УДК 004

Пархуць Ю.Л.
(НУ «Львівська політехніка»)

ОСНОВНІ АСПЕКТИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В МЕРЕЖАХ МОБІЛЬНОГО ЗВ'ЯЗКУ СТАНДАРТУ GSM

Незважаючи на те, що технічний розвиток засобів передачі інформації на сучасному етапі найбільш сконцентрований саме на сфері мобільного зв'язку, проблема забезпечення захисту даних в стільникових мережах є невирішеною і водночас достатньо актуальною. Оскільки на території нашої держави найбільш поширеними є мобільні мережі GSM (Global System for Mobile Communications) стандарту, то розгляд питання інформаційної безпеки варто почати саме з даної технології зв'язку. Даний стандарт офіційно був затверджений у 1990р. як глобальний цифровий стандарт мобільного зв'язку з часовим розділенням каналів TDMA і використанням алгоритмів шифрування інформації з відкритим ключем.

Детальний опис стандарту GSM розкритий в працях Громакова Ю.А., Северина А.В., Шевцова В.А., Соколова А.В. Ми ж зосередимо основну увагу на аспектах безпосередньо пов'язаних з інформаційною безпекою. Найближчим до користувача елементом мережі, що його ідентифікує є мобільний пристрій, який має свій унікальний серійний номер IMEI (International Mobile Equipment Identity – міжнародний ідентифікатор мобільного пристрою) та SIM карта (Subscriber Identity Module – модуль ідентифікації абонента), яка в свою чергу володіє ідентифікаційним номером IMSI (International Mobile Subscriber Identity – міжнародний ідентифікаційний номер абонента) [2, с.10-11].

Основним мозковим елементом мережі є підсистема мережі та комутації NSS (Network and Switching Subsystem), основна роль в якому відводиться центру комутації мобільних послуг MSC (Mobile services Switching Center). Окрім виконання функцій комутатора, центр комутації виконує процедури безпеки, які застосовуються для управління доступами до радіоканалів. Важливу роль з точки зору інформаційної безпеки грають реєстри HLR (Home Location Register – реєстр власних абонентів) і VLR (Visitor Location Register - реєстр переміщень абонентів) [2, с.8-10].

HLR містить базу даних про всіх абонентів своєї мережі, а саме:

- ✓ IMSI абонента;
- ✓ телефонний номер абонента (MSISDN - Mobile Subscriber ISDN);
- ✓ ключ ідентифікації абонента (Ki);
- ✓ індекс закритої групи користувачів і код її блокування;
- ✓ ідентифікація номера абонента, що додзвонюється;
- ✓ набір паролів, що використовуються абонентом;
- ✓ клас пріоритетного доступу та ін.

VLR зберігає інформацію про абонентів, які знаходяться в межах його території (тут обслуговуються як свої так і користувачі інших мереж). Відповідно VLR переважно є декілька, кожен з яких контролює свою частину мережі і містить наступну інформацію:

- ✓ тимчасовий номер абонента (TMSI);
- ✓ ідентифікатор області знаходження абонента (LAI);
- ✓ дані про використання основних служб;
- ✓ номер зони при естафетній передачі;
- ✓ параметри ідентифікації та шифрування;

В HLR для кожного абонента постійно присутнє посилання на відповідний VLR, який на даний момент працює з цим абонентом (причому VLR може належати чужій мережі) [1, с.146-147]. Отже в реєстрах HLR і VLR знаходиться значна частина таємної інформації, що використовується при ідентифікації та аутентифікації абонента, шифрування даних, які він передає, інформація про місце знаходження абонента і т.д.

Наступний, важливий з точки зору захисту елемент мережі – це центр авторизації AuC (Authentication Center), який виконує функції по аутентифікації абонента. Даний центр складається із декількох блоків, які формують ключі та алгоритми аутентифікації. AuC перевіряє права абонента і приймає рішення про надання йому доступу до мережі, вибирає параметри процесів аутентифікації і визначає ключі шифрування абонентських станцій. Робота AuC базується на основі даних реєстру ідентифікації обладнання EIR (Equipment Identity Register), що містить білий (санкціонований), сірий (проблемний) та чорний (заборонений) переліки номерів IMEI.

