УДК 621.396

ПРОБЛЕМИ ЗАХИСТУ ІНФОРМАЦІЇ В МЕРЕЖАХ МОБІЛЬНОГО ЗВ'ЯЗКУ ТРЕТЬОГО ПОКОЛІННЯ

І. І. Пархоменко, канд. техн. наук, доц., ***Ю. О. Кривий***

Національний авіаційний університет

parkh08@ukr.net, kriviy@ukr.net

Розглянуто модель архітектури мережі UMTS, види атак на неї. Наведено механізми забезпечення захисту інформації в мережах UMTS, які протистоять загрозам, що мали місце в мережах другого покоління(GSM).

Ключові слова: інформаційна безпека, шифрування, мобільний зв'язок, бездротові технології.

Considered model of network architecture UMTS, types of attacks on this network. Also considered mechanisms to ensure information security in networks UMTS, which resist the threats that have taken place in the networks of second generation (GSM).

Keywords: information security, encoding, mobile communications, wireless technology.

Постановка проблеми

Справжню революцію у сфері телекомунікацій здійснила поява великої кількості бездротових технологій, таких як *GSM* (*Global System for Mobile Communications* — глобальна система для мобільних комунікацій), 802.11 (серія стандартів, які визначають взаємодію бездротових комп'ютерних мереж), *UMTS* (*Universal Mobile Telecommunications System* — універсальна мо-більна телекомунікаційна система), *CDMA* (*Code Division Multiple Access* — технологія з кодовим поділом каналів), *GPRS* (*General Packet Radio Service* — послуга пакетної передачі даних).

Стільниковий зв'язок став важливою частиною повсякденного життя.

Крім використання стільникових телефонів для спілкування, ми можемо користуватись Інтернетом, відправляти мультимедійні повідомлення та обмінюватись електронною поштою та файлами.

Однак бездротові мережі мають певні недоліки порівняно з дротовими мережами: відкритість радіоефіру, обмежена пропускна здатність та системна складність. Ці обмеження значно впливають на проектування засобів захисту для забезпечення аутентифікації, цілісності та конфіденційності.

Універсальна мобільна телекомунікаційна система — одна з провідних технологій мобільного зв'язку третього покоління (3G). Вона розроблялась як розвиток *GSM* і ґрунтується на мережі *GPRS*.

За даними *UMTS Forum* [2] кількість абонентів 3G/*UMTS* мереж стала більшою ніж 500 млн абонентів.

Аналіз досліджень і публікацій

Питаннями дослідження захисту мереж третього покоління займалися такі вчені, як Р. А. Бельфер, Ю. Г. Горшков, А. П. Акулов.

Мета

Мета даної роботи — огляд архітектури, атак на *UMTS* та аналіз можливих проблемних місць у моделі безпеки та способи їх подолання.

Архітектура мережі

В основі мережі лежить ядро з комутацією пакетів, яке сполучається з зовнішньою мережею Інтернет. Цей факт робить мережу вразливою для нових типів атак, таких як *DOS* атаки, віруси, «черв'яки» і т.д., які поширені в мережі Інтернет.

Щоб виокремити загрози такої мережі потрібно зрозуміти мережеву інфраструктуру. З рис. 1 видно, що 3G мережа складається з двох основних частин:

- радіомережа доступу (*Radio Access Network*);
- базова мережа (*Core Networ*).

Радіомережа доступу складається з існуючої *GPRS/GSM* мережі, до якої підключені мережа з комутацією пакетів (МКП) і мережа з комутацією каналів (МКК). МКП у свою чергу з'єднюється з системою *UTRAN* (*Universal Terrestrial Radio Access Network*) для повного переходу до 3G. *UTRAN* складається з підсистеми в склад якої входить контролер радіомережі (КР), до якого під'єднано декілька базових передавальних станцій (БПС).

Базова радіомережа складається з МКП та МКК (рис. 1). МКП складається з серверів *SGSM* (*Serving GPRS Support Node*) та *GGSM* (*GPRS Gateway Service Node*). Кожний SGSN з'єднює один чи більше КР з МКП. Його функціонал включає управління доступом, мобільністю, маршрутом та сповіщенням. *GGSM* — логічний шлюз з'єднання з Інтернет. Інформаційні сервери забезпечують декілька функцій: визначення розташування абонентів і аутентифікацію користувачів. Є також *DNS*, *DHCP* і сервери *RADIUS*, які взаємодіють з *SGSN/GGSN* і забезпечують функції контролю та управління.

