTE використовуються:

- великі смуги частот;
- високорівнева модуляція сигналу;
- технологія MIMO.

Разом вони забезпечують адекватну завадостійкість, високі швидкості передачі даних і ємність мережі.

Принципи побудови і функціонування мереж LTE

LTE включає в себе мережу радіодоступу (Evolved Universal Terrestrial Radio Access Network, E-UTRAN) і вдосконалене пакетне ядро (Evolved Packet Core, EPC). Мережа LTE побудована як сукупність нових базових станцій eNB (Evolved NodeB або eNodeB), де сусідні eNB з'єднані між собою інтерфейсом X2. eNB підключені до EPC за допомогою інтерфейсу S1. На рис.2 показано взаємодію нових елементів в архітектурі мережі: S-GW (Serving Gateway) – обслуговуючих шлюзів, що містять ПЗ управління по протоколу ММ (MME - Mobility Management Entity).

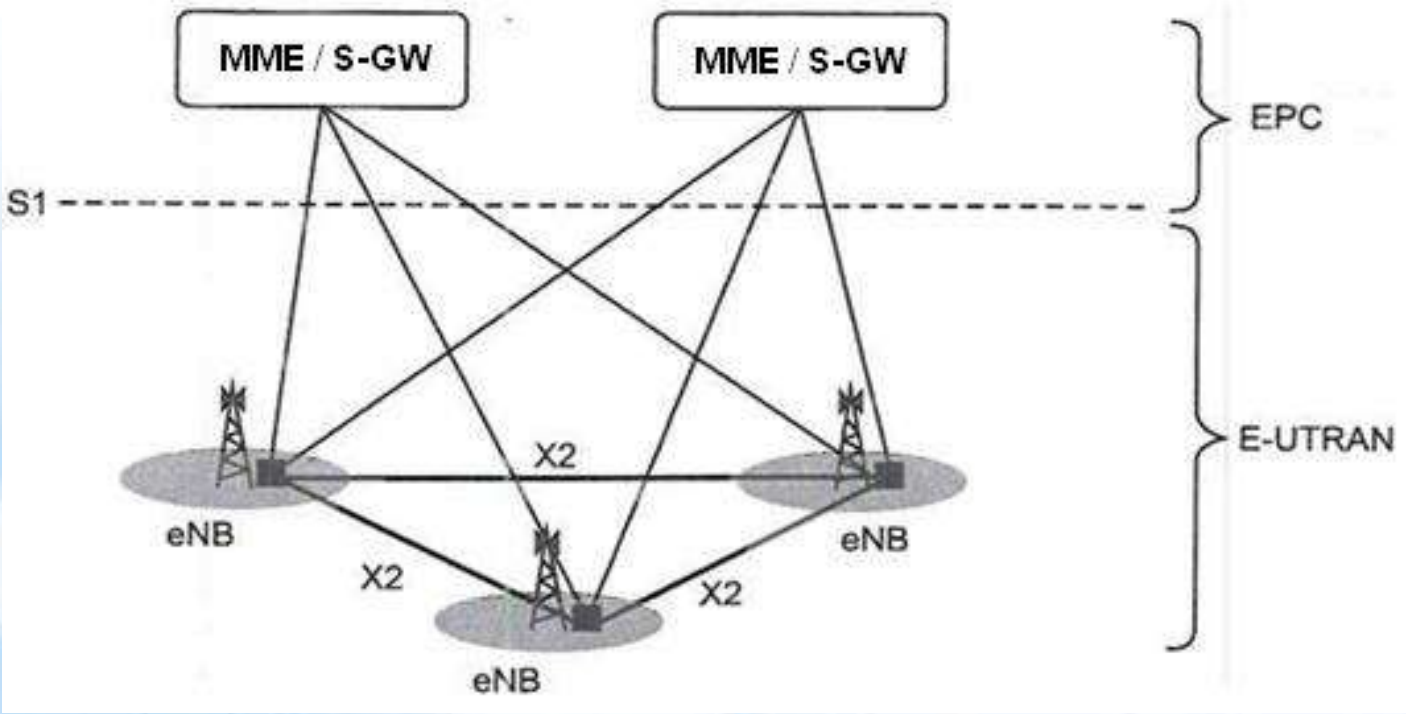


Рис. 2. Спрощена архітектура мережі LTE

Принципи побудови і функціонування мереж LTE

У мережі радіодоступу радіоінтерфейс між UE і eNB здійснений на основі технології ортогонального частотного рознесення (Orthogonal Frequency Division Multiplexing, OFDMA). Робота EPC заснована на технології IP. Таку структуру відносять до All-IP Network (AIPN). Структура мережі LTE приведена на рис. 3. Ядро мережі EPC (Evolved Packet Core) складається з обслуговуючого шлюзу S-GW (Serving Gateway), шлюзу для виходу на пакетні мережі P-GW (Packet Data Network Gateway), структури управління по протоколу Mobility Management MME (Mobility Management Entity) , пов'язаної з S-GW і eNodeB сигнальними інтерфейсами.

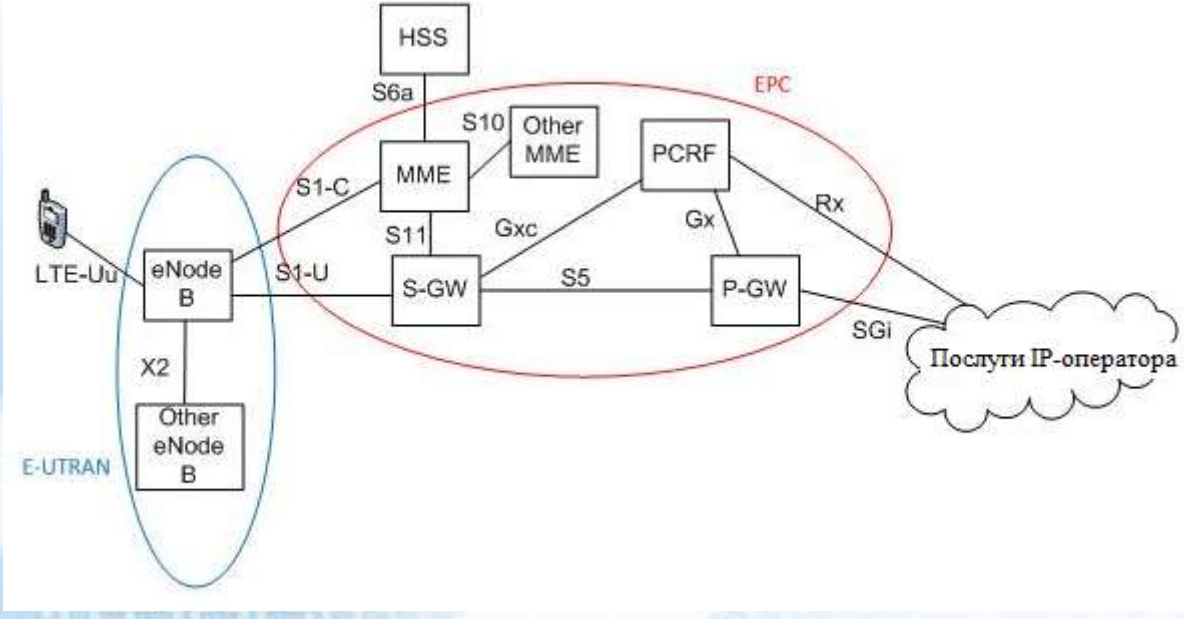


Рис. 3. Структура мережі LTE

Принципи побудови і функціонування мереж LTE

Функції eNodeB (Evolved NodeB)

eNodeB об'єднує в собі функції базових станцій і контролерів мереж 3-го покоління:

- забезпечує передачу трафіку і сигналізації по радіоканалу,
- управляє розподілом радіоресурсів,
- забезпечує наскрізний канал трафіку до S-GW,
- підтримує синхронізацію передач і контролює рівень перешкод в соті,
- забезпечує шифрацию і цілісність передачі по радіоканалу,
- вибирає MME і організовує сигнальний обмін з ним,
- виробляє стиснення заголовків IP-пакетів,
- підтримує послуги мультимедійного мовлення,
- при використанні структури з підсилювачами потужності на антеною щоглі організовує управління антенами за спеціальним інтерфейсу Iuant.

Інтерфейс S1, як показано на рис.3, підтримує передачу даних з S-GW і сигналізації через MME. Відзначимо, що eNB може мати з'єднання з декількома S-GW.

Інтерфейси X2 використовують для організації хендовера між сусідніми базовими станціями, в тому числі і при балансуванні навантаження між ними. При цьому інтерфейси X2 можуть бути логічними, тобто для їх організації не обов'язково реальне фізичне з'єднання між eNB.

Принципи побудови і функціонування мереж LTE

Функції обслуговуючого шлюзу S-GW:

- маршрутизація переданих пакетів даних,
- установка якісних показників (Quality of Service, QoS) послуг, що надаються,
- буферизація пакетів для UE, які перебувають в стані Idle Mode,
- надання облікових даних для тарифікації та оплати виконаних послуг.

S-GW є якірної структурою, що забезпечує мобільність абонентів. Кожну працюючу UE обслуговує певний S-GW. Теоретично UE може бути пов'язана з декількома пакетними мережами; тоді її будуть обслуговувати кілька серверів S-GW.

Принципи побудови і функціонування мереж LTE

Функції P-GW (Packet Data Network Gateway)

Шлюз для виходу на пакетні мережі P-GW організовує точку доступу до зовнішніх IP-мереж. Відповідно P-GW є якірним шлюзом для забезпечення трафіку. Якщо абонент має статичний IP-адресу, то P-GW його активізує. У разі, якщо абонент повинен отримати на час сеансу зв'язку динамічний IP-адресу, P-GW запитує його з сервера DHCP (Dynamic Host Configuration Protocol) або сам виконує необхідні функції DHCP, після чого забезпечує доставку IP-адреси абонента. До складу P-GW входить PCEF (Policy and Charging Enforcement Function), який входить забезпечує якісні характеристики послуг на зовнішньому з'єднанні через інтерфейс Sgi і фільтрацію пакетів даних. При обслуговуванні абонента в домашній мережі функції P-GW і S-GW можуть виконувати як два різних, так і один пристрій. Інтерфейс S5 являє собою тунельне з'єднання GPRS або Proxy Mobile Ipv6. Якщо P-GW і S-GW знаходяться в різних мережах (наприклад, при обслуговуванні абонента в роумінгу), то інтерфейс S5 замінюють інтерфейсом S8.