Основним виконавчим елементом мережі є підсистема базових станції BSS (Base Station Subsystem), що здійснює управління розподіленням радіоканалів, контролює з'єднання, регулює їх послідовність, забезпечує режим роботи з стрибкозмінною частотою, забезпечує модуляцію та демодуляцію сигналів, кодування та декодування повідомлень, адаптацію швидкості передачі для мовного сигналу, даних і виклику, визначає послідовність передачі повідомлень персонального виклику. Управління і координація роботи мережі відбувається за допомогою підсистеми управління та підтримки OSS (Operating and Support Subsystem), яка складається з різного роду служб і систем, що контролюють роботу мережі і трафік.

Процеси ідентифікації та аутентифікації абонента відбуваються за наступним принципом. При кожному включенні мобільного телефону, мережа формує запит на ідентифікаційний номер SIM карти і телефон передає IMSI абонента. Даний номер починається із коду країни, далі йдуть цифри, які визначають домашню мережу абонента, і слідом – унікальний номер користувача. VLR мережі, в межах дії якого знаходиться абонент, отримавши номер IMSI, визначає домашню мережу користувача і зв'язується з її HLR для отримання всієї необхідної інформації про даного абонента. А HLR, в свою чергу, записує в себе посилання на відповідний VLR, щоб при необхідності можна було взнати де шукати абонента. Крім ідентифікаційного номеру IMSI кожна SIM карточка містить ще й свій унікальний ключ аутентифікації Ki та алгоритм аутентифікації A3. При реєстрації абонента, AuC домашньої мережі генерує 128-бітне випадкове число RAND і пересилає його на телефон користувача. В SIM карті використовуючи ключ Ki та число RAND за алгоритмом A3 відбувається обчислення 32-бітної відповіді SRES (Signed RESult). Точно такі ж обчислення відбуваються і в центрі аутентифікації мережі AuC за допомогою вибраного з HLR ключа Ki користувача. Телефон надсилає свій результат обчислення SRES, який порівнюється із відповідним значенням, обчисленим в AuC, і за отриманим результатом порівняння приймається рішення про авторизацію абонента [1, с.142-144].

Механізм шифрування даних використовує вже згадувані вище випадкове число RAND і ключ авторизації абонента Ki, які за алгоритмом A8, що знаходиться в SIM карточці, визначають 64-бітний ключ шифрування Kc. Даний ключ використовується для шифрування і розшифрування при передачі даних між мобільною станцією та базовою станцією. Додатковий рівень секретності забезпечується періодичною зміною ключа. Kc разом із номером TDMA фрейму за алгоритмом A5 визначають 114-бітну послідовність, яка в подальшому накладається за допомогою операції XOR на два 57-бітних блоки пакету даних.

Алгоритм A5 виконує шифрування потоку даних трьох синхронізованих лінійних регістрів із зворотнім зв'язком (LFSR) степенів 19, 22 і 23. В цих регістрах сигнал зворотного зв'язку формується лінійною логічною схемою, відбувається перетворення згортки зовнішньої вхідної послідовності з послідовністю комбінаційних коефіцієнтів. Якщо зобразити зовнішній вхідний сигнал у вигляді многочлена, в якому степені незалежної змінної означають часову затримку, а комбінаційні коефіцієнти аналогічним чином зобразити в вигляді другого многочлена, то регістр із лінійним зворотнім зв'язком можна розглядати як пристрій ділення першого многочлена на другий. При відсутності зовнішньої вхідної послідовності регістр може сам по собі використовуватися для формування m -

послідовностей (періодична послідовність максимальної довжини, яка використовується в якості псевдовипадкової послідовності). Максимальна довжина послідовності рівна 2n-1, де n – степінь реєстру зсуву. Принцип формування m - послідовності регістром LFSR наведений на рис.2.

