УДК 621.382

# ЗАБЕЗПЕЧЕННЯ ЗАДАНИХ ПОКАЗНИКІВ БЕЗПЕКИ ПЕРЕДАЧІ ДАНИХ В 4G МЕРЕЖАХ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ

**Правило В.В.**
*Навчально-науковий інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна*
*E-mail: v.v.pravylo@ukr.net,*

## ENSURING THE SPECIFIED SECURITY INDICATORS OF DATA TRANSMISSION IN 4G NETWORKS OF SPECIAL PURPOSE

A set of measures is being considered to ensure a given level of data transmission security in 4G networks. Possible ways of unauthorized access by attackers to the network were analyzed. Directions for ensuring the security of special purpose 4G networks are proposed.

Сучасні військові операції вимагають високої мобільності, ефективності та безпеки. Для забезпечення цих вимог Збройні Сили України активно впроваджують нові технології, в тому числі 4G мережі.

4G мережі дозволяють військовим залишатися на зв'язку один з одним, навіть якщо вони знаходяться в русі. Вони також забезпечують більш високу швидкість передачі даних, що важливо для координації дій та управління технікою.

Для забезпечення заданого рівня безпеки передачі даних в 4G мережах необхідно використовувати комплекс заходів, включаючи шифрування, аутентифікацію та авторизацію.

Забезпечення заданого рівня безпеки передачі даних в 4G мережах передбачає використання наступних заходів:

- Застосування шифрування з відкритим ключем для аутентифікації та авторизації пристроїв. Це дозволяє забезпечити більш надійну ідентифікацію пристроїв і користувачів.
- Використання криптографії з симетричним ключем для захисту даних від несанкціонованого доступу. Це дозволяє забезпечити більш надійне шифрування даних.
- Використання технології SDN для управління мережею та виявлення атак. Це дозволяє швидко і ефективно виявляти та реагувати на атаки.

4G мережі використовують протоколи аутентифікації та авторизації, які можуть бути вразливими до атак. Це означає, що зловмисники можуть отримати доступ до мережі, використовуючи підроблені ідентифікатори. Вони не забезпечують достатнього захисту від атак на рівні даних. Це означає, що зловмисники можуть отримати доступ до даних, навіть якщо вони не зможуть отримати доступ до мережі. Для забезпечення заданого рівня безпеки передачі даних 4G мережах необхідно використовувати комплекс заходів, включаючи криптографію, аутентифікацію та авторизацію.

Криптографія використовується для захисту даних від несанкціонованого доступу. Криптографія використовує математичні алгоритми для перетворення даних в нечитабельний формат, який можна розшифрувати лише за допомогою правильного ключа.

Для шифрування даних, що передаються в 4G мережах, доцільно використовувати алгоритми шифрування ERCA та EPS (EEA).

ERCA – це алгоритм симетричного шифрування, який використовує ключі довжиною 256 біт. Він заснований на алгоритмі Rijndael, який є одним із найбезпечніших алгоритмів симетричного шифрування, доступних на сьогодні.

EPS (EEA) – це алгоритм асиметричного шифрування, який використовує ключі довжиною 128 біт. Він є алгоритмом відкритого ключа, що означає, що існують два ключі: приватний ключ і відкритий ключ. Приватний ключ використовується для шифрування даних, а відкритий ключ використовується для дешифрування даних.

В таблиці 1 представлені основні відмінності між алгоритмами ERCA і EPS.

Таблиця 1. Основні відмінності між алгоритмами ERCA і EPS.

| **Характеристика** | **ERCA** | **EPS** |
|---|---|---|
| **Тип шифрування** | Блочний | Пакетний |
| **Довжина ключа** | 256 біт | 128 біт |
| **Дані, які захищаються** | Голосові дзвінки, текстові повідомлення, дані передачі даних | Сигнали управління мережею, дані, які передаються між базовими станціями |

Аутентифікація використовується для перевірки ідентифікаторів пристроїв та користувачів. Аутентифікація допомагає гарантувати, що лише авторизовані пристрої та користувачі можуть отримати доступ до мережі.

Авторизація використовується для визначення того, що пристрої та користувачі можуть робити в мережі. Авторизація допомагає гарантувати, що лише авторизовані пристрої та користувачі можуть отримувати доступ до певних ресурсів або виконувати певні дії.

Поточна система безпеки 4G/LTE не визначає наскрізну архітектуру безпеки, яка може забезпечити безпечні сеанси для двох UE, підключених до двох різних мереж LTE.