Принципи побудови і функціонування мереж LTE

Функції MME (Mobility Management Entity)

Керуючий блок MME насамперед підтримує виконання процедур протоколу Mobility Management: забезпечення безпеки роботи в мережі при підключенні UE і вибір S-GW, P-GW. MME пов'язаний з HSS своєї мережі за допомогою інтерфейсу S6a. Інтерфейс S10, що з'єднує різні MME, дозволяє обслуговувати UE при переміщеннях абонента, а також при його знаходженні в роумінгу.

Функції PCRF

Policy and Charging Resource Function (PCRF) по суті являє собою керуючий сервер, що забезпечує централізоване управління ресурсами мережі, облік і тарифікацію послуг, що надаються. Як тільки з'являється запит на нове активне з'єднання, ця інформація надходить на PCRF. Він оцінює наявні в його розпорядженні ресурси мережі й направляє в PCEF шлюзу P-GW команди, які встановлюють вимоги до якості послуг і до їх тарифікації.

Принципи побудови і функціонування мереж LTE

Базові станції в LTE стали більш інтелектуальнімі и самостійними - вони отримали можлівість маршрутізуваті трафік, что дозволило організовувати з'єднання между абонентами безпосередно, минаючи ядро мережі. В результате у зловмісників з'явилася можлівість
атакуваті самі базові станції, які працюють только за протоколом IP, тому полегшується несанкціонованій доступ до мережі і, отже, могут буті вікорістані класичні атаки на канальному рівні, шірокомовні шторми й інші варіанти нападів.
Щоб звесті до мінімуму атаки на конфіденційну інформацію, базова станція повинна забезпечити виконання таких важлівіх операцій, як кодування и розшифровку користувачів даних, а також зберігання ключів.

Принципи побудови і функціонування мереж LTE

Для мінімізації шкоди, що наноситися в разі крадіжкі информации про ключі з базових станцій розроблені спеціальні заходи протідії:

- *перевірка цілісності пристрою;*
- *взаємна аутентіфікація базової станції оператора (видача сертифікатів);*
- *безпечні оновлення;*
- *механізм контролю доступу;*
- *сінхронізація годині;*
- *фільтрація трафіку*

Принципи побудови і функціонування мереж LTE

Існують чотири основні вимоги до механізмів безпеки технології LTE:

- *забезпечити як мінімум такий же рівень безпеки, як і в мережах типу 3G, не доставляючи незручностей користувачам;*
- *забезпечити захист від Інтернет-атак;*
- *механізми безпеки для мереж 4G не повинні створювати перешкод для переходу зі стандарту 3G на стандарт LTE;*
- *забезпечити можливість подальшого використання програмно-апаратного модуля UMTS (універсальна сім-карта).*

Принципи побудови і функціонування мереж LTE

Стандарт LTE виділяє п'ять основних груп безпеки це, насамперед:

- *архітектура безпеки мережі повинна забезпечити користувачів надійним доступом до сервісів і захист від атак на інтерфейси;*
- *мережевий рівень повинен дозволяти вузлам мережі безпечно обмінюватися як даними користувачів, так і керуючими даними і забезпечувати захист від атак на провідні лінії;*
- *користувальницький рівень повинен забезпечувати безпечний доступ до мобільного пристрою;*
- *рівень додатків повинен гарантувати безпечний обмін повідомленнями;*
- *видимість і можливість зміни налаштувань безпеки повинна дозволяти користувачеві дізнаватися, чи забезпечується безпека і включати різні режими для її забезпечення.*

Принципи побудови і функціонування мереж LTE

До числа основних очевидних загроз інформаційної безпеки в мережах LTE належать:

- атаки DoS на мережу (Denial of Service). Ємність радіоканалу в LTE передбачається велика, але все ж вона має обмеження. Мережеві ресурси базової станції діляться між абонентами, і хоча є обмеження для монополізації смуги окремим користувачем, тим не менш, атака на відмову в обслуговуванні мережі цілком можлива;
- вірусні атаки. Хоча таким атакам піддаються пристрої, а не мережа, технологія LTE збільшує швидкість поширення шкідливих програм, оскільки сам цей стандарт є високошвидкісним;
- атаки на додаткові сервіси. Власне, LTE розроблялося не тільки для забезпечення доступу до Інтернету мобільних користувачів, а скоріше як платформа для впровадження нових відео, ігрових та багатьох інших послуг. Ці сервіси можуть бути уразливі для самих різноманітних атак — як з Інтернету, так і з мобільного мережі. Цілком можливо, що, атакувавши один з сервісів, зловмисники зможуть впровадити в клієнтські пристрої небезпечні програми.

Принципи побудови і функціонування мереж LTE

Всі функції захисту в LTE об'єднані стандартом і передбачають захист на декількох рівнях: на рівні доступу до мережі, на рівнях мережевого і користувальницького доменів, на рівні додатків та на рівні відображення і конфігурацій рисунок 4.

Рис. 4 Функції захисту в LTE

Принципи побудови і функціонування мереж LTE

Кожен з цих рівнів передбачає аутентифікацію і авторизацію всіх пристроїв, чого немає в Інтернеті. Технологія LTE передбачає використання не тільки IP-адреси, але і системи розповсюдження ключів шифрування для всіх пристроїв, підключених до мережі з можливістю переходу зі 128 до 256-бітові ключі і введення нових алгоритмів, зберігаючи зворотну сумісність. Крім алгоритмів шифрування і забезпечення комплексної безпеки в мережах 4G використовуються додаткові алгоритми, які навіть за умови того, що один з них буде зламаний, решта забезпечать безпеку мережі LTE. Крім того, в LTE зберігаються і методи аутентифікації користувачів по прив'язці до SIM карти, як в традиційному мобільному зв'язку. Користувач може заблокувати доступ до телефону з PIN-кодом.

Безпека в мережах LTE

Безпека в мережах LTE полягає в декількох видах:
Захист абонентів.
Захист переданих повідомлень.
Шифрування повідомлень.
Аутентифікація і абонента, і мережі.

Захист абонента полягає в тому, що в процесі обслуговування його приховують тимчасовими ідентифікаторами.

Для закриття даних в мережах LTE використовується потокове шифрування методом накладення на відкриту інформацію псевдослучайной послідовності (ПСП) за допомогою оператора XOR (виключає або). У цих мережах для забезпечення безпеки всередині мережі застосовується принцип тунелювання з'єднань. Шифрування можна піддавати пакети S1 і X2 за допомогою IPsec ESP, а також піддаються шифрування сигнальні повідомлення цих інтерфейсів.

Безпека в мережах LTE

У момент підключення або активізації абонентського обладнання (UE) в мережі, мережа запускає процедуру аутентифікації і угоди про ключі AKA (Authentication and Key Agreement). Метою цієї процедури є взаємна аутентифікація абонента і мережі і вироблення проміжного ключа KASME. Робота механізму AKA займає частки секунди, які необхідні для вироблення ключа в додатку USIM і для підтримання зв'язку з Центром реєстрації (HSS). Внаслідок цього, для досягнення швидкості передачі даних мереж LTE необхідно додати функцію оновлення ключової інформації без ініціалізації механізму AKA. Для вирішення цієї проблеми в мережах LTE пропонується використовувати ієрархічну ключову інфраструктуру. Тут також, як і в мережах 3G, додаток USIM та Центр аутентифікації (AuC) здійснює попередній розподіл ключів. Коли механізм AKA инициализируется для здійснення двосторонньої аутентифікації користувача і мережі, генеруються ключ шифрування CK і ключ загального захисту, які потім передаються з ПО USIM в Мобільне обладнання (ME) і з Центру аутентифікації в Центр реєстрації (HSS). ME і HSS, використовуючи ключову пару (CK; IK) і ID використовуваної мережі, виробляє ключ KASME. Встановивши залежність ключа від ID мережі, Центр реєстрації гарантує можливість використання ключа тільки в рамках цієї мережі. Далі KASME передається з Центру реєстрації в пристрій мобільного управління (MME) поточної мережі, де він використовується в якості майстер-ключа. На підставі KASME виробляється ключ Knas-enc, який необхідний для шифрування даних протоколу NAS між мобільним пристроєм (UE) і MME, і Knas-int, необхідний для захисту цілісності. Коли UE підключається до мережі, MME генерує ключ KeNB і передає його базових станцій. У свою чергу, з ключа KeNB виробляється ключ Kup-enc, який використовується для шифрування даних користувача протоколу U-Plane, ключ Krrc-enc для протоколу RRC (Radio Resource Control - протокол взаємодії між Мобільними пристроями і базовими станціями) і ключ Krrc-int, призначений для захисту цілісності.