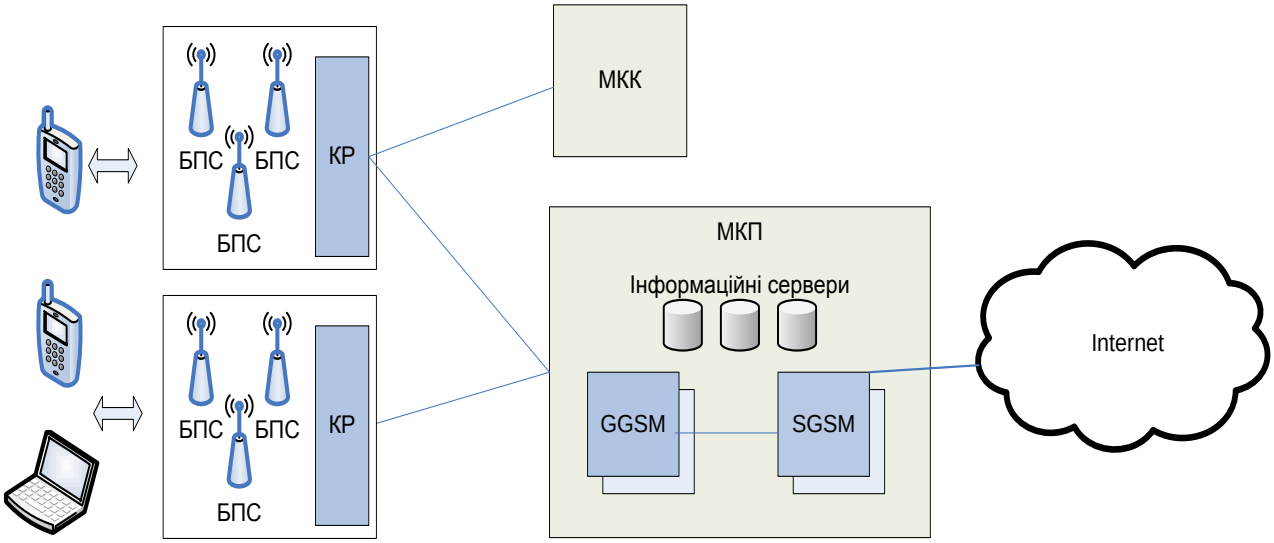

Рис. 1. Архітектура мережі

Отже, інфраструктура такої мережі масивна і складна з чисельними об'єктами, які взаємодіють. Тому забезпечення безпеки в кожному можливому каналі зв'язку є значною проблемою.

Бездротові стільникові мережі мають значні обмеження порівняно з дротовими мережами, а саме:

1. Відкритість бездротового середовища: оскільки дані передаються в радіоефірі, то немає ніякого фізичного бар'єра який перешкодить зловмиснику отримати доступ.

2. Обмежена пропускна здатність: хоча пропускна здатність бездротових мереж постійно збільшується, однак вона не може конкурувати з дротовими технологіями.

3. Складність системи: бездротові системи більш складні через забезпечення мобільності і здатності ефективно використовувати канал.

4. Обмежена обчислювальна потужність: процесори, встановлені на бездротових пристроях, не достатньо потужні, щоб виконувати інтенсивну обробку інформації.

5. Відносно ненадійне з'єднання з мережею: під час передачі сигналу по радіоканалу на нього діє більше завад ніж у дротових. Наведемо основні недоліки мережі, які слід враховувати при розгортанні стільникової інфраструктури, важливість яких збільшилась з появою 3G.

За допомогою *аутентифікації* оператор переконується, що суб'єкт дійсно той, за кого він себе видає.

За великої кількості абонентів оператор повинен бути впевнений, що надає послуги тим абонентам, які мають на це право.

Оскільки мета 3G — дозволити людям отримати зв'язок у будь-якій точці світу, то перехресна аутентифікація стає проблемою.

Інтенсивно збільшується кількість телефонів з операційними системами, що мають ті самі можливості що і настільні комп'ютери тому потенційною проблемою є *мобільні операційні системи*.