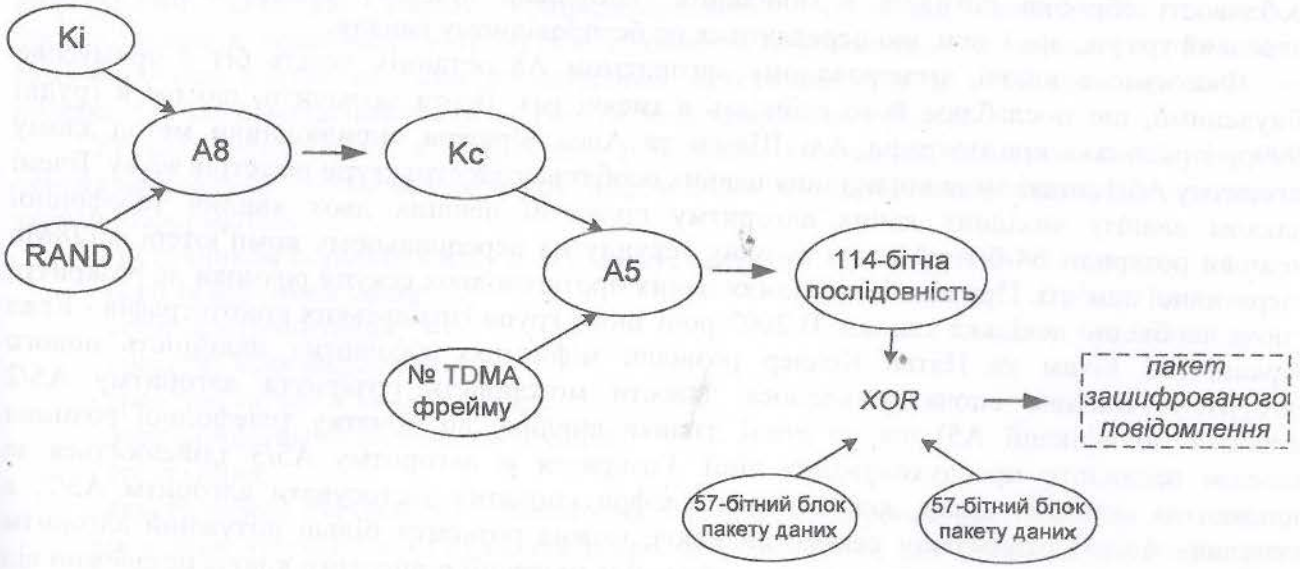

Рис.1. Принцип шифрування даних абонента

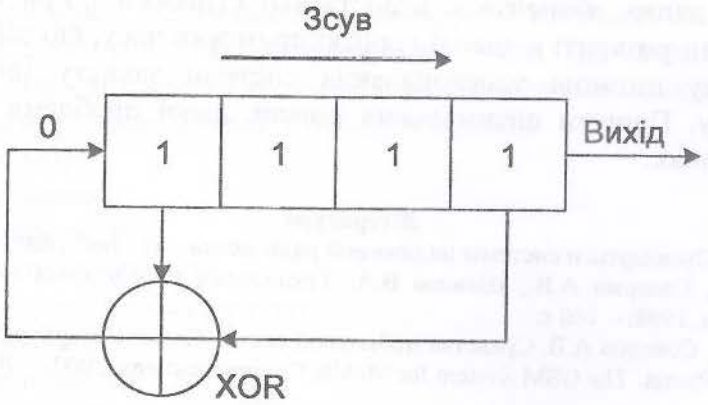

Рис.2. Принцип формування m - послідовності лінійним регістром із зворотнім зв'язком