Безпека в мережах LTE

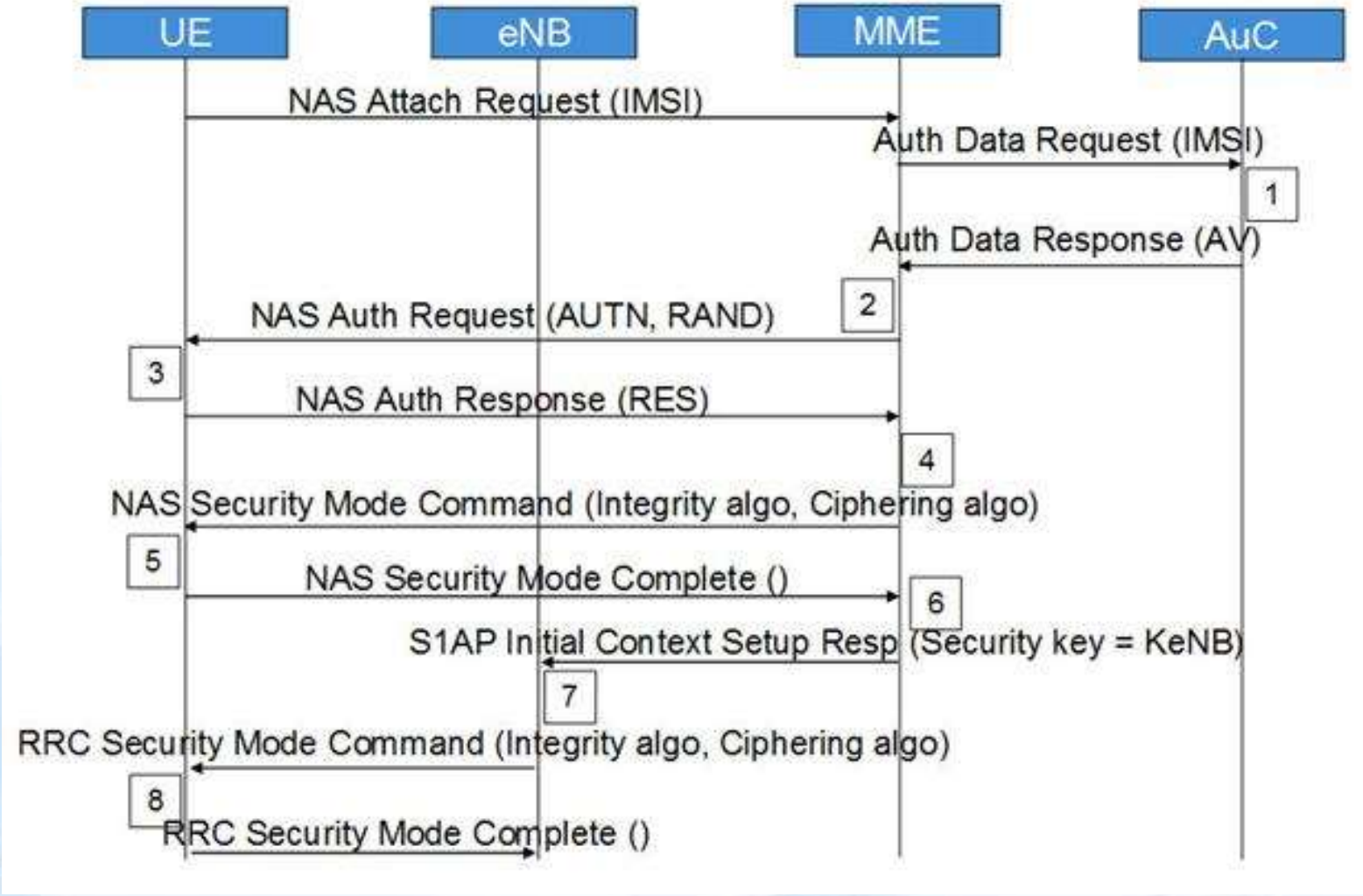
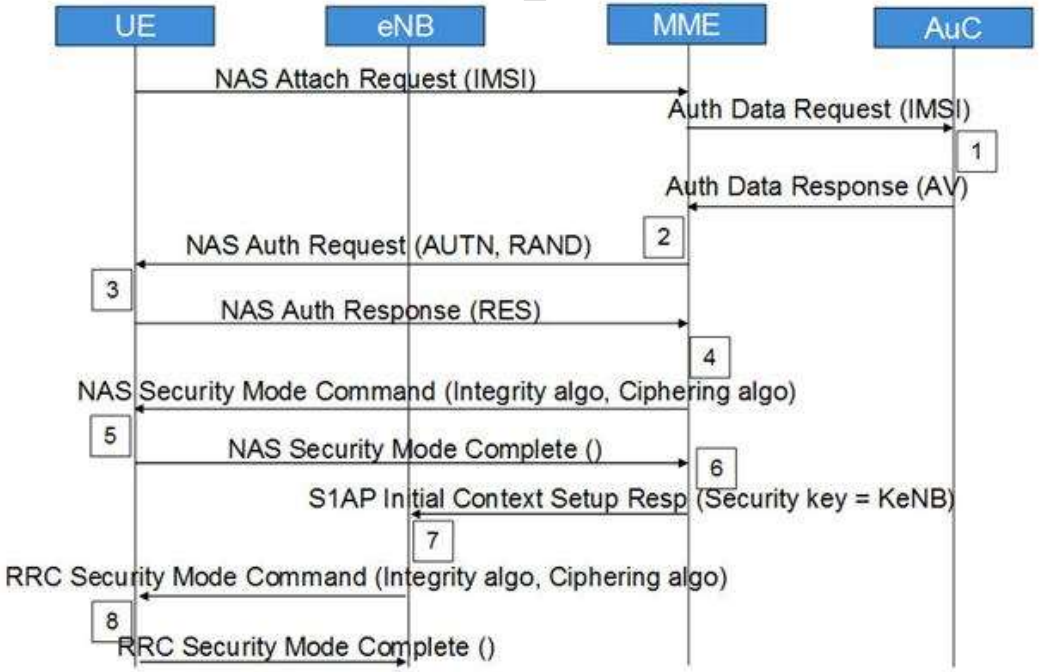


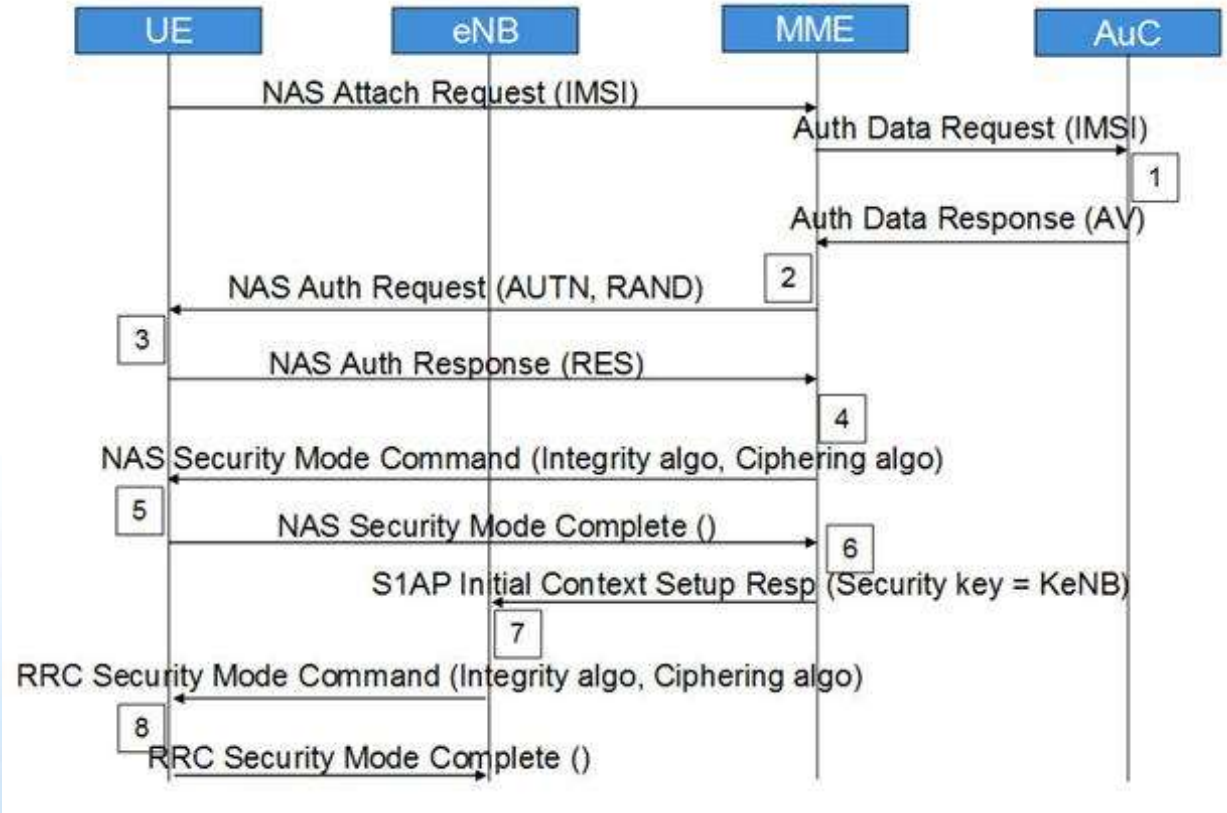
Рис. 5 Діаграмма аутентифікації та генерації ключа