У них можуть виявитись «дірки», якими скористаються зловмисники.

Веб-сервіс є компонентом, який забезпечує функціональність доступу через мережу, використовуючи стандартний HTTP протокол. Це робить стільниковий пристрій вразливим до загроз, таких як віруси, переповнення буфера, атаки «відмова в обслуговуванні» і т.д.

Оскільки в стільниковій мережі достатньо легко *визначити розташування* абонентів, то через конфіденційність цю інформацію потрібно приховувати, і не дозволити зловмиснику отримати її.

У випадку втрати або *викрадення мобільного пристрою*, він має бути захищеним від несанкціонованого використання, щоб не можна було отримати доступ до електронних листів, документів, телефонних номерів тощо.

Види атак

Через складну архітектуру мережі можливі різноманітні види атак, наведемо основні з них (рис. 2):

Відмова в обслуговуванні (*DoS*), імовірно являє саму потужну атаку, яка може призвести всю мережеву інфраструктуру в неробочий стан.

Реалізується при надмірній передачі даних через мережу, що призводить до неможливості користувачів використовувати сервіси.

Розподілена відмова в обслуговуванні (*DDoS*) — використовується велика кількість вузлів для здійснення атаки.

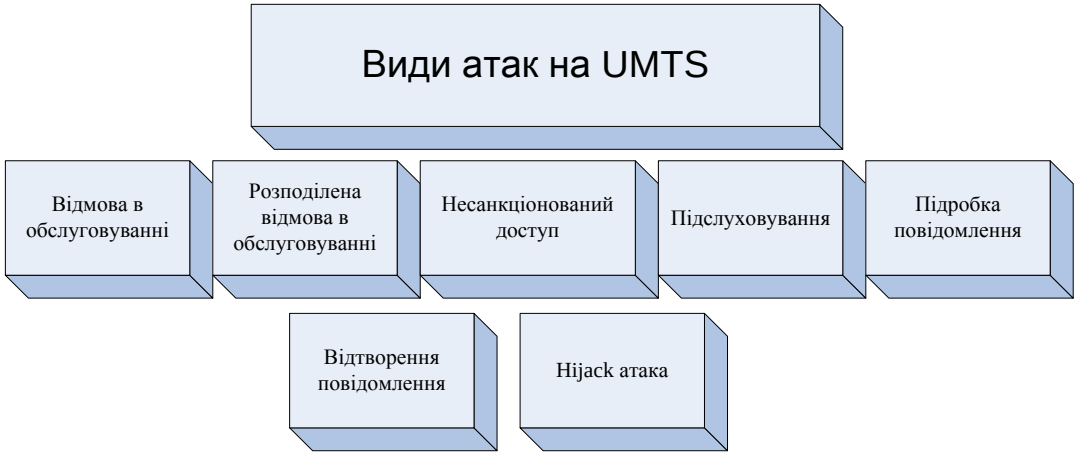

Рис. 2. Види атак

При н*есанкціонованому доступі* не використовується належний метод аутентифікації. Тоді атакуючий може отримати вільний доступ до мережі і нелегально використовувати її сервіси.

Підслуховування — зловмисник може підслухати і перехопити передачу конфіденційної інформації.

Підробка повідомлення — коли канал передачі незахищений, зловмисник може фальсифікувати повідомлення і передавати їх в мережу.

Навіть, якщо канал передачі безпечний, атакуючий може перехопити зашифроване повідомлення і знов *відтворити* та відправити його легальному користувачу. Тоді користувач не знатиме, чи отримане повідомлення є коректним. *Hijack атака* — зловмисник може підключитись до мережі і діяти як законна базова станція.

Механізми захисту

Безпека UMTS ґрунтується на механізмах, розроблених для мереж 2G. Основні функції здійснення безпеки такі:

- аутентифікація користувача;
- шифрування даних для передачі по радіоінтерфейсу;
- тимчасова ідентифікація.

Аутентифікація користувача в *UMTS* так само, як і в мережі *GSM*, здійснюється за допомогою шифрування з загальним ключем по протоколу типу «запит-відгук». При аутентифікації мережі оператору *UMTS* надається можливість вибору алгоритму.

