УДК 621.396.662.072.078 **Сайко В.Г.**

АНАЛІЗ СПОСОБОВ ТА АЛГОРИТМІВ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ В МЕРЕЖАХ РУХОМОГО РАДІОЗВЯЗКУ НОВОГО ПОКОЛІННЯ

Здійснено оглядовий аналіз особливостей основних методів та засобів (протоколів) безпеки в мобільних мережах цифрового радіозв'язку нового покоління.

Ключові слова: автентифікація, шифрування, криптозахист.

Основною тенденцією розвитку телекомунікаційних технологій є прагнення до персоналізації шляхом забезпечення мобільності абонентів і реалізації комплексу інфокомунікаційних послуг. Ця тенденція обумовила динамічний розвиток мереж рухливого зв'язку в останні роки. Однак тенденції поширення сучасних стандартів і встаткування зв'язку стримуються цілим рядом факторів, серед яких виділяються необхідність значних капіталовкладень в інфраструктуру мережі й необхідність забезпечення інформаційної безпеки перспективної мережі зв'язку. [1-7]. Для ефективного впровадження в Україні мереж нового покоління розглядаються дві радіотехнології покоління 3G: WCDMA UMTS, розроблена в рамках проекту 3GPP, і cdma2000 (3GPP2).

Загальні алгоритми забезпечення безпеки. Основні алгоритми забезпечення безпеки в стільникових системах зв'язку (ССЗ) покоління 3G:

f_0 - функція генерування параметрів виклику (Random challenge generating function);

f_1 - функція автентифікації мережі (Network authentication function);

f_2 - функція автентифікації абонента (User challenge response authentication function);

f_3 - функція генерування ключа шифрування (Cipher key derivation function);

f_4 - функція генерування ключа перевірки цілісності (Integrity key derivation function);

f_5 - функція генерування ключа анонімності (Anonymity key derivation function). У ССЗ 3-го покоління використається схема взаємної аутентифікації МС і мережі (рис. 1). Після одержання від мобільної станції (МС) запиту обслуговування мережа ініціює процедуру автентифікації.

Для цього центр автентифікації мережі 3G генерує випадкове число RAND за допомогою функції f_0, після чого приступає до генерування параметра автентифікації AUTN, використовуючи функцію f_1. Крім названого числа RAND для цього використається попередньо розподілений довгостроковий секретний ключ K і номер переданої послідовності даних SQN (для ускладнення визначення місця розташування абонента він підсумується по модулі 2 із ключем анонімності (*anonymity key*) KA, генеровані функцією f_5). Потім "кортеж" параметрів RAND, SQN?KA й AUTN передається на МС по радіоефіру.

Процедура автентифікації МС мережею нагадує процедуру в мережах GSM. МС обчислює параметр RES за допомогою функції f_2, на вхід якої надходять секретний ключ K і прийняте число RAND. Параметр RES передається в мережу, що робить аналогічні обчислення, одержуючи RES? і порівнює його з RES. Якщо ті рівні, мережа "визнає" МС. Таким чином, у системах 3G передбачені процедури підтвердження дійсності як МС, так і самої мережі. Слід зазначити, що при розробці архітектури доступу в UMTS багато уваги приділено забезпеченню зворотної сумісності з GSM/GPRS. З погляду безпеки сумісність із системою попередником, що має набагато більше слабкий захист, украй небажана.

Для забезпечення криптографічного захисту каналу мережа й МС генерують ключі шифрування й перевірки цілісності кожний довжиною 128 біт з використанням відповідно функції f_3 і f_4 (вхідними параметрами є числа RAND і K), після чого обидві сторони здійснюють потокове шифрування переданої інформації. Цілісність повідомлень контролюється формуванням і перевіркою криптографічних контрольних сум.

