УДК 658.52; 681.3

АНАЛІЗ ЗАХИЩЕНОСТІ БЕЗДРОТОВИХ МЕРЕЖ З ВИКОРИСТАННЯМ WEP-ТЕХНОЛОГІЇ

О. К. Юдін, д-р техн. наук, проф.; ***О. Весельська***

Національний авіаційний університет

kszi@ukr.net

У статті досліджено ефективність захисту інформаційних ресурсів у бездротових мережах на основі використання WEP-протоколу та симетричного алгоритму шифрування RC4. Розглянуто шляхи та подальші можливості підвищення ефективності методів захисту інформації.

Ключові слова: бездротові мережі, криптографія, шифрування, інформаційна безпека, ключі.

In the article the quality of information security in wireless networks by using WEP-encryption scheme and RC4 symmetrical streaming algorithm was studied. The tips and ways to improve the security of information are given.

Keywords: wireless networks, cryptography, encryption, information security, keys.

Вступ

У вересні 1999 р. міжнародна організація інженерів IEEE-SA ухвалила два стандарти бездротових мереж: 802.11b – 2,4 ГГц, 11 Мб і 802.11a — 5 ГГц, 54 Мб. З тих пір бездротові мережі швидко поширились на всі сфери людської діяльності, такі як торгівля, освіта, охорона здоров'я і т. д. Важливим фактором у поширенні бездротових мереж та інтеграція їх до складу комутативних (дротових) — нагальна потреба в організації системи вільного віддаленого доступу до основних бізнес-додатків і інформаційних ресурсів, а також потреба у використанні базових сервісів та послуг інформаційно-комунікаційних систем (ІКСМ). Незалежними тестовими компаніями, такими як *Wireless Ethernet Compatibility Alliance* (WECA) було значно полегшено систему взаємодії різнорідних мереж та стандартизовано процес їх інтеграції до загального інформаційного середовища [1].

Мета цих дій — мобільність системи передачі даних для клієнтів як основна вимога для побудови корпоративних мереж великих організацій. Проте деякі перешкоди, зокрема: безпека інформаційних ресурсів і потоків даних, високий рівень доступності до додатків та послуг користувачами різних класів, система розподілу спектру в бездротових мережах заважають розгортати масштабні бездротові інформаційні системи на багатьох підприємствах.

Постановка завдання

Організація безпеки бездротових мереж — завдання, що потребує комплексних розв'язків її організації.

Незахищеність бездротових мереж — це найбільший недолік, який заважає тотальній заміни дротових мереж. Сьогодні в бездротових мережах IEEE 802.11 стандарту існує декілька поколінь технологій забезпечення та організації захисту інформаційних ресурсів: WEP, WPA, WPA2 (IEEE 802.11i); використання протоколів авторизації IEEE 802.1x; використання VPN (*Virtual Private Network*) для побудови захищеної мережі та обміну даними [3].

Мета дослідження — аналіз стандартів і методів, що забезпечують захист інформаційних ресурсів бездротових мереж з умови використання технології шифрування WEP (*Wired Equivalent Privacy*).

Цілями даної роботи є:

- дослідження ефективності захисту інформації, що забезпечує схема шифрування WEP;
- дослідження продуктивності WEP залежно від методів його реалізації та визначення подальших напрямів і можливостей їх підвищення;
- оцінка криптостійкості симетричного потокового алгоритму RC4;
- формування рекомендацій щодо організації та впровадження нових методів підвищення рівня захищеності інформації в бездротових мережах із використанням протоколів WEP.

Аналіз методів шифрування

Спочатку проведемо аналіз методів захисту даних на базі WEP протоколів. Схема шифрування WEP є необов'язковою для використання в бездротових мережах передачі даних, проте, не зважаючи на це, доступна як механізм першого покоління забезпечення захищеної взаємодії між

вузлами інформаційної системи та захисту потоків даних у бездротових мережах.

Основними завданнями WEP є:

— обмеження доступу до мережі неавторизованим користувачам, що не мають відповідного WEP-ключа або згідно з правилами політики безпеки;

— організація запобіжних дій щодо дешифрування даних, які зашифровані за допомогою WEP (у разі відсутності WEP-ключа у неавторизованого користувача).

WEP-протокол являє собою механізм симетричного шифрування. Якщо WEP дозволений, передавач бере вміст кадру (відкритий текст), тобто лише корисну інформацію, та запускає алгоритм шифрування. Після цього оригінальний вміст кадру замінюється на дані, отримані після закінчення виконання алгоритму шифрування. Кадри даних, що були зашифровані, посилаються із WEP-бітом у контрольному полі MAC-заголовка. Одержувач кадру із зашифрованими даними пропускає кадр через зворотний ідентичний алгоритм розшифрування.