Всі алгоритми аутентіфікації мережі в *UMTS* можна розділити на дві группи — без використання шифрування і з використанням блокового симетричного шифрування. Прикладом першого є алгоритм формування коду аутентифікації повідомлення за протоколом *HMAC*.

До другої групи належить використання блочного шифрування повідомлення в режимі зчеплення блоків *CBC*.

Останній зашифрований блок служить для формування коду аутентифікації повідомлення блочного симетричного шифрування.

Для передачі даних у стандарті *UMTS* визначені функції шифрування f8 і функція f9, яка відповідає за цілісність. Функція f8 базується на алгоритмі *KASUMI*, який був розроблений групою *SAGE* (*Security Algorithms Group of Experts*) що є частиною Європейського Інституту з Стандартизації в області телекомунікацій. За основу було взято існуючий алгоритм *MISTY*1 і оптимізований для використання в стільниковому зв'язку. *KASUMI* використовує 64-бітний розмір блоку і 128-бітний ключ та 8-раундову схему Фейстеля. У кожному раунді використовується 128-бітний раундовий ключ, що складається з восьми 16-бітних підключей, отриманих з вихідного ключа.

На додаток до принципів, використаних в мережах другого покоління, *UMTS* також реалізує:

- взаємну аутентифікацію (не тільки абонент автентифікований мережею, але і клієнт аутентифікує мережу, щоб усунути можливість атаки з використанням помилкової базової станції);
- взаємне підтвердження ключів шифрування і аутентифікації між користувачем і обслуговуючої мережею;
- захист цілісності (введені вдосконалені алгоритми і ключі для забезпечення цілісності даних);
- мережеву безпеку (забезпечує шифрування всередині та між різними мережами);
- безпека сервісів і додатків (удосконалені механізми забезпечення надійності для сервісів та додатків).

Усі, вищеперераховані принципи та запропоновані методи забезпечення захисту інформації в мережах *UMTS* протистоять таким загрозам, які мали місце в мережах другого покоління:

- підключення фальшивих базових станцій;

- крадіжка каналу під час сесії;
- перехоплення ключів шифрування і аутентифікації;
- загроза порушення цілісності даних;
- складність упровадження нових механізмів інформаційної безпеки.

Висновки

UMTS став першим масовим стандартом бездротового зв'язку, що забезпечує серйозний рівень захисту інформації користувача. Було використано дві принципово нові речі.

По-перше, було розглянуто можливість атаки за допомогою підставної базової станції, чого не передбачалося раніше.

По-друге, завдяки публічності проведених досліджень, було проведено детальніший аналіз криптостійкості.

Отримані результати відповідають сучасним вимогам і заслуговують на довіру. Важливим є й та обставина, що оператор може вибирати функцію-ядро системи безпеки.

Однією з прогалин у системі захисту даних у мережах *UMTS* є відсутність застосування системи сертифікатів користувачів.

Це обумовлено низькою продуктивністю процесорів, що застосовуються в більшості стільникових телефонів, які нині не в змозі ці сертифікати обробляти.

Однак, як тільки процесори стануть потужнішими, така система буде впроваджена. Використання цієї системи дасть змогу застосовувати електронно-цифровий підпис в обміні інформацією в бездротових мережах, чого на сьогодні поки ще не зроблено.

Нововведення дозволить забезпечити гарантовану цілісність переданих документів — захищений документообіг, підтвердження справжності їх відправника; створення довірчої комунікації в мережі. Тому система безпеки в мережах UMTS з часом буде вдосконалюватися, що обумовлено інтенсивним розвитком засобів і методів несанкціонованого доступу до інформації, а як наслідок — появою нових загроз.

ЛІТЕРАТУРА

1. *Бельфер Р. А.* Анализ систем связи в аспекте проектирования информационной безопасности // Электросвязь / Р. А. Бельфер. — 2004. — № 3.

2. http://www.mobile-arsenal.com.ua/news/5579/

3. *Security* In Wireless Cellular Networks. Ali I. Gardez.

4. *Бельфер Р. А.* Безопасность мобильных систем связи 3G / Р. А. Бельфер, А. П. Акулов // Вестник связи, 2001. — № 12.

5. *Шнайер Б.* Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си / Б. Шнайер. — М. : Издательство Триумф, 2003. — 816 с.

Стаття надійшла до редакції 09.03.2011.