Такий регістр генерує періодичні m – послідовності, які враховують наступні стани: 1111, 0111, 1011, 0101, 1010, 1101, 0110, 0011, 1001, 0100, 0010, 0001, 1000, 1100, 1110. Для цього зовнішня вхідна послідовність LFSR повинна відповідати примітивному многочлену степеня n по модулю 2. Управління синхронізацією являє собою порогову функцію від середніх бітів для кожного із трьох регістрів зсуву. Сума степенів всіх трьох регістрів рівна 64 і 64–бітний ключ використовується для ініціалізації вмісту регістрів зсуву. Робота таких трьох регістрів і лежить в основі алгоритму шифрування потоків даних А5. Стверджується, що алгоритм А5 має ефективну довжину ключа – 40 біт. На ранніх етапах функціонували два варіанти алгоритму А5, а саме А5/1 та А5/2. Перший алгоритм, більш досконалий, застосовувався переважно в країнах Західної Європи. Слабша версія – А5/2 частіше використовувалася в країнах Центральної та Східної Європи. В 2002р. Асоціація GSM затвердила новий алгоритм шифрування – А5/3, який був розроблений спільними зусиллями

комітету безпеки Асоціації GSM, організацією 3GPP і комітетом з алгоритмів безпеки Європейського інституту телекомунікаційних стандартів ETSI. Цей алгоритм був призначений для використання як в звичайних 2G мережах так і в модернізованих 2,5G (GPRS) та 3G (HDCSD і EDGE). Алгоритм A5/3 реалізований на апаратному рівні і враховує особливості обробки сигналів в мобільних телефонах, причому шифрується не лише голосовий трафік, але і дані, що передаються по безпровідному каналу.

Фактично в ключі, згенерованому алгоритмом A8 останніх десять біт є примусово обнуленими, що послаблює його стійкість в тисячі раз. Варта зазначити, що ще в грудні 1999р. ізраїльські криптографи Аді Шамір та Алек Бірюков оприлюднили метод злому алгоритму A5/1, шляхом використання певних особливостей структури регістрів зсуву. Вчені шляхом аналізу вихідних даних алгоритму протягом перших двох хвилин телефонної розмови розкрили 64-бітний ключ за одну секунду на персональному комп'ютері з 128Mb оперативної пам'яті. При аналізі вихідних даних протягом двох секунд розмови на розкриття ключа необхідно декілька хвилин. В 2003 році знову група ізраїльських криптографів - Елад Баркан, Елі Біхам та Натан Келлер розвіяли міфи про абсолютну надійність нового алгоритму. Вченим спочатку вдалося довести можливість розкриття алгоритму A5/2 (слабшої модифікації A5) ще на етапі дзвінка виклику до початку телефонної розмови шляхом пасивного прослуховування лінії. Розкриття ж алгоритму A5/3 здійснюється за допомогою активної атаки, яка змушує телефон спочатку застосувати алгоритм A5/2, а зламавши його і отримавши секретний ключ, можна розкрити більш потужний алгоритм A5/3, адже протокол передбачає однаковий процес генерації сеансового ключа незалежно від вибраного алгоритму шифрування.

Отже результати досліджень відомих криптографів показали що існуючі алгоритми шифрування потоку даних абонента є недостатньо стійкими і при наявності необхідної апаратури можуть бути розкриті в доволі короткі проміжки часу, що зайвий раз підтверджує необхідність розгляду питання удосконалення системи захисту інформації в мережах стільникового зв'язку. Пошуки оптимальних рішень даної проблеми будуть розглянуті в подальших дослідженнях.

Література

1. Громаков Ю.А. Стандарты и системы подвижной радиосвязи.- М.:ЭкоТрендз Ко, 1998. – 240 с.

2. Громаков Ю.А., Северин А.В., Шевцов В.А. Технологии определения местоположения в GSM и UMTS.- М.:ЭкоТрендз Ко, 1998. – 140 с.

3. Андрианов В.И., Соколов А.В. Средства мобильной связи.- Санкт-Петербург:БХВ, 2001. – 256 с.

4. M. Mouly, M.B. Pautet. The GSM System for Mobile Communications. 2002. – 702 p.

В статті розглянуто систему захисту даних абонента в мережах мобільного зв'язку, наведено детальний огляд структурних елементів GSM мережі, що пов'язані із інформаційною безпекою абонента, проаналізовані принципи ідентифікації та аутентифікації користувача і шифрування його даних,визначено доцільність пошуку рішень по підвищенню надійності системи захисту інформації абонента.

Рецензент:д.т.н. Кунах Н.І.
Надійшла 09.12.2010
Після доробки 27.12.2010