УДК 621.396

Семенова О. О.
Стець Д. С.

МЕТОДИ ПІДВИЩЕННЯ ЗАХИЩЕНОСТІ СИСТЕМИ LTE

Вінницький національний технічний університет

Анотація
У роботі розглядаються основні методи захисту системи LTE, їх процеси та реалізація.
Ключові слова: LTE, CDMA, KASME.

Abstract
This paper considers the main methods of protecting the LTE system, their processes and implementation.
Keywords: LTE, CDMA, KASME.

Вступ

Мобільний зв'язок четвертого покоління передбачає використання цілого спектру технологій, які раніше розвивалися паралельно. Це технологія кодового поділу сигналів CDMA, технологія цифрового мобільного зв'язку GSM/GPRS, заснована на часовому поділі сигналу, і стандарт радіо-Ethernet під назвою WiMAX, який заснований на динамічному поділі ресурсу базової станції між абонентами. Всі вони внесли свій вклад в специфікацію LTE, також реалізованої в двох основних варіантах: технологія з дуплексним частотним поділом FDD (Frequency Division Duplex) і часовим поділом TDD (Time Division Duplex). Тепер всі проблеми пов'язані з протоколом IP. Якщо в 3G голосовий трафік і дані передавалися по двом різним мережам – по мережі з комутацією каналів (через MSC – Mobile Switching Centre) і по мережі даних (через вузли маршрутизації даних і обслуговування абонентів GGSN/SGSN), то в мережах 4G весь трафік проходить через єдину архітектуру EPC (Evolved Packet Core) по протоколу IP.

Основна частина

У системах LTE використовуються механізми безпеки для мереж 3G, які дозволяють забезпечити аутентифікацію абонентів, конфіденційність даних користувача, а також конфіденційність даних при їх передачі за протоколами U-Plane (призначені для користувача дані) і C-Plane (керуючі), а також комплексний захист протоколу C-Plane при його спільному використанні з іншими міжнародними стандартами обміну. Для аутентифікації застосовується процедура аутентифікації і узгодження ключів AKA (Authentication and Key Agreement). БС здійснюють зберігання ключа шифрування тільки на період сеансу зв'язку з мобільним терміналом. Алгоритми шифрування і забезпечення комплексної безпеки ґрунтуються на технології Snow 3G і стандарті AES. Планується використовувати ще два додаткових алгоритми, на випадок якщо один з алгоритмів буде зламаний, ті, що залишилися, повинні забезпечити безпеку мережі LTE. Нині для перевірки цілісності даних і шифрування алгоритми, які використовуються в LTE, мають 128-бітні ключі. Але й існує можливість використання 256-бітних ключів. Як алгоритми шифрування використовуються такі:

- 128-EEA1 заснований на алгоритмі Snow 3G. У точності повторює алгоритм UEA2, специфікований для мереж UMTS;
- 128-EEA2 заснований на алгоритмі AES.

Для перевірки цілісності даних, специфікації пропонують наступні алгоритми:

- 128-EIA1 заснований на алгоритмі Snow 3G. У точності повторює алгоритм UIA2, специфікований для мереж UMTS;
- 128-EIA2 заснований на алгоритмі AES.

Для закриття даних в мережах LTE використовується потокове шифрування методом накладення на відкриту інформацію псевдовипадкової послідовності за допомогою оператора «виключне або».

Так само, як і в мережах третього покоління, додаток USIM та центр аутентифікації (AuC) здійснює попередній розподіл ключів (ключа K). Коли механізм AKA ініціалізується для здійснення двосторонньої аутентифікації користувача і мережі, генерується ключ шифрування CK і ключ загального захисту, які потім передаються з програмного забезпечення USIM в мобільне обладнання (ME) і з центру аутентифікації в центр реєстрації (HSS).

Мобільне обладнання та центр реєстрації, використовуючи ключову пару (CK; IK) і ID використовуваної мережі виробляє ключ KASME. Встановлюючи 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 використовується в якості базової інформації ключової ієрархії.

На основі KASME виробляється ключ KNASenc, необхідний для шифрування даних протоколу NAS між мобільним пристроєм і пристроєм мобільного управління (MME), і ключ KNASint, необхідний для захисту цілісності. Коли мобільний пристрій підключається до мережі, MME генерує ключ KeNB і передає його базовим станціям. У свою чергу, з ключа KeNB виробляється ключ KUPenc, який використовується для шифрування даних користувача протоколу U-Plane, ключ KRRCenc для протоколу RRC (Radio Resource Control – протокол взаємодії між мобільними пристроями і базовими станціями) і ключ KRRCint, призначений для захисту цілісності [1].

Щоб звести до мінімуму схильність до атак, БС повинна забезпечувати безпечне середовище, яке гарантує виконання операцій: шифрування і розшифрування даних користувача, зберігання ключів. Тому заходи протидії розроблені спеціально для мінімізації шкоди, що завдається в разі крадіжки ключової інформації з БС:

- перевірка цілісності пристрою;
- взаємна аутентифікація БС оператора (видача сертифікатів);
- безпечні оновлення;
- механізм контролю доступу;
- синхронізація часу;
- фільтрація трафіку [2].

В разі проведення успішної атаки на БС зловмисник отримає контроль над ресурсами БС і доступ до всіх конфіденційних даних.

У LTE зберігаються і методи аутентифікації користувачів за прив’язкою до карти USIM, як в традиційному мобільному зв’язку: користувач може заблокувати доступ до телефону за PIN-кодом.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ / REFERENCES

1.Особенности обеспечения ИБ в сетях LTE [Електроний ресурс]. – Режим доступу до ресурсу: www/URL:http://www.rusnauka.com/12_KPSN_2014/Informatica/4_166376.doc.htm - 04.05.14.

2. Защита данных в LTE – системах [Електроний ресурс]. – Режим доступу до ресурсу: www/URL:http://ru.wikipedia.org/wiki/Архитектура_системы_безопасности_в_сетях_LTE - 05.05.14

Стець Дмитро Сергійович – студент групи АРЗ–18м, факультет інфокомунікацій, радіоелектроніки та наносистем, Вінницький національний технічний університет, м. Вінниця, e-mail: stetsdima@ukr.net.

Семенова Олена Олександрівна – канд. техн. наук, доцент кафедри телекомунікаційних систем та телебачення, Вінницький національний технічний університет, м. Вінниця.

Stets Dmytro S. – group ARZ–18m, The Faculty of Infocommunications, Radioelectronics and Nanosystems, Vinnytsia National Technical University, Vinnytsia, e-mail: stetsdima@ukr.net

Semenova Olena O. – Cand. Sc. (Eng), Associate professor at the Department of Telecommunication systems and television, Vinnytsia National Technical University, Vinnytsia, e-mail: semenovaolena@yahoo.com