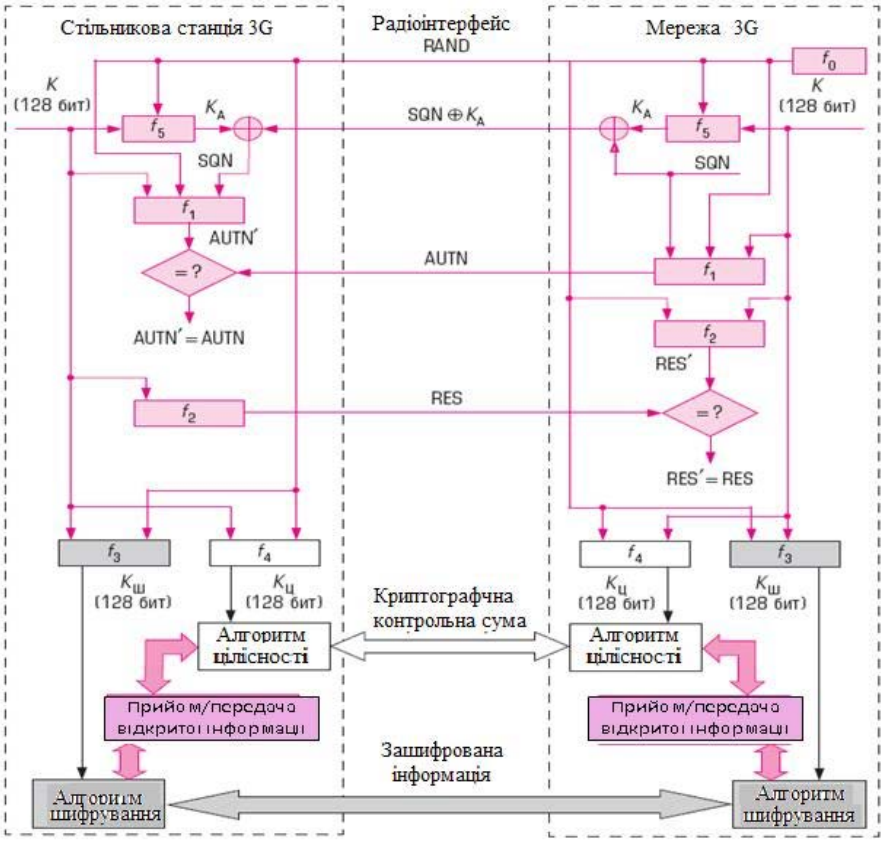

Рис. 1. Узагальнена схема ідентифікації та криптозахисту в системах 3G

Шифрування даних, що передаються через мережу. Процес шифрування даних (рис. 2) відбувається досить просто за винятком того, що шифрування відбувається на другому рівні й в пристрої присутні декілька передавальних інтерфейсів, кожен з яких використовує свій лічильник. Таким чином, при використанні цих лічильників, які, до речі, мають достатньо короткий період, маска шифрування, що видається блоком, зможе на них повторюватися, що приведе до повторення вхідних даних функції f_8 і, як наслідок, різкого зниження крипостійкості системи. Тому використовується додатковий лічильник, з довшим періодом, званий Hiperframe Number, що збільшується кожного разу, коли лічильник інтерфейсу переповнюється. На вхід COUNT-C подається конкатенація значень цих двох лічильників Сама функція f_8 визначена в стандарті і єдина. Її специфікація доступна як 3GPP TS 35.201 і вона базується на блоковому шифрі KASUMI, специфікація 3GPP TS 35.202).

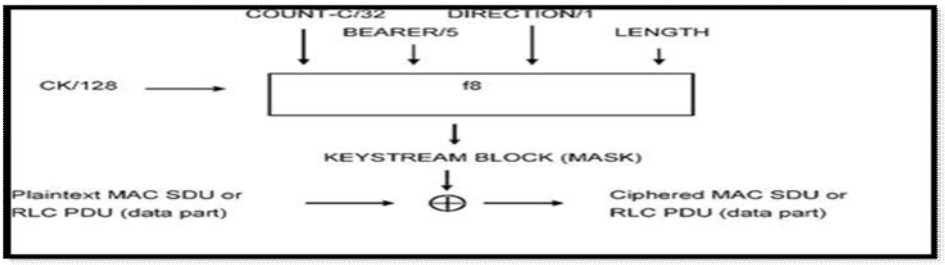

Рис. 2. Процес шифрування даних

Забезпечення цілісності даних. Організація забезпечення цілісності (рис. 3) і багато в чому аналогічна організації шифрування: зашифроване повідомлення пропускається через f_9. COUNT-I має те ж значення, що і лічильник для процесу шифрування. Новим є тільки параметр FRESH. Розглянемо наступну ситуацію: на початку з'єднання USIM повідомляє про