Безпека в мережах LTE



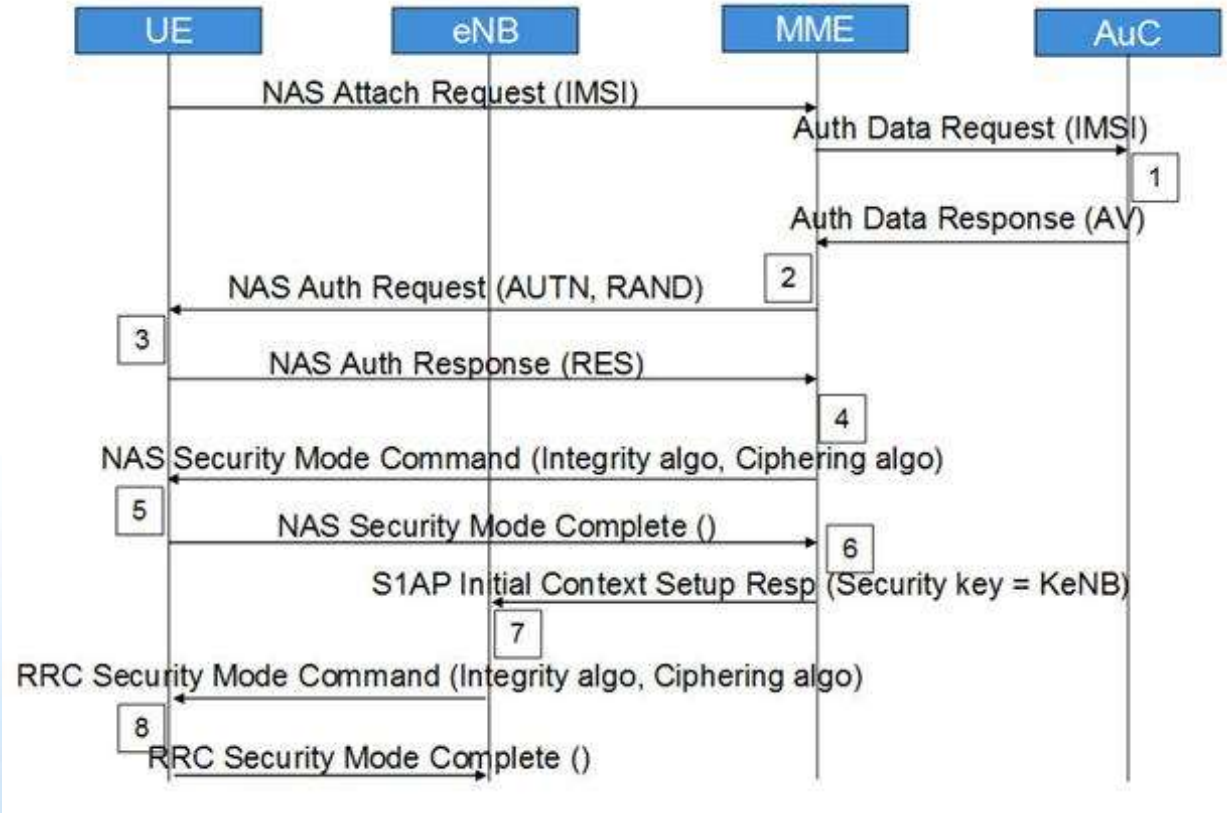
Крок 1. Запит про підключення до мережі від мобільної станції (UE). MME запитує аутентифікаційні дані, що відносяться до конкретного IMSI, відправляючи Authentication Data Request. AuC / HSS вибирає PSK, що відноситься до конкретного IMSI і обчислює аутентифікаційні дані по PSK. AuC / HSS відправляє назад AV с Authentication Data Response.

Безпека в мережах LTE



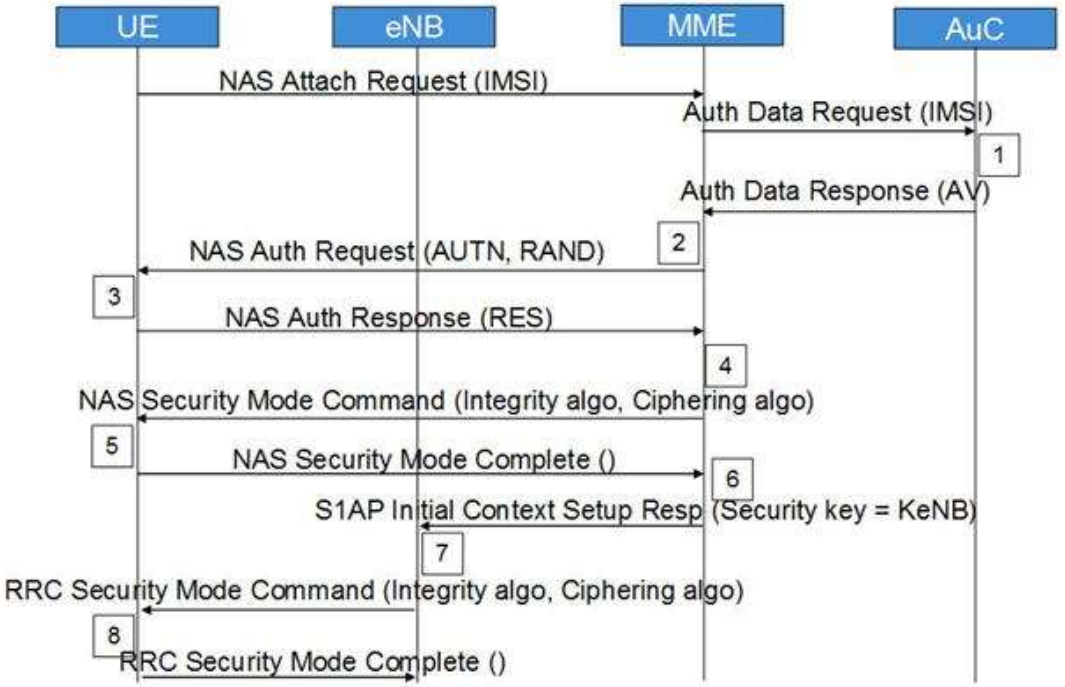
Крок 2. MME отримує IK, CK, XRES, RAND і AUTH з AV. MME відправляє AUTH і RAND за допомогою Authentication Request до UE.

Безпека в мережах LTE



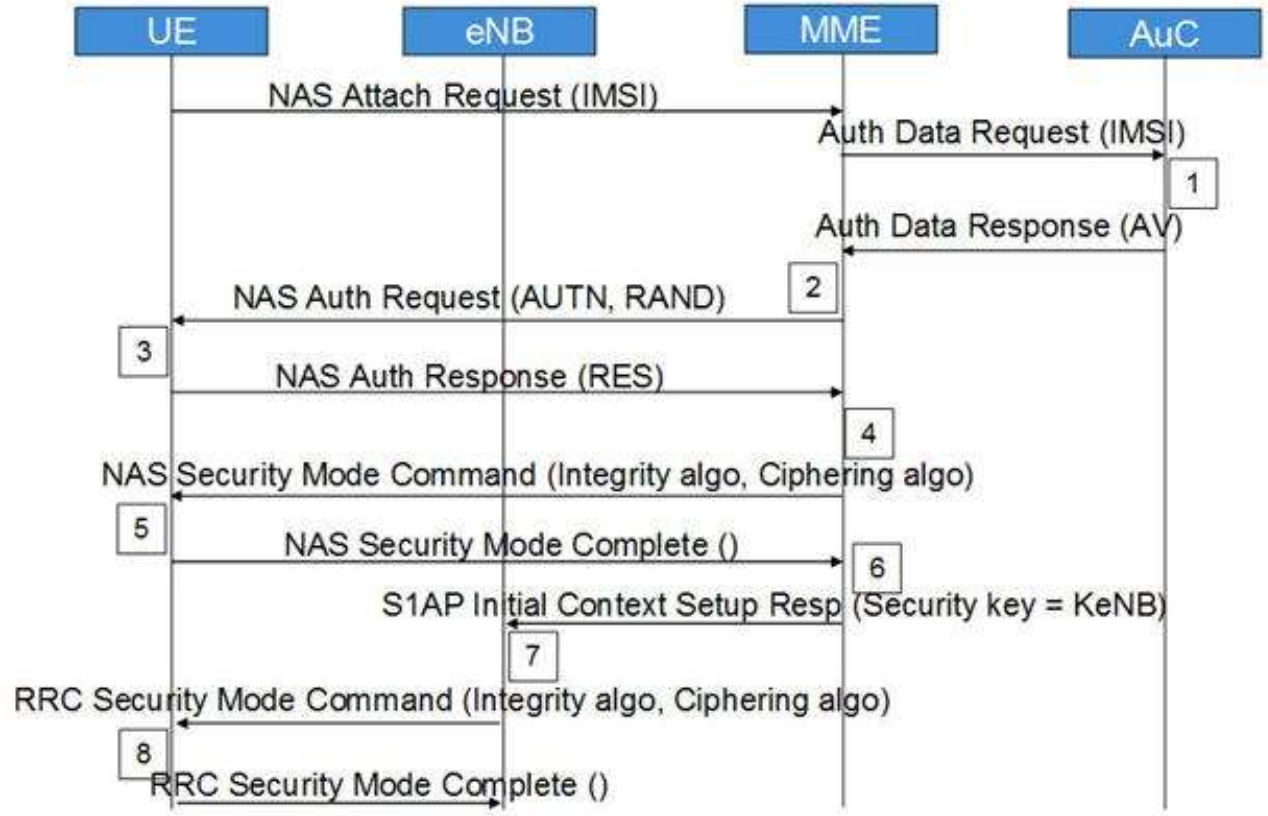
Крок 3. UE аутентифікує NW, перевіряючи отриманий AUTH. Після чого обчислює IK, CK, RES, XMAC зі свого ключа захисту, AMF, (OP), AUTH і RAND. Вона відправляє RES з Authentication response.