У результаті на виході отримуємо оригінальний кадр, що передається протоколам вищого рівня, відповідно до ієрархічної моделі OSI [3]. Продуктивність WEP залежить від виду реалізації — апаратної або програмної, а також від конкретного пристрою.

Деякі пристрої дають змогу досягти продуктивності передачі даних у мережі лише на 2–3 % гіршої, ніж без використання шифрування. Однак дуже часто, особливо при програмній реалізації, відбувається істотне зменшення продуктивності мережі. WEP-технологія використовує потоковий шифр RC4 (запропонований Роном Рівестом) з RSA Data Security, Inc. (RSADSI). Алгоритм шифрування RC4 — це симетричний потоковий шифр, що підтримує ключі різної довжини. Симетричний шифр — це шифр, що використовує ідентичний ключ для шифрування і розшифрування. Він сильно відрізняється від блочних шифрів, які обробляють фіксовану кількість байт. Ключ — це деяка інформація, котра може бути доступна як відправнику, так і одержувачу. RC4 допускає різну довжину ключа — до 256 біт. В IEEE 802.11b вибрана довжина ключа в 40 біт. Проте деякі виробники підтримують також і 128 бітний ключ та надають пристрої для роботи з такою довжиною ключа.

Алгоритм RC4 характеризується такими властивостями:

- адаптивністю для апаратних засобів та програмного забезпечення (ПЗ), що означає використання в ньому лише примітивних обчислювальних операцій, які використовуються звичайними процесорами;
- компактністю в термінах розміру ключа, а також особливою вигідною реалізацією на процесорах з побітно-орієнтовною обробкою;
- низькими вимогами до пам'яті, що дозволяє реалізувати алгоритм на пристроях з обмеженими технічними характеристиками;
- простотою та легкістю виконання.

Алгоритм RC4 будується, як і будь-який потоковий шифр, на основі параметризованого ключем генератора псевдовипадкових чисел. Алгоритм реалізації RC4 складається з двох частин:

1) створення ключа (іноді називають розширенням ключа);

2) процесом реалізації безпосередньо самого алгоритму шифрування.

*Створення ключа***.** Ключ RC4 являє собою послідовність байтів довільної довжини, за якою будується початковий стан шифру S — перестановка всіх 256 байт.

На початку роботи алгоритму S заповнюється послідовними значеннями від 0 до 255, а K заповнюється ключем (за необхідності для заповнення всього масиву ключ повторюється). Після цього кожний черговий елемент S_j обмінюється місцями з елементом під номером i, номер якого визначається елементом ключа K, самим елементом і сумою номерів елементів, з якими проходив обмін у попередніх ітераціях, тобто $j = S_i + K_i + j$.

```
 void swap(unsigned char *s, unsigned int i, unsigned int j)  //Функція перестановки елементів Si
{                //та Sj методом «бульбашки»
    unsigned char tmp;
    tmp = s[ i ];
    s[ i ] = s[ j ];
    s[ j ] = tmp;
}
    void init(unsigned char *key, unsigned int length)  //Функція ініціалізації алгоритму RC4
{       //(Key-Scheduling Algorithm)
for (i = 0; i < 256; i++)     //Ініціалізація масиву S та його
S[ i ] = i; //заповнення елементами від 0 до 255
    for (i = j = 0; i < 256; i++)
{
    j = (j + key[i % length] + S[ i ]) % 256; // Скремблювання та виклик функції
    swap(S, i, j); //перестановки двох елементів
    }
    i = j = 0;
    }
```

Алгоритм шифрування. Черговий елемент псевдовипадкової перестановки S_i всіх байтів

обмінюється з елементом S_j, де $i = (i + 1) \bmod 256$, а $j = (j + S_i) \bmod 256$.

Як черговий байт видається значення третього елементу S, номер якого визначається як сума елементів S_i та S_j.

```
unsigned char output()
//Генератор псевдовипадкової послідовності
{
// (Pseudo-Random Generation Algorithm)
i = (i + 1) % 256;  //Генерація номерів елементів, що передаються в
j = (j + S[ i ]) % 256;
//функцію перестановки
swap(S, i, j);
return S[(S[ i ] + S[ j ]) % 256]; //Визначення одного псевдовипадкового байту
}
```

Далі на кожен байт вихідного повідомлення накладається згенерований псевдовипадковий байт за допомогою логічної операції «XOR» («виключне АБО»).

```
for(i = 0; i < strlen(mess); i++)
{
init(key, strlen(key));
//Алгоритм ключового розкладу (KSA)
wifr [ i ] = mess [ i ] ^ output(); //Використання функції «XOR» для кодування вихідних //даних (PRGA)
}
```

Для демонстрування роботи розробленого програмного додатка використаємо таку структуру:

