УДК 004.89

ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ПЕРЕДАЧІ ІНФОРМАЦІЇ В LTE

Варваринець С.В., Правило В.В.
Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: sofiya.ponzel@gmail.com, valeriy_pravilo@ukr.net

Providing of safety of information transfer in LTE

In this article we will consider the concept of safety of information, procedure of its providing transfer (procedure of mutual authentication and agreement about the keys, encipherings and providing of integrity of information). Also will consider the basic requirements to safety of information transfer in the networks of LTE.

Останнім часом абревіатура LTE (Long Term Evolution – довготривала еволюція) на слуху. У всьому світі оператори мобільного зв'язку тестують, вивчають і впроваджують новий стандарт, який обіцяє стати дійсно чимось глобальним [1].

Безпека мережі – перш за все захист мережі і всіх підключених до неї ресурсів від різних загроз. Безпека включає в себе як фізичні, так і програмні міри протидії, які необхідні для захисту інфраструктури мережі від несанкціонованого доступу, некоректної роботи, неправомірного доступу, модифікації та руйнування [4].

Тому під безпекою будемо розуміти захист від несанкціонованого доступу до мережі і забезпечення конфіденційності при передачі як інформації користувача, так і інформації управління.

Захист від несанкціонованого доступу реалізується за допомогою процедури аутентифікації, яка ініціюється MME (Mobility Management Entity, блок управління мобільністю) при надходженні запитів на реалізацію певних процедур, а саме: підключення (Attach), оновлення даних місцезнаходження (Location updating), реалізації послуги (Service), відновлення з'єднання (Connection Reestablishment). А конфіденційність в свою чергу забезпечується за рахунок закриття (шифрації) переданої інформації.

В основі реалізації безпеки лежить використання часових ідентифікаторів та різних ключів.

Перша процедура забезпечення безпеки мережі LTE – взаємна аутентифікація і угода про ключі (AKA – Authentication and Key Agreement).

Вихідні дані для реалізації процедури AKA:

- IMSI – Міжнародний ідентифікатор UE (SIM карти);
- K – Абонентський ключ; SNID (Serving Network Identity) – ідентифікатор обслуговуваної мережі, рівний PLMN ID даної мережі;
- Network Type – тип мережі 0: GSM/UMTS, 1 – LTE;
- IMSI і K зберігаються як в HSS, так і на SIM карті UE.

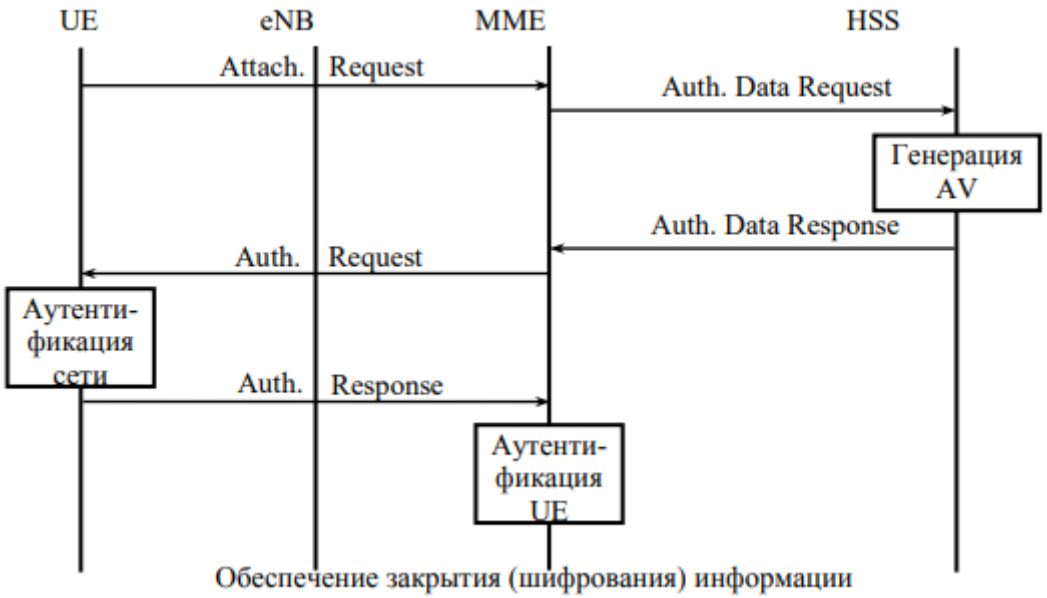

Рис. 1. Процес реалізації процедури АКА

Друга процедура забезпечення безпеки мереж LTE – це закриття (шифрування) і забезпечення цілісності інформації.

Шифрування та забезпечення цілісності інформації реалізується як і в площині управління, так і в площині користувача.