Безпека в мережах LTE



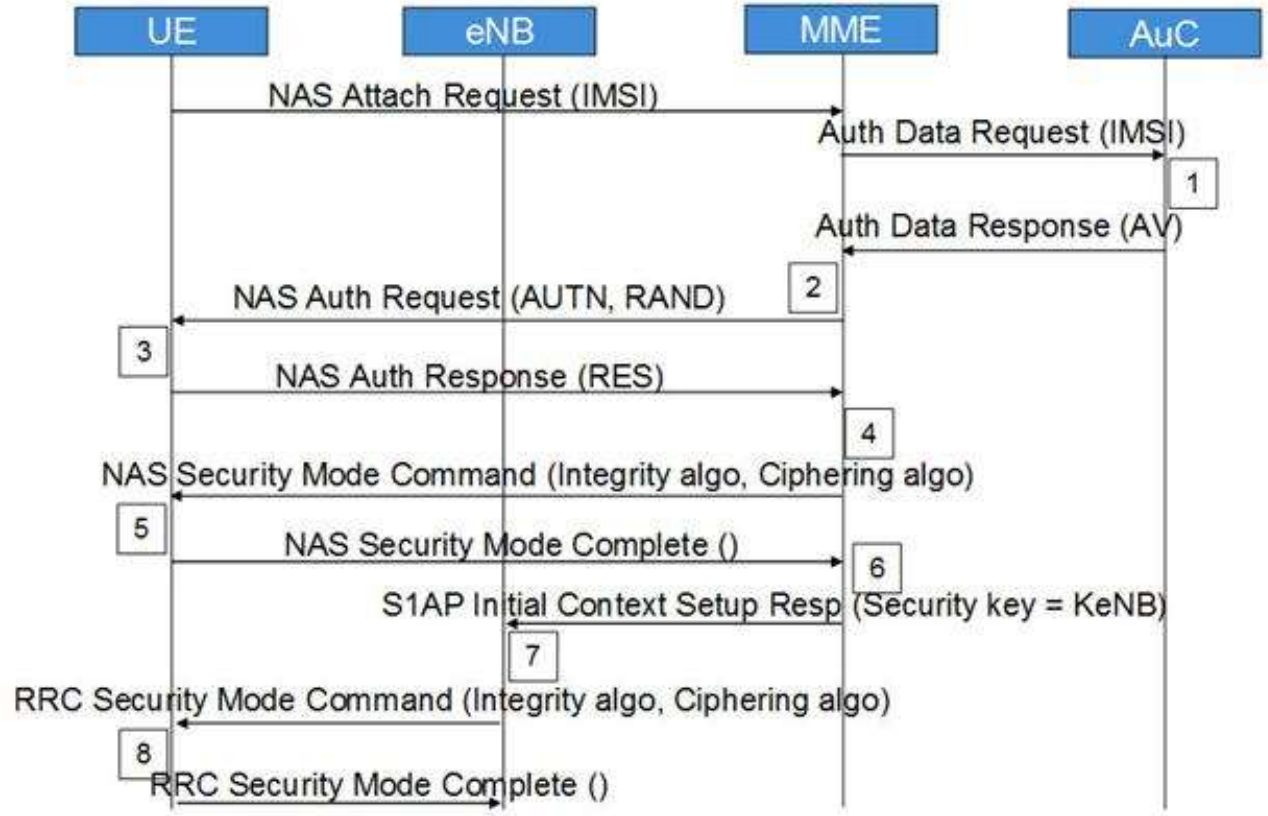
Крок 4. Після отримання RES, MME порівнює його з XRES і якщо вони збігаються, то аутентифікація пройшла успішно, в іншому випадку, MME відправляє збій аутентифікації (Authentication failure) до UE. MME скидає лічильник DL NAS. Розраховує KASME, KeNB, Knas-int, Knas-enc. Відправляє NAS команду режиму безпеки (алгоритм цілісності, алгоритм шифрування, NAS набір ключів ID, функцію безпеки UE) з цілісністю охоронюваних, але не зашифрованих, використовуючи Knas-inc.

Безпека в мережах LTE



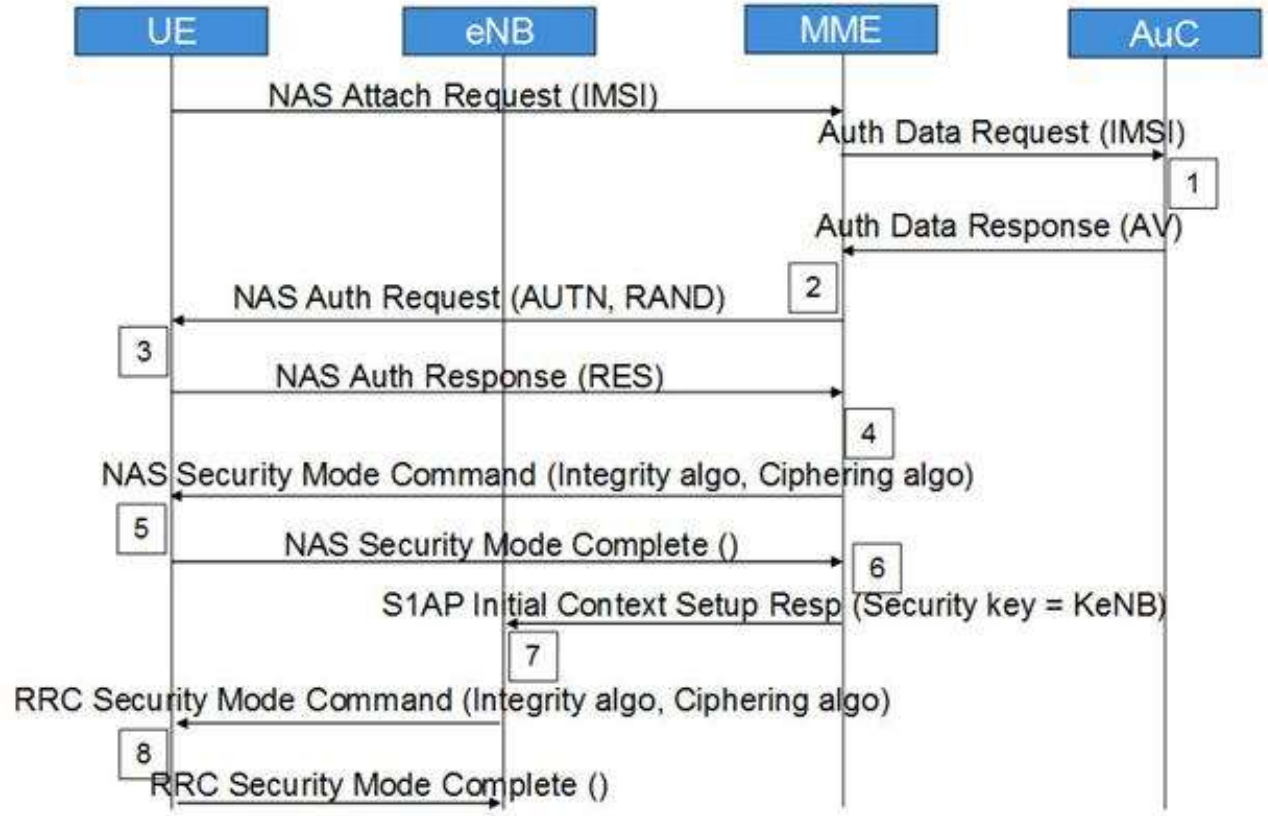
Крок 5. Після отримання NAS команди режиму безпеки, UE обчислює KASME, KeNB, Knas-int, Knas-enc. UE відправляє NAS режиму безпеки виконаний з цілісністю, захищених і зашифрованих.

Безпека в мережах LTE



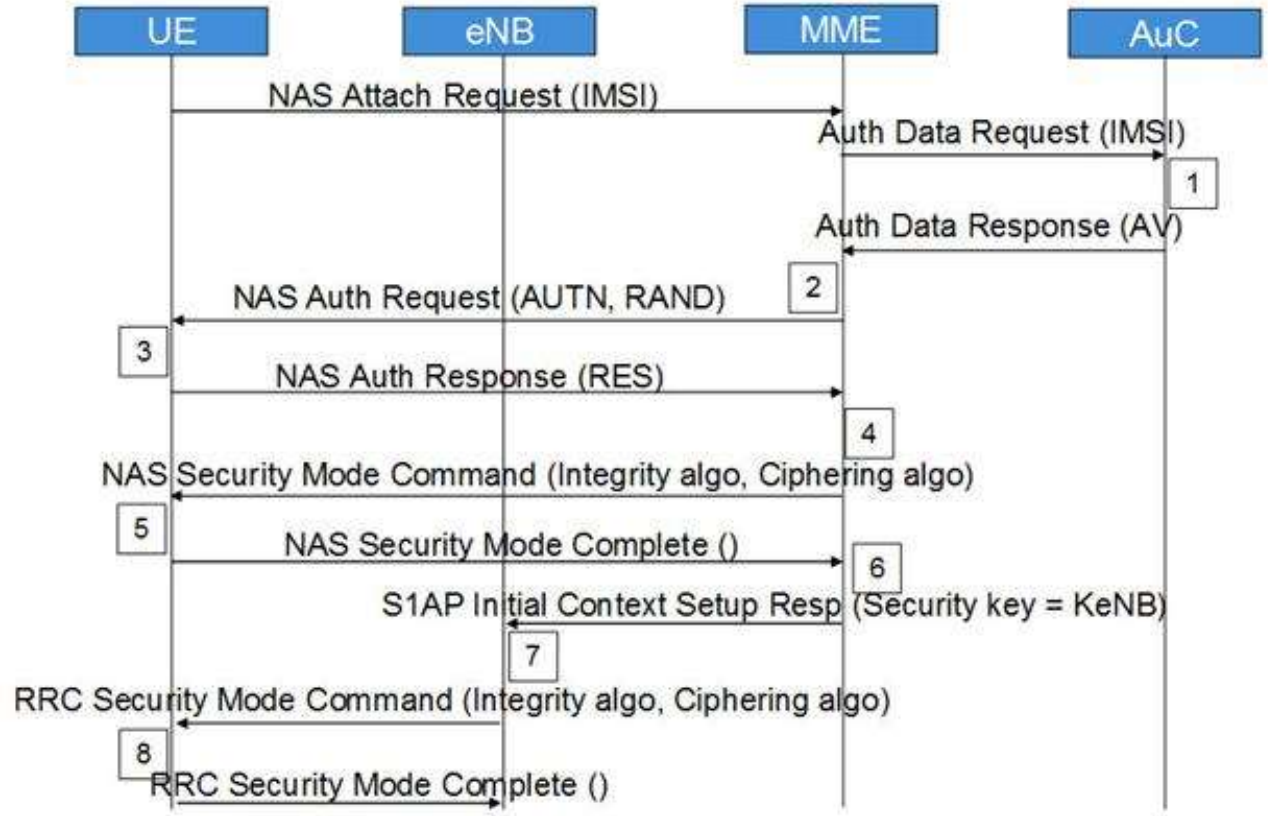
Крок 6. Після отримання NAS команди режиму безпеки від UE, MME відправляє KeNB в eNB з S1AP первісна установка початкового контексту (ключ захисту).