своє HFN обслуговуючої мережі, і якщо ключ не встиг змінитися (не відбувалося нової процедури автентифікації), хакер може повідомити станції раніше перехоплену інформацію з дуже маленьким HFN. Тому на кожному з'єднанні обслуговуюча мережа призначає випадковий параметр FRESH. Може виникнути сумнів: чому тут не враховується BEARER, ідентифікатор інтерфейсу? Адже так з'явиться можливість повторити записане повідомлення на іншому інтерфейсі? Відповідь проста. BEARER вже зашифрований в самому повідомленні, і для іншого інтерфейсу дані вже не вважатимуться вірними.

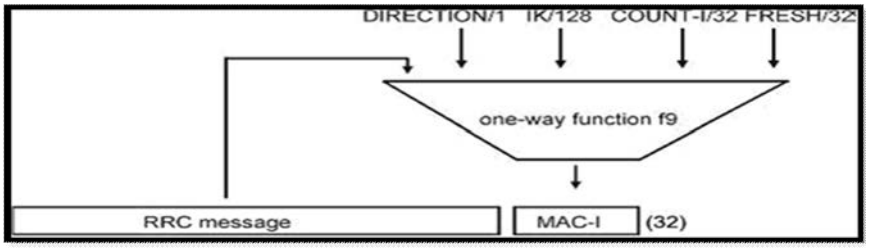

Рис. 3. Організація забезпечення цілісності даних

«Законне» перехоплення. Одною з основних проблем при розробці механізмів забезпечення безпеки була незаконність її забезпечення в деяких країнах. З цією ж проблемою свого часу зіткнулися й мережі 2G, але тоді за мету не ставилося зробити універсальний всесвітній стандарт мереж мобільного зв'язку. Тому в стандарті UMTS також присутні механізми перехоплення з'єднань, а також фільтрації потрібного від непотрібного вмісту за допомогою спеціального устаткування. Точність позиціювання досягається за допомогою ще однієї можливості мереж UMTS – пристрою «Positioning System»[3].

Алгоритми шифрування в UMTS. Перед початком обміну інформацією, кожна сторона повинна переконатися в тому, що спілкується саме з тим, хто їй потрібен, а не зі зловмисником, що імітує співрозмовника з метою перехоплення цієї інформації (рис. 4). У випадку каналу радіозв'язку мобільних мереж такими сторонами є Абонент (User Equipment кінцевого користувача) і Мережа (передаточних вузол провайдера мобільного зв'язку). Головним помітним нововведенням є алгоритм автентифікації та узгодження ключів, наведений коротко нижче [7]. Автентифікаційні центри (AuC) і USIM зберігають копії основного ключа абонента, за допомогою якого відбувається спілкування абонента з мережею. За запитом мережі AuC створює таблицю з n (зазвичай $n = 5$) п’яти компонентних автентифікаційних векторів. Компонентами даних векторів є:

- випадкове число RAND
- очікуваний відповідь XRES
- ключ шифрування CK
- ключ цілісності IK
- маркер автентифікації AUTN, причому останні 4 компоненти виходять з RAND і K і порядкового номера вектора SQN.

Автентифікація та вироблення ключа. Обслуговуюча мережа (а конкретно - її VLR) вибирає наступний (k-тий) автентифікаційний вектор з упорядкованої таблиці і посилає RAND (k) і AUTN (k) користувачеві. USIM перевіряє, чи вироблений AUTN (k) є дійсний маркер автентифікації і, якщо так, генерує і посилає відповідь RES (k).

Для передачі даних у стандарті UMTS були визначені функції шифрування f_8 і f_9, які відповідають відповідно за шифрування і цілісність. З урахуванням специфіки каналу, що використовується, та переданих даних, а також технологічних можливостей з виробництва обслуговуючих схем, для f_8 і f_9 були визначені наступні вимоги:

- f_8 повинна являти собою поточний шифр;
- f_9 повинна бути функцією множення / підсумовування;

- обидві функції повинні бути реалізовані на невеликих чіпах з низьким енергоспоживанням;
- не повинно бути обмежень щодо заміни цих функцій на терміналах (в абонентському обладнанні).

