УДК 621.396:65.012.8(083.94)

ЗАХИСТ ІНФОРМАЦІЙНИХ ПОТОКІВ У МОБІЛЬНИХ МЕРЕЖАХ СТАНДАРТУ CDMA2000

А. Б. Петренко, канд. техн. наук, доц.; ***А. Б. Єлізаров***, канд. техн. наук, доц.;
С. А. Шматок, д-р техн. наук, проф.; ***В. О. Ващук***

*Національний авіаційний університет

**Національний технічний університет України «КПІ»

e-mail: vashchook@gmail.com

Досліджено системи безпеки даних, що забезпечують конфіденційність зв'язку стандарту мобільного зв'язку CDMA 2000, а саме алгоритм автентифікації, його основні принципи функціонування та можливі атаки для несанкціонованого доступу до мережі.

Ключові слова: ключ автентифікації, мобільний алгоритм автентифікації та шифрування голосу, CDMA, секретний набір даних, автентифікація, безпека зв'язку, мобільна мережа, система автентифікації.

In this paper is investigation of data security fo ensure the confidentiality of mobile communication standard CDMA2000. Namely the authentication algorithm, it's basic function principles and possible attacks for unauthorized network access.

Keywords: authentication key, Cellular Authentification and Voice Encryption, CDMA, Shared Secret Data, authentication, secure communications, mobile network, authentication system.

Вступ

Останнім часом мобільні мережі досить швидко розвиваються. В мобільних мережах стандарту CDMA (*Code Division Multiple Access*) кожний канал системи повністю використовує весь виділений частотно-часовий ресурс, оскільки радіоканали систем CDMA перекриваються як часом, так і частотою. Розділення сигналів окремих каналів здійснюється за рахунок того, що кожний канал має свою «піднесучу» — адресну кодову послідовність, сформовану за законом однієї з 64 функцій Уолша. Суттєвою перевагою зв'язку з шумоподібними сигналами є захищеність каналу від перехоплення, завад та підслуховування. Стандарт був прийнятий у 1993 р., як внутрішній стандарт цифрового зв'язку та отримав назву IS-95 (*Interim Standard*), працював у діапазоні 800МГц. Стандарт передбачає сумісність з існуючими (у 1990-х роках) мережами мобільного зв'язку стандарту AMPS (*Advanced Mobile Phone Service*). Для систем, працюючих за стандартом IS-95, виділена та сама смуга частот, що й для AMPS, таким чином CDMA працює «поверх» існуючої AMPS [1].

На мобільному ринку України нині послуги рухомого мобільного зв'язку CDMA2000 надають три оператори: МТС (лише передача даних), Інтертелеком та PEOPLEnet. Послугами даного типу зв'язку користується понад 2,3 млн громадян [2]. Оскільки при переході від одного покоління мереж до наступного, нове покоління накладається на попереднє, використовуючи обладнання попереднього з не значними змінами. Отже, варто розглянути функціонування стандарту CDMA2000, особливу увагу приділити системам, методам захисту абонентських даних при передачі їх у каналах зв'язку, автентифікацію та можливі вразливості.

Аналіз досліджень

Аналізуючи функціонування мобільних мереж стандарту CDMA2000, необхідно звернути особливу увагу на методи, способи та засоби захисту CDMA.

Алгоритм автентифікації є однією зі складових надійності будь-якої мережі, в котрій передаються дані різного типу, особливо якщо це мобільні мережі.

Автентифікацію та подальший захист даних забезпечують:

– функція CAVE (*Cellular Authentification and Voice Encryption*), функція перемішування, що використовується в протоколах автентифікації запит/відповідь і для генерації ключів;

– операція XOR — накладає повторювальну маску на голосові дані для забезпечення безпеки їх передачі;

– шифр ORYX — потоковий шифр, призначений для використання в послугах бездротового доступу до даних;

– шифр CMEA (*Control Message Encryption Algorithm*) — простий блоковий шифр, використовується для шифрування службових повідомлень.

Постановка завдання

Мета роботи — аналіз стандартів, прийнятих та запроваджених для забезпечення функціонування систем захисту інформаційних потоків мобільної мережі стандарту CDMA. Особливо тих, що стосуються алгоритмів та систем автентифікації користувачів у мережі оператора мобільного зв'язку.

Поставлене завдання реалізується шляхом аналізу та дослідження стандартів, алгоритмів та систем захисту даних що передаються каналами мобільного зв'язку.

Виклад основного матеріалу

Стандарт IS-95C забезпечує високий ступінь безпеки переданих повідомлень і даних про абонентів. Насамперед він має більш складний, ніж GSM (*Global System for Mobile Communications*), радіоінтерфейс, що забезпечує передачу повідомлень кадрами з використанням канального кодування і перемежування з наступним «розширенням» переданих сигналів за допомогою складових *широкосмугового сигналу* (ШСС), сформованих на основі 64 послідовностей Уолша і псевдовипадковими послідовностями з кількістю елементів 2^{15}–1 та 2^{42}–1.

Безпека зв'язку забезпечується також застосуванням процедур автентифікації і шифрування повідомлень.

Процедура автентифікації в стандарті IS-95C відповідає процедурі автентифікації стандарту D-AMPS (IS-54B).

У рухомій станції зберігається один ключ А і один набір загальних секретних даних (*Shared Secret Data — SSD*), які використовуються під час роботи як у режимі з частотним поділом каналів, так і в режимі CDMA IS-95C.

Рухома станція може передавати «цифровий підпис» для автентифікації, що складається з 18 біт. Ця інформація передається на початку повідомлення (у відповіді рухомій станції на запит мережі у разі пошуку станції), додається до реєстраційного повідомленням або пакету даних, переданих по каналу доступу.

Передбачається можливість поновлення загальних секретних даних у рухомій станції [3].

Безпека абонентської інформації в цьому стандарті ґрунтується на чотирьох фундаментальних елементах:

1) функція CAVE — функція перемішування, що використовується в протоколах автентифікації запит—відповідь і для генерації ключів;

2) операція XOR — повторювана маска, накладається на голосові дані для забезпечення безпеки їх передачі;

3) шифр ORYX — потоковий шифр, призначений для використання в послугах бездротового доступу до даних;

4) шифр CMEA (*Control Message Encryption Algorithm*) — простий блоковий шифр, використовується для шифрування службових повідомлень.

Криптографічні протоколи стандарту CDMA ґрунтуються на 64-бітному автентифікаційному ключі A-key (*Authentication Key*) і серійному номері мобільного телефону ESN (*Electronic Serial Number*). Для автентифікації абонента при реєстрації мобільного телефону в мережі, а також подальшої генерації допоміжних ключів (беруть участь у забезпеченні конфіденційності передачі голосових даних і кодованих повідомлень) використовується випадкове двійкове число RANDSSD (*Random Shared Secret Data*), що генерується автентифікаційним центром AC (*Authentification Center*) для реєстру власних абонентів HLR (*Home Location Register*) і має довжину 56 біт.

Ключ A-key запрограмований у мобільному телефоні та зберігається в центрі автентифікації мереж [4].

У кожному телефоні зберігається два числа:

• A-key — це 64-бітове число-ключ, яке вводиться при продажі телефону і зберігається в базі. Оскільки A-key не передається в ефір, його не можна перехопити і використовувати, як це робилося з серійними номерами [4];

• ESN (*Electronic Serial Number)* — 32-бітний код, що привласнюється мобільному телефону при його виготовленні і використовується для ідентифікації.

При включенні телефону базова станція передає йому випадкове число RANDSSD. На основі A-key, ESN, MSID (*Mobile Subscription Identification Number*) і RANDSSD за допомогою алгоритму шифрування CAVE генерується 128-бітний підключ SSD, який складається з двох частин SSD_A і SSD_B по 64 біти кожний. SSD_A і A-key зберігаються в телефоні і на станції і ніколи не передаються по мережі [5].

CAVE — це програмно-сумісна нелінійна змішувальна функція. Вона складається з трьох компонентів:

• 32-бітний LFSR (*Linear-Feedback Shift Register*) — регістр зсуву з лінійним зворотним зв'язком;

• шістнадцять 8-бітних змішувальних регістрів;

• таблиця перетворення, що складається з 256 елементів.

Алгоритм шифрування складається з трьох етапів:

1) початкове завантаження даних у регістри A, B, C, D, R00-R15;

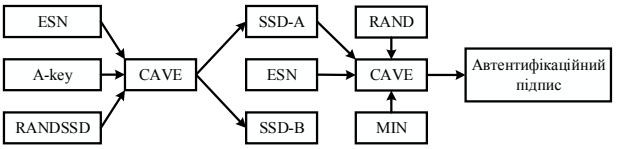
2) операція змішування в 4 або 8 раундів за допомогою таблиці CAVE та операцій з регістрами A, B, C, D;

3) виведення даних.

Періодично (приблизно один раз на тиждень) станція посилає стільниковому телефону повідомлення про генерацію нового тимчасового ключа, SSD_A; при отриманні цього повідом-

лення (SSD_UPDATE) телефон розраховує новий тимчасовий ключ SSD_A, використовуючи A-KEY, ESN, MSID, і випадкове число зі станції. Таким чином, сам ключ автентифікації (SSD_A) є тимчасовим і періодично міняється, і «клонування» MS (*Mobile Station*) стає невиправданим, а також знаходження SSD_A методом послідовного перебору, оскільки після першої ж зміни ключа працювати далі буде тільки один телефон з новим ключем.