Безпека в мережах LTE



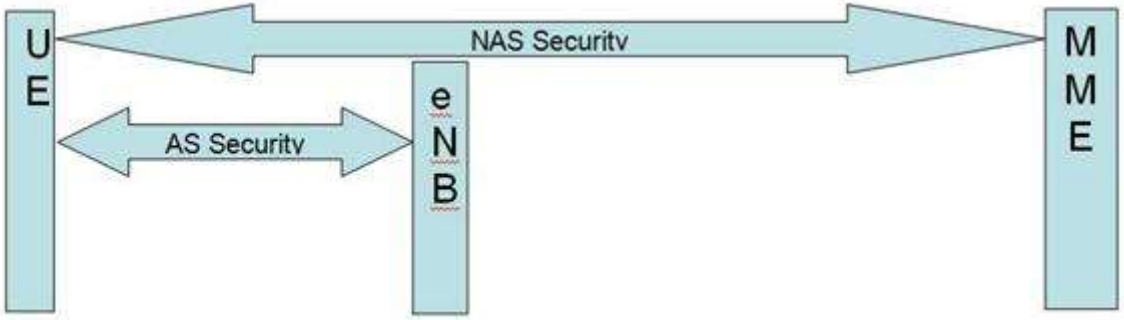
Крок 7. Після отримання KeNB, eNB обчислює Krrc-int, Krrc-enc, Kup-enc. Потім воно відправляє RRC ключ захисту команду з AS цілісністю алгоритму і AS шифрує алгоритм.

Безпека в мережах LTE



Крок 8. Після отримання RRC команди ключа захисту UE обчислює Krrc-int, Krrc-enc, Kup-enc. UE відправляє RRC виконаний ключ шифрування на eNB.

Безпека в мережах LTE



Архітектура безпеки LTE визначає механізм безпеки і для рівня NAS і для рівня AS.

Безпека NAS (Non-Access Stratum - шару без доступу):
Виконана для NAS повідомлень і належить області UE і MME.
У цьому випадку необхідна при передачі повідомлень NAS між UE і MME - цілісність, захищена і зашифрована з додатковим заголовком безпеки NAS.
Безпека AS (Access Stratum - шару з доступом):
Виконана для RRC і площині призначених для користувача даних, що належать області UE і eNB. Рівень PDCP на сторонах UE і eNB відповідає за шифрування і захист цілісності.
RRC повідомлення захищені цілісністю і зашифровані, проте дані U-Plane тільки зашифровані.

Безпека в мережах LTE

Генерація векторів аутентифікації

Для генерації векторів аутентифікації використовується криптографічний алгоритм з допомогою односпрямованих функцій (f1, f2, f3, f4, f5) коли прямий результат виходить шляхом простих обчислень, а зворотний результат не може бути отриманий зворотним шляхом, тобто не існує ефективного алгоритму отримання зворотного результату. Для цього алгоритму використовується випадкове 128 бітове випадкове число RAND, майстер-ключ K абонента, також 128 біт і порядковий номер процедури SQN (Sequence Number). Лічильник SQN змінює своє значення при кожній генерації вектора аутентифікації. Схожий лічильник SQN працює і в USIM. Такий метод дозволяє генерувати кожен раз новий вектор аутентифікації, не повторюючи попередній вже використаний вектор аутентифікації.

Крім цих трьох вихідних величин: SQN, RAND і K в алгоритмі f1 бере участь поле управління аутентифікацією Authentication Management Field (AMF), а в алгоритмах f2 - f5 вихідні параметри - RAND і K, що і продемонстровано на рис. 3, 4. На виходах відповідних функцій отримують Message Authentication Code (MAC) - 64 біта; XRES - eXpected Response, результат роботи алгоритму аутентифікації <32 - 128 біт>; ключ шифрування CK, що генерується з використанням вхідних (K, RAND) -> f3-> CK; ключ цілісності IK, згенерований з використанням входить (K, RAND) -> f4-> IK; і проміжний ключ Anonymity Key (AK), що генерується за допомогою (K, RAND) -> f5-> AK - 64 біта.

При обслуговуванні абонента мережею LTE ключі CK і IK в відкритому вигляді в ядро мережі залишають поза передачею. В цьому випадку HSS генерує KASME за допомогою алгоритму KDF (Key Derivation Function), для якого вихідними параметрами є CK і IK, а також ідентифікатор яка обслуговує мережі і SQNÅAK. Вектор аутентифікації містить RAND, XRES, AUTN і KASME, на основі якого відбувається генерація ключів шифрування і цілісності, які використовуються у відповідному алгоритмах.

Безпека в мережах LTE

Генерація векторів аутентифікації

Для генерації векторів аутентифікації використовується криптографічний алгоритм з допомогою односпрямованих функцій (f1, f2, f3, f4, f5) коли прямий результат виходить шляхом простих обчислень, а зворотний результат не може бути отриманий зворотним шляхом, тобто не існує ефективного алгоритму отримання зворотного результату. Для цього алгоритму використовується випадкове 128 бітове випадкове число RAND, майстер-ключ K абонента, також 128 біт і порядковий номер процедури SQN (Sequence Number). Лічильник SQN змінює своє значення при кожній генерації вектора аутентифікації. Схожий лічильник SQN працює і в USIM. Такий метод дозволяє генерувати кожен раз новий вектор аутентифікації, не повторюючи попередній вже використаний вектор аутентифікації.

Крім цих трьох вихідних величин: SQN, RAND і K в алгоритмі f1 бере участь поле управління аутентифікацією Authentication Management Field (AMF), а в алгоритмах f2 - f5 вихідні параметри - RAND і K, що і продемонстровано на рис. 3, 4. На виходах відповідних функцій отримують Message Authentication Code (MAC) - 64 біта; XRES - eXpected Response, результат роботи алгоритму аутентифікації <32 - 128 біт>; ключ шифрування CK, що генерується з використанням вхідних (K, RAND) -> f3-> CK; ключ цілісності IK, згенерований з використанням входить (K, RAND) -> f4-> IK; і проміжний ключ Anonymity Key (AK), що генерується за допомогою (K, RAND) -> f5-> AK - 64 біта.

При обслуговуванні абонента мережею LTE ключі CK і IK в відкритому вигляді в ядро мережі залишають поза передачею. В цьому випадку HSS генерує KASME за допомогою алгоритму KDF (Key Derivation Function), для якого вихідними параметрами є CK і IK, а також ідентифікатор яка обслуговує мережі і SQNÅAK. Вектор аутентифікації містить RAND, XRES, AUTN і KASME, на основі якого відбувається генерація ключів шифрування і цілісності, які використовуються у відповідному алгоритмах.

Безпека в мережах LTE

Генерація векторів аутентифікації

Коли мобільна станція отримує з ядра мережі три параметра (RAND, AUTN і KSIASME, де KSI - Key Set Identifier, індикатор встановленого ключа, однозначно пов'язаний з KASME в мобільної станції).

Після чого використовуючи RAND і AUTN, USIM на основі алгоритмів безпеки, тотожних зберігаються в HSS, виробляє обчислення XMAC, RES, CK і IK.

Потім у відповіді RES UE передає в MME обчислене RES, яке має збігтися з XRES, отриманим з HSS. Так мережу аутентифікує абонента. Обчисливши XMAC, UE порівнює його з MAC, отриманим нею в AUTN. При успішній аутентифікації абонентом мережі (MAC = XMAC) UE повідомляє про це у відповіді RES. Якщо аутентифікація мережі не вдалася (MAC ≠ XMAC), то UE направляє в MME відповідь CAUSE, де вказує причину невдачі аутентифікації.

При успішному завершенні попереднього етапу MME, eNB і UE виробляють генерацію ключів, використовуваних для шифрування і перевірки цілісності одержуваних повідомлень. У LTE є ієрархія ключів, яка приведена на рис. 8.

Вектори аутентифікації (рис. 6, 7):
Ключі IK і CK генеруються і в центрі аутентифікації, і в USIM;
Ключ AK генерується тільки в центрі аутентифікації;
Відповідь XRES генерується тільки в центрі аутентифікації, а RES генерується в USIM;
Код MAC генерується тільки в центрі аутентифікації, а відповідний йому параметр XMAC генерується в USIM;
Маркер AUTH генерується тільки в центрі аутентифікації.