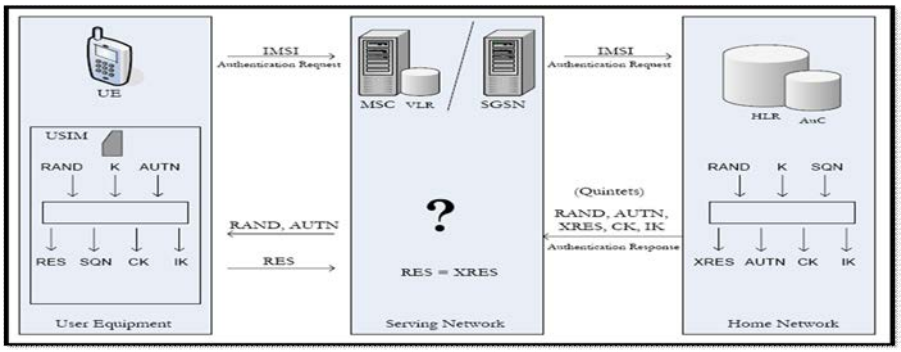

Рис. 4. Автентифікація абонента мережі UMTS

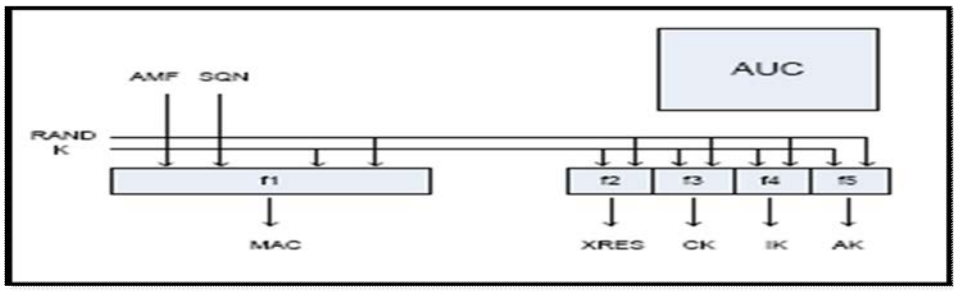

Рис. 5. Автентифікаційні вектор передачі даних.

Алгоритм перевірка цілісності в UMTS. Функція f_9, являє собою послідовну функцію множення-накопичення з KASUMI в ядрі. До кожного повідомлення, яке відсилається, прикріпляється MAC-I (32-х бітний псевдовипадковий рядок - вихід f_9), і такій ж рядок обчислюється приймаючою стороною. Справа в тому, що вихід функції f_9 практично непередбачуваним чином залежить від вхідних параметрів, так що тільки правильне поєднання IK і лічильника гарантує достовірність отриманого повідомлення.

ЛІТЕРАТУРА

1. Мерит М.. Безопасность беспроводных сетей / М. Мерит, Д. Полино. - М.: Компания "АйТи" ДМК Пресс, 2004 - 288 с.

2. Гепко И.А. Возможности обеспечения информационной безопасности в стандартах сотовой связи 2-го и 3-го поколения: Сравнительный анализ. / И.А. Гепко, А.А. Москаленко, А.В. Бондаренко // Зв'язок - 2006 - № 5. - С. 29-33.

3. Security in 3G Networks [Електронний ресурс]: Режим доступу до ресурсу: http://ws3.re.mipt.ru/mediawiki/index.php/Security_in_3G_Networks.

4. Крупнов А.Е. Защита нового поколения. Информационная безопасность в сетях 3G Електронний журнал] / А.Е. Крупнов, А.И. Скородумов. - Режим доступу до журналу: http://www.iksnavigator.ru/vision/457145.html.

5. [Електронний ресурс]:www.3gpp.org.

6. [Електронний ресурс]:http://www.technofresh.ru/technology/appearance/3g.htm.

7. Алгоритмы шифрования в се-тях_UMTS [Електронний ресурс]: Режим доступу до ресурсу: http://ws3.re.mipt.ru/mediawiki/index.php/Алгоритмы_шифрования_в_се-тях_UMTS.

Надійшла: 18.10.2012р.

Рецензент: д.т.н., проф. Дудикевич В.Б.