З частотою один раз на 20 хв базова станція генерує 128-бітове випадкове число RAND і передає його широкомовно. Потім мобільний пристрій на основі SSD_A і RAND за допомогою алгоритму CAVE генерує 18-бітний цифровий підпис AUTH_SIGNATURE, який передається по мережі на станцію і там порівнюється із незалежно обчисленим числом на базовій станції (див. рисунок). Якщо вони не збігаються, то автентифікація вважається невдалою, і користувачеві відмовляють про з'єднання [5].



Процес автентифікації

При цьому випадкове число RAND може бути як однаковим для всіх користувачів, так і заново генеруватися щоразу, використання конкретного методу визначається оператором. Перший варіант забезпечує дуже швидку автентифікацію.

Як мобільний телефон, так і мережа ведуть 6-бітові лічильники дзвінків, що забезпечує можливість детектування двійників: для цього достатньо лише контролювати відповідність значень лічильників на телефоні і в центрі комутації MSC (*Mobile Switch Center*). Секретний ключ A-key може бути перепрограмований за необхідності, але в разі його зміни інформація на мобільному телефоні і в регістрі мережі HLR (*Home Location Register*) повинна бути синхронізована. Зміна ключа може бути «прошита» на заводі, дилером у точці продажу, абонентом через інтерфейс телефону, а також за допомогою спеціального сервісу OTASP (*Over The Air Service Provisionig*). Цей сервіс використовує в процесі передачі 512 бітний алгоритм узгодження ключів Діффі–Хелмана, що гарантує досить високий рівень безпеки. OTASP забезпечує легкий спосіб зміни ключа A-key мобільного телефону на випадок появи в мережі двійника мобільного телефону, оскільки така зміна автоматично спричинить відключення послуг двійника мобільного телефону і повторне включення послуг легітимного абонента. Таким чином, таємність ключа A-key є практично важливим компонентом безпеки CDMA системи.

Але під час упровадження нового покоління мережі на мережу попереднього покоління, не одразу оператори впроваджують новий стандарт у 100 % відповідності. І це є підґрунтям для виникнення двійників.

Проблема двійників з'явилася з початком експлуатаційних робіт стільникової мережі CDMA в Гонконзі. Головною перешкодою служили самі мобільні термінали, які використовувалися в цих мережах: вони не підтримували найпростішого і потужного засобу з боротьби з клонами — A-key.

Автентифікація основана на алгоритмі CAVE та повністю ефективна проти звичайних (англ. *regular*) «клонів-шахраїв». Будь-яка спроба повного клона отримати доступ до мережі з автентифікацією буде не вдалою. Причина в тому, що в той час як клон ідентифікує себе як інший абонент використовуючи незаконно отримані дані про ESN та MSID, він не буде мати доступу до мережі, через відсутність правильного SSD. Таким чинам, автентифікація може повністю вирішити проблему шахрайств за допомогою клонів [6].

Більш проблематичним є наявність повного (англ. *complete*) клона, який має коректний A-key, більш небезпечніший тому, що він у стані успішного оновлення ключа SSD та проведення успішної автентифікації.

Наявність повного клону вказує на проблему, пов'язану з безпекою мережі, бази даних у оператора, що спричинило розголошення секретного ключа A-key.

Проте автентифікація, основана на алгоритмі CAVE проводить *Call History Count* (COUNT), що б сприяти виявленню клона, навіть у разі існування повного клона, після виявлення в обслуговуванні може бути відмовлено і ця дія змусить з'явитися законного абонента в центр обслуговування для відновлення надання послуг зв'язку [6].

COUNT — 6-бітовий лічильник подій за модулем 64, він ведеться як на мобільній станції, так і на стороні оператора. Події, які призводять до збільшення значення лічильника, визначаються адміністративними налаштуваннями оператора, можуть включати ініціалізацію реєстрації в новій обслуговуючій станції (MSC), дзвінки, повідомлення або періодично.