Безпека в мережах LTE

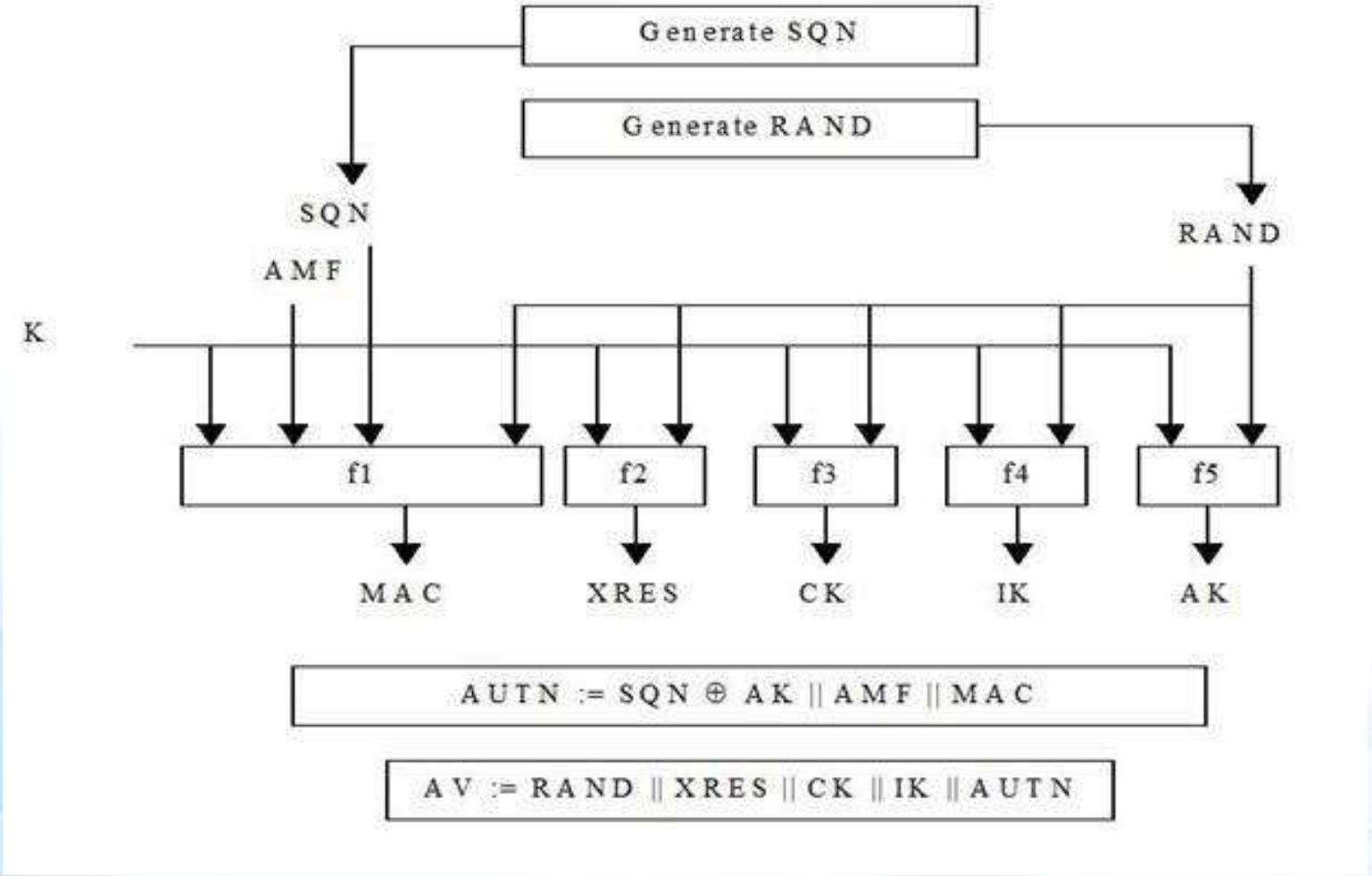


Рис. 6. Створення векторів на передавальній стороні

Безпека в мережах LTE

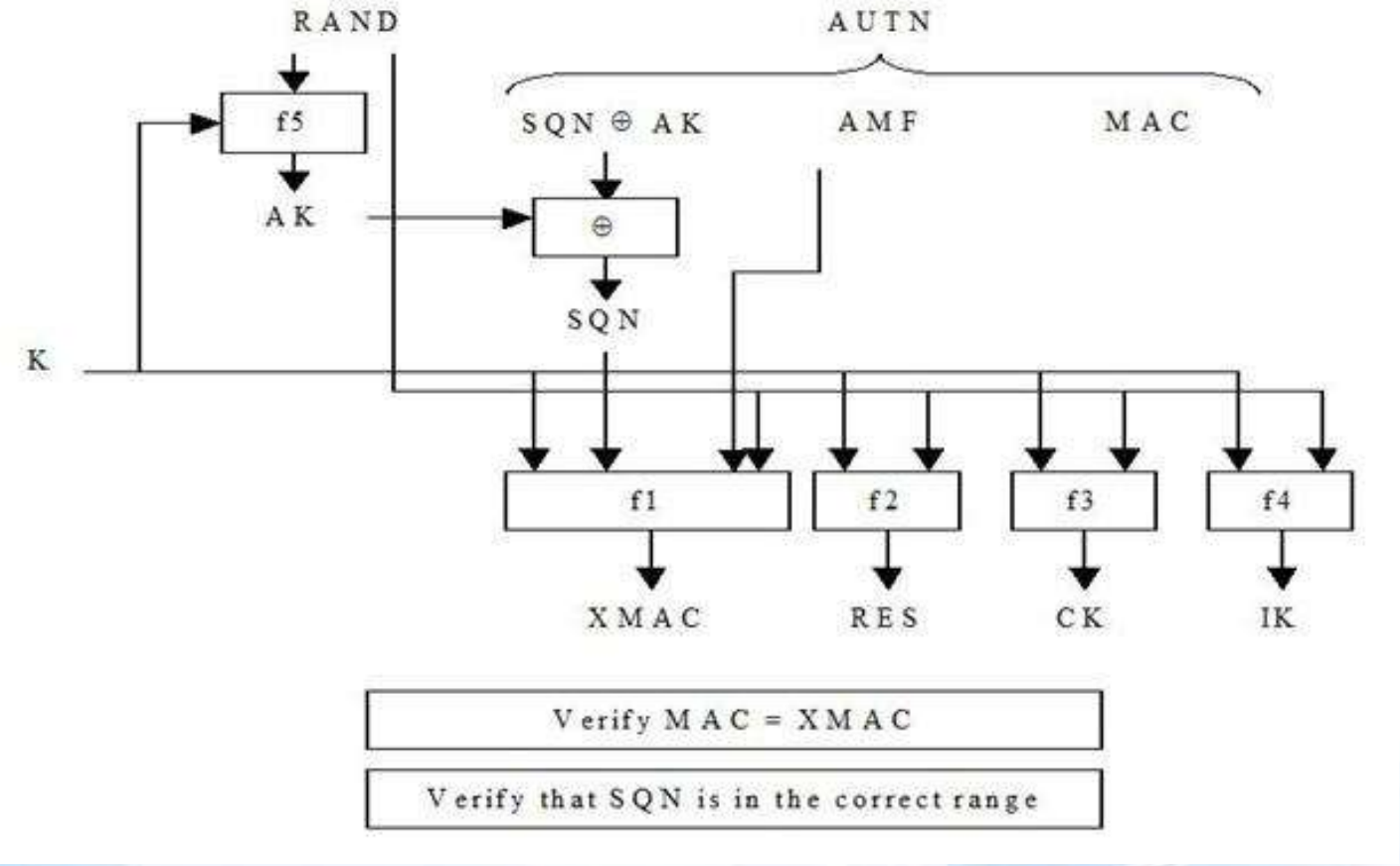


Рис. 7. Перетворення векторів на приймальній стороні (в USIM)

Безпека в мережах LTE

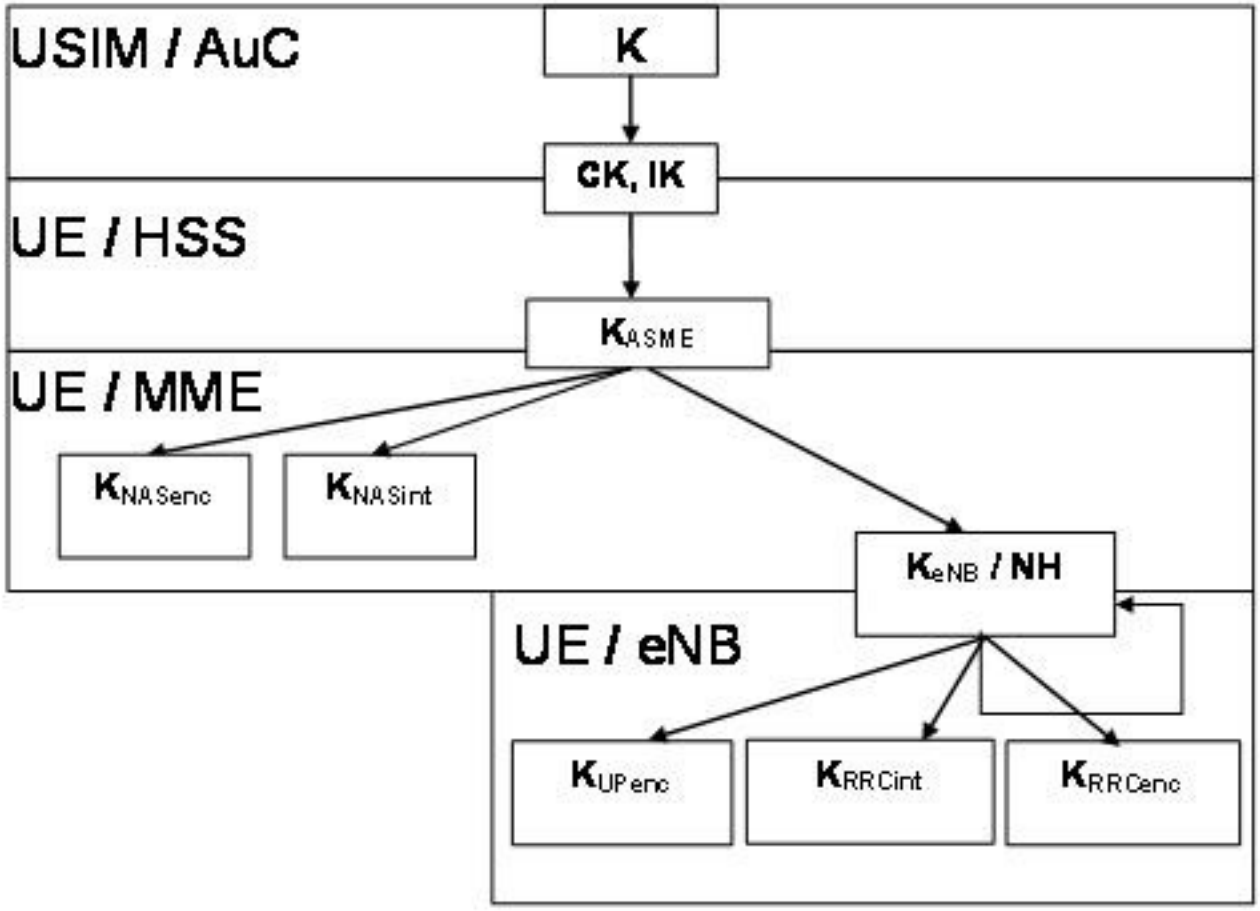


Рис. 8. Ієрархія ключів в LTE

Безпека в мережах LTE

Захист повідомлень протоколу RRC

Сигнальні повідомлення протоколу RRC (AS) також шифрують і забезпечують їх цілісність. Пакети трафіку тільки шифрують. Ці операції проводять в обслуговуючій eNB і UE. Схема отримання ключів шифрування і цілісності для AS і UP трафіку відрізняється від попереднього випадку тим, що вихідним параметром тут служить вторинний проміжний ключ KeNB (256 біт). Цей ключ генерують, також використовуючи KDF, де вхідними параметрами є: KASME, лічильник сигнальних повідомлень NAS вгору, колишнє значення KeNB, ідентифікатор стільники і номер частотного каналу в напрямку вгору. Отже, за будь-якої періодичної локалізації UE відбувається зміна KeNB.

Також KeNB змінюється і при хендовера; при цьому в алгоритмі генерації нового KeNB можна використовувати додатковий параметр NH (Next Hop), фактично лічильник числа базових станцій, по ланцюжку обслуговуючих абонента. Всі реалізовані процедури безпеки в мережі LTE продемонстровані на рис. 9.

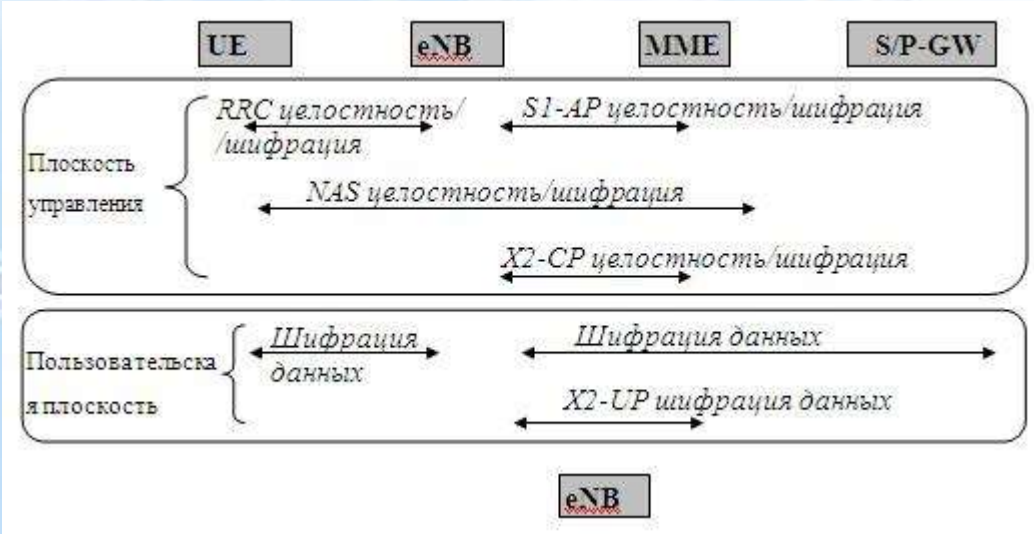


Рис. 9. Реалізовані процедури безпеки в мережі LTE

Безпека в мережах LTE

Алгоритм шифрування і дешифрування повідомлень представлений на рис. 9.

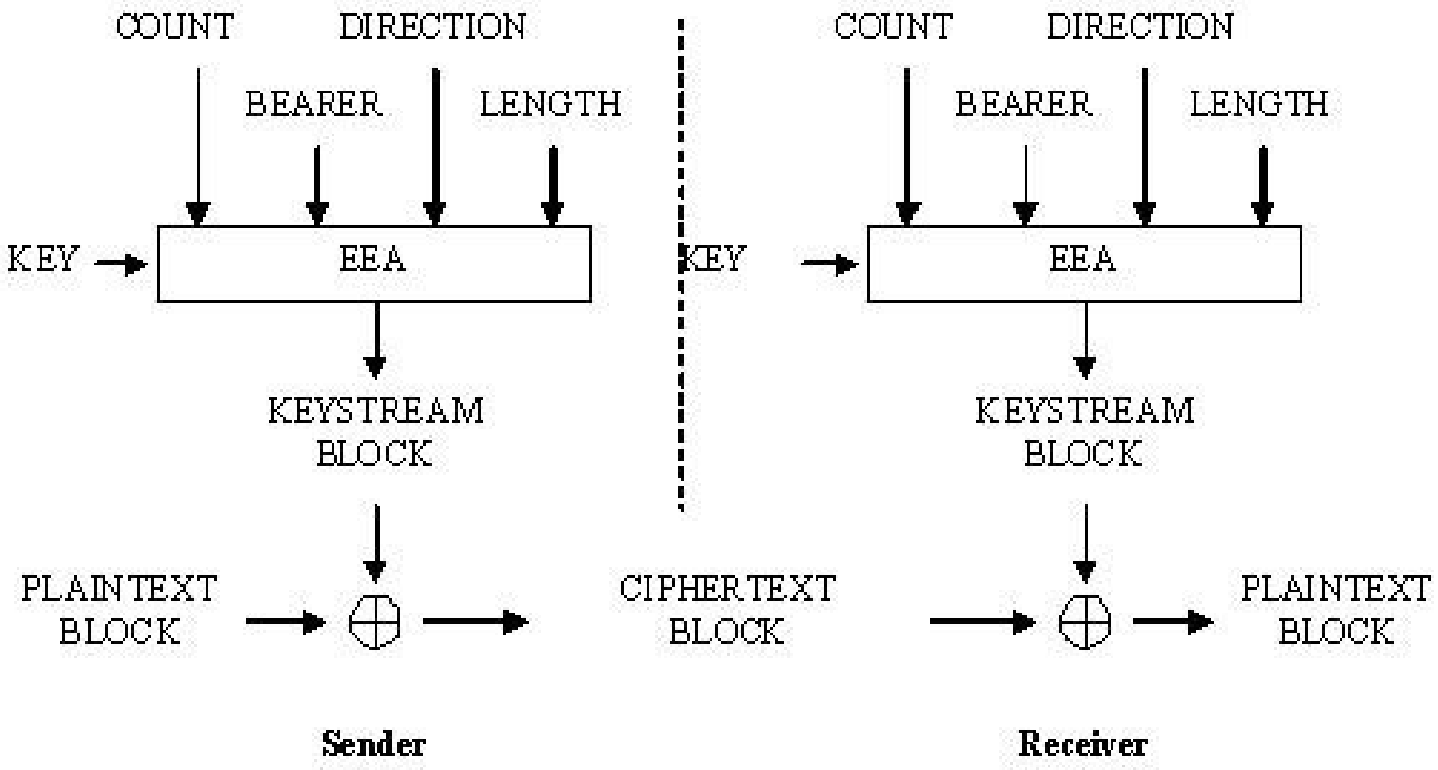


Рис. 10. Алгоритм шифрування/дешифрування в LTE

Безпека в мережах LTE

Вихідними параметрами в цьому алгоритмі є шифрує ключ KEY (128 біт), лічильник пакетів (блоків) COUNT (32 біта), ідентифікатор наскрізного каналу BEARER (5 біт), покажчик напрямку передачі DIRECTION (1 біт) і довжина шифрувального ключа LENGTH. Відповідно до обраного алгоритму шифрування EEA (EPS Encryption Algorithm) виробляється шифрувальне число KEYSTREAM BLOCK, яке при передачі складають по модулю два з зашифрованих вихідним текстом блоку PLAINTEXT BLOCK. При дешифрування на приймальному кінці повторно роблять цю ж операцію.

Процедура захисту цілісності повідомлення складається в генерації "хвоста" MAC (Message Authentication Code) (32 біта), що приєднується до переданому пакету. Алгоритм генерації MAC і перевірки цілісності отриманого пакета шляхом порівняння XMAC з MAC (вони повинні співпасти) відображено на рис. 11.

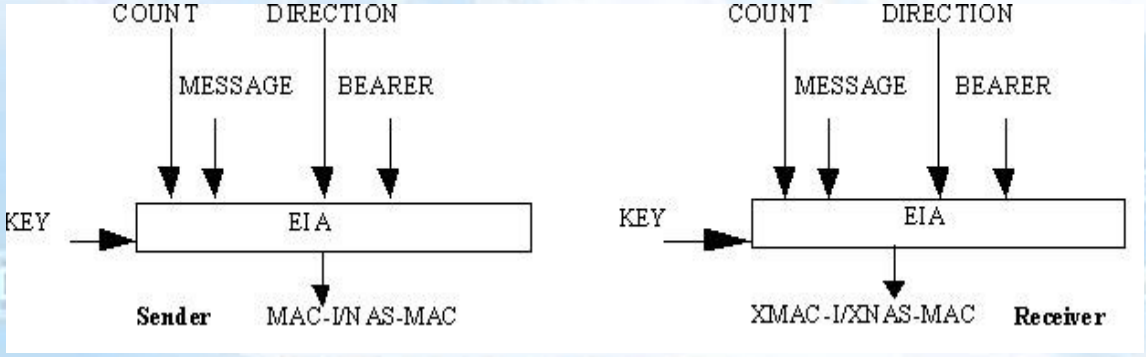


Рис. 11. Алгоритм перевірки цілісності в LTE

В алгоритмі EIA (EPS Integrity Algorithm) використаний ключ цілісності KEY (128 біт), лічильник повідомлень COUNT (32 біта), ідентифікатор наскрізного каналу BEARER (5 біт), покажчик напрямку передачі DIRECTION (1 біт) і саме повідомлення MESSAGE.