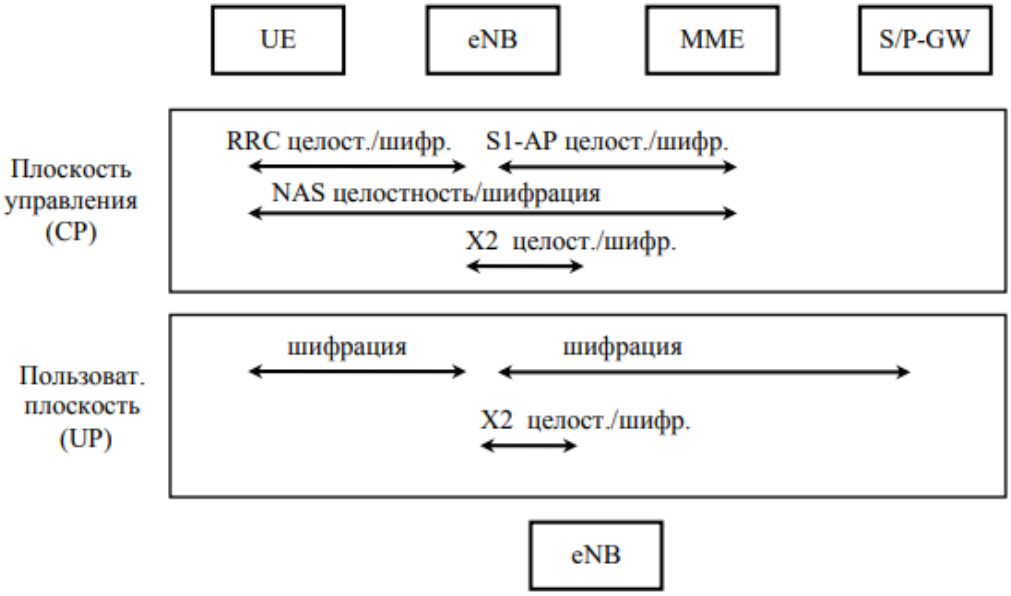

Рис. 2. Реалізація безпеки в площинах управління та користувача

А вже після успішного завершення процедури АКА MME, eNB і UE приступають до генерації ключів, які необхідні для шифрування і перевірки цілісності інформації [2].

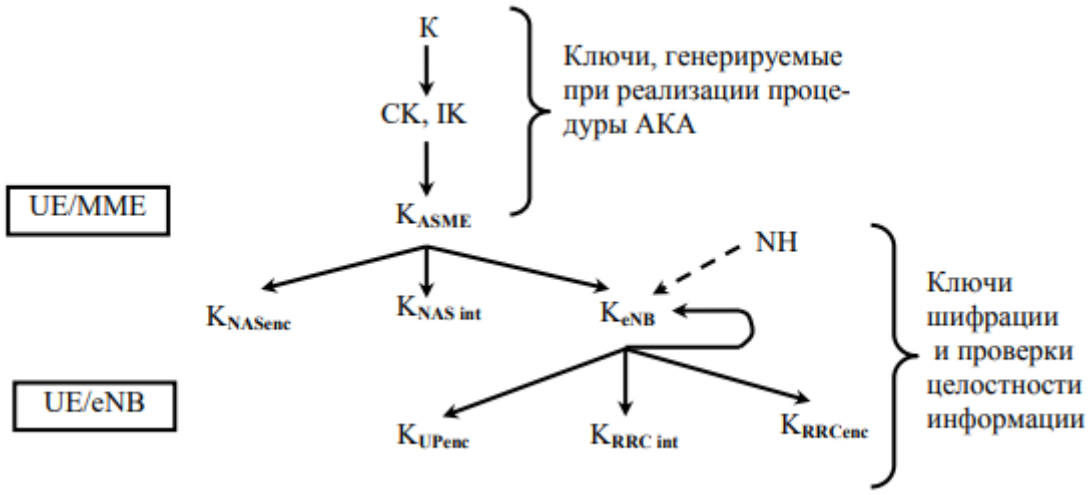

Рис. 3. Ієрархія ключів

Архітектура мереж LTE (Long Term Evolution) досить сильно відрізняється від схеми, яка використовується у вже існуючих мережах FOMA (3G). І саме ця відмінність породжує необхідність адаптувати та покращувати механізми забезпечення безпеки. Залишається найбільш важливою вимогою до механізмів безпеки гарантія хоча б того ж рівня безпеки, який на даний момент існує в мережах стандарту 3G. Наразі існує чотири основні вимоги до механізмів безпеки мережі LTE:

- Забезпечити (як мінімум) такий же рівень безпеки, як і в мережах стандарту 3G, не приносячи незручностей користувачам
- Забезпечити захист від Інтернет-атак
- Механізми безпеки для мереж LTE не повинні створювати завад для переходу зі стандарту 3G на стандарт LTE
- Забезпечити можливість подальшого використання програмно-апаратного мудулю USIM (Universal Subscriber Identity Module, універсальна сім-карта) [3].

Література

1. LTE: без пяти минут 4G [Електронний ресурс] - Режим доступу: https://itc.ua/articles/standart_lte_56151/
2. В. И. Данилов. Сети и стандарты мобильной связи
3. Защита данных в сетях LTE [Електронний ресурс] - Режим доступу: https://amonitoring.ru/article/lte_security/
4. Что такое безопасность сети [Електронний ресурс] - Режим доступу: https://www.hpe.com/ru/ru/what-is/network-security.html