З розвитком мобільних мереж третього покоління в двох різних напрямках CDMA та UMTS (*Universal Mobile Telecommunications System*) стало необхідним забезпечити функціонування мобільних станцій стандарту CDMA в мобільних мережах стандарту UMTS — для забезпечення мобільності самих користувачів, для користу-

вання мобільними мережами третього покоління без заміни мобільної станції, оскільки алгоритм автентифікації, який використовується в UMTS, більш надійний. У 2005 р. був запропонований новий метод автентифікації (TIA-945) абонентів у мобільних мережах стандарту CDMA, який має працювати зверх алгоритму CAVE — *Enhanced Subscriber Authentication* (ESA). Даний алгоритм автентифікації базується на 3GPP *Authentication and Key Agreement* (AKA) для UMTS. Підтримка MAP для AKA в мережах CDMA визначається в IS-945 з підтримкою всіх наступних радіоінтерфейсів після CDMA Rev C включно. Однак, щоб полегшити сумісність і дати можливість поетапного впровадження AKA між різними абонентами CDMA, пристроями та мережами що підтримують AKA, повинні також забезпечувати автентифікацію на базі CAVE. IS-945 також оновлює параметри можливості автентифікації (AUTHCAP) та можливості системи (SYSCAP), щоб забезпечити в роумінгових та домашніх мережах ідентифікацію та автентифікації для MS [6].

Основні переваги AKA передбачають сильну і двосторонню підтримку автентифікації. Надійніша автентифікація забезпечується використанням 128-бітних ключів автентифікації та хеш-функцією SHA-1. Двостороння автентифікація забезпечується через «маркер» автентифікації, переданого MS під час запиту автентифікації. Механізм задання унікальності AKA схожий на CAVE, з погляду мережевої автентифікації мобільної станції. Додавання маркера забезпечує MS інформацією, яка дозволяє йому автентифікуватися в мережі до завершення виклику. Можливість двосторонньої автентифікації запобігає атакам на базову станцію, які могли б вплинути на конфіденційність зв'язку, або поставити під загрозу особисту інформацію, що засвідчує особу.

Додаткові функції безпеки входять в AKA і гарантують більшу безпеку ніж функція CAVE. Після двосторонньої автентифікації суб'єктів AKA проводить генерацію нових шифр-ключа та ключа цілісності (*Cipher key* (*CK*), *integrity key* (IK)). Дані 128-бітні ключі дають змогу встановити безпечний зв'язок між MS та обслуговуючою MSC для підтримки розширених послуг безпека такі, як сигнальні повідомлення цілісності даних, сигнальну інформацію шифрування елемента та шифрування даних користувача.

Також генерується 128-бітний автентифікаційний ключ UIM (*User Identity Module*) — UAK (*UIM authentication key*), який використовується для захисту від загроз клонованих мобільних станцій під час роботи з UIM.

Мобільна станція та домашня мережа генерують ці ключі незалежно. Ключі, згенеровані домашньою мережею, задають вектори автентифікації в гостьовій мережі та ніколи не передаються каналами зв'язку як MSC так і MS.

Висновки

Проаналізувавши основні алгоритми, що забезпечують автентифікацію користувачів у мобільній мережі стандарту CDMA2000, було доведено надійність даної мережі, оскільки автентифікація проводиться за допомогою даних що не передаються каналами зв'язку, а ті, що передаються, не дають зловмиснику використати їх у своїх цілях.

Треба зазначити, що цей стан захищеності можливий лише за умови, якщо оператор упроваджує функціонування мобільних мереж CDMA2000 у 100 % відповідності специфікаціям розроблених стандартів.

ЛІТЕРАТУРА

1. *Нікітін Г. І.* Застосування функцій Уолша в стільникових системах зв'язку з кодовим розподілом каналів: навч. посібник / Г. І. Нікітін // СПб. : ДУАП — 2003. — 86 с.

2. *Шаповал В*. Кількість користувачів мобільного зв'язку в Україні становить 58,63 млн. — [Електронний ресурс] / В. Шаповал // IT Expert — 2013. — Режим доступу до джерела: http://itexpert.org.ua/rubrikator/item/24657-kolichestvo-polzovatelej-mobilnoj-svyazi-v-ukraine-dostiglo-5863-mln.html.

3. *Адмін* CDMA One (IS-95). Технічні характеристики. — [Електронний ресурс] / Адмін // PBXLib.com.ua — 2013. — Режим доступу до джерела: http://pbxlib.com.ua/mobile/article_125.html.

4. *Wingert Christopher* CDMA 2000 1xRTT Огляд безпеки / Christopher Wingert, Mullaguru Naidu // Qualcomm. — 2002.

5. *Іванова Т. Г.* Захищеність мереж CDMA. — [Електронний ресурс] / Т. Г. Іванова // Московский физико-технический институт — 2004. — С. 3–5. — Режим доступу до джерела: http:// re. mipt. ru/ infsec/2004/essay/2004_CDMA_Security__Ivanova.pdf.

6. CDMA автентифікація / CDG Document 138 // CDMA Development Group. — 2006. — 75 с.

Стаття надійшла до редакції 25.04.2014.