Для вирішення цієї проблеми пропонується використовувати пакетний ключ, час життя якого зводиться до пакетного періоду.

Це дослідження спрямоване на вдосконалення локальної системи безпеки 4G/LTE, подальше розширення наскрізної системи безпеки для захисту даних користувачів між різнорідними мережами доступу LTE. Цей процес, за допомогою якого кожна пара UE всюди отримує свій KASME, подібний до процесу 4G/LTE (рис.1) .

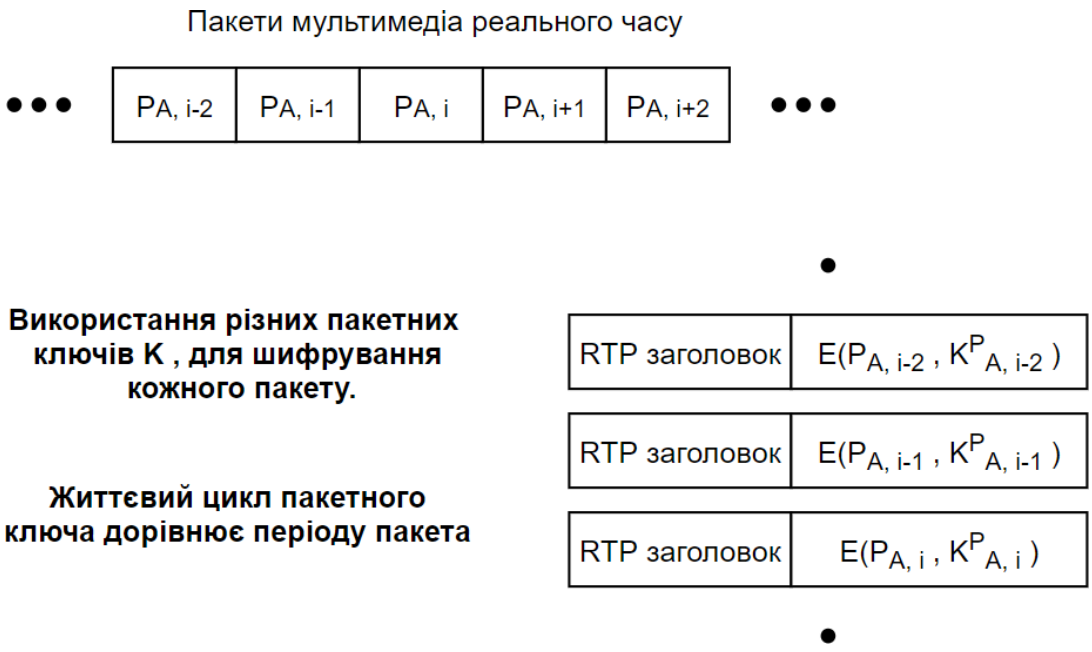


Рис. 1. Використання ключів пакетів для захисту потоку пакетів.

Аутентифікація в рамках забезпечення заданого рівня безпеки передачі даних в 4G мережах використовується для перевірки ідентифікаторів пристроїв та користувачів. Це допомагає гарантувати, що лише авторизовані пристрої та користувачі можуть отримати доступ до мережі.

Авторизація в рамках забезпечення заданого рівня безпеки передачі даних в 4G мережах використовується для визначення того, що пристрої та користувачі можуть робити в мережі. Це допомагає гарантувати, що лише авторизовані пристрої та користувачі можуть отримувати доступ до певних ресурсів або виконувати певні дії.

Таким чином пропонується забезпечення заданого рівня безпеки передачі даних в 4G мережах за допомогою схеми впровадження ключа пакетів. Дане рішення збільшує рівень безпеки при передачі, а також після перехоплення зловмисником потоку пакетів.

**Література**

1. 3GPP TR 25.814 Physical layer aspects for evolved Universal Terrestrial, Radio Access (UTRA), Release 7), V7.1.0, 2006. pp.64

2. G.-H. Tu, C.-Y. Li, C. Peng, Y. Li and S. Lu, "New security threats caused by IMS-based SMS service in 4G LTE networks".

3. J. Henrydoss and T. Boult, "Critical security review and study of DDoS attacks on LTE mobile network".

4. R. P. Jover, J. Lackey and A. Raghavan, "Enhancing the security of LTE networks against jamming attacks", EURASIP J. Inf. Secur.