УДК 007.681

**ЗАХИСТ ПЕРЕДАЧІ ІНФОРМАЦІЇ У МЕРЕЖАХ МОБІЛЬНОГО ЗВ’ЯЗКУ ТРЕТЬОГО ПОКОЛІННЯ**

Андрощук С.С.*,* студент групи ІБ-41*;* **Гриник Р.О.**, викладач

Львівський ДУ БЖД, Львів, Україна

Мережі третього покоління 3G працюють на частотах дециметрового діапазону (близько 2 ГГц), швидкість передавання даних становить понад 2 Мбіт/с. Такі мережі надають можливість організувати відеозв'язок, дивитись на мобільному телефоні фільми й телепрограмми та ін. В світі існує два стандарти 3G: UMTS (чи W-CDMA) та CDMA-2000. UMTS більш розповсюджений в основному в Європі, CDMA2000 – в Азії та США [1].

Термін 3G використовується для опису сервісів мобільного зв’язку стандартів наступного покоління, які забезпечуються більш високу якість звуку, а також високошвидкісний інтернет-звязок та мультимедійні сервіси. Мобільні мережі третього покоління (3G) відрізняються від мереж другого покоління (2G), таких як наприклад цифровий стандарт мобільного звязку GSM, зв'язок перехідного покоління (2.5G) GRPS набагато більшою швидкістю передавання даних, а також більш широким набором і високою якістю послуг, що надаються. Протоколи, що забезпечують безпеку передавання інформації в CDMA-IS-41 мережах, є одними з кращих в індустрії. Крім того сам CDMA стандарт за своєю побудовою робить перехоплення сигналу і його розшифрування дуже складним і дорогим завданням доступним, фактично, тільки державним спецслужбам. Криптографічні протоколи стандарту CDMA ґрунтуються на 64-бітному аутентифікаційному ключі (A-key) і серійному номері мобільного телефону - Electronic Serial Number (ESN). Для аутентифікації абонента при реєстрації мобільного телефону в мережі, а також подальшої генерації допоміжних підключень для забезпечення конфіденційності передавання голосових даних і кодованих повідомлень використовується випадкове двійкове число RANDSSD, що генерується аутентифікаційним центром реєстру власних абонентів (далі HLR/AC - Home Location Register/Authentification Center). A-key запрограмований в мобільному телефоні і зберігається в аутентифікаційному центрі мережі. CDMA використовує стандартизований алгоритм шифрування CAVE (Cellular Authentification and Voice Encryption) для генерації 128 бітного підключа SSD (Shared Secret Data). A-key, ESN і випадкове число що генерується мережею RANDSSD подаються на вхід CAVE генеруючого SSD. SSD складається з двох частин: SSD\_A, яку використовують для створення аутентифікаційного цифрового підпису, і SSD\_B, використовуваної при генерації ключів для шифрування голосових даних і службових повідомлень. SSD може бути переданий гостьовій мережі при роумінгу абонента для забезпечення локальної аутентифікації. Новий SSD може бути згенерований при поверненні абонента в домашню мережу або зміні гостьової мережі у роумінгу [2].

У стільникових стандартах третього покоління (3G) використовуються ще більш криптостійкі протоколи забезпечення безпеки системи, що включають використання 128-бітного секретного і аутентифікаційного ключів. У мережах третього покоління стандарту CDMA 2000 для хешування та перевірки достовірності використовується Secure Hashing Algorithm-1 (SHA-1), для шифрування повідомлень - Advanced Encryption Standard (AES Rijndael). Також для всіх наступних версій після CDMA 2000 Release C буде використовуватися AKA (Authentification and Key Agreement) протокол для аутентифікації і узгодження ключів. AKA протокол разом з алгоритмом Kasumi буде використовуватися і в WCDMA-MAP мережах для шифрування та перевірки достовірності повідомлень [3].

В даний час устаткування стандарту CDMA є найновішим і найдорожчим але в той же час найнадійнішим і найзахищенішим. Технологічні рішення і стійкі криптографічні протоколи, що знайшли застосування в цьому стандарті, забезпечують високий рівень конфіденційності мереж, побудованих на його основі. Підслухати з ефіру розмову можна, але вартість і складність обладнання здатного на таке значно вище ніж для інших стандартів.

**ЛІТЕРАТУРА**

* + - 1. “Specification of the 3GPP confidentiality and integrity algorithms; Document 2: KASUMI specification (Release 6)“. Technical specification.
      2. Convergence Technologies for 3G Networks. IP, UMTS, EGPRS and ATM. Jeffrey Bannister, Paul Mather, Sebastian Coope.
      3. Шерстнев А.Е. “Обзор технологии EDGE: основные принципы обеспечения безопасности”. Москва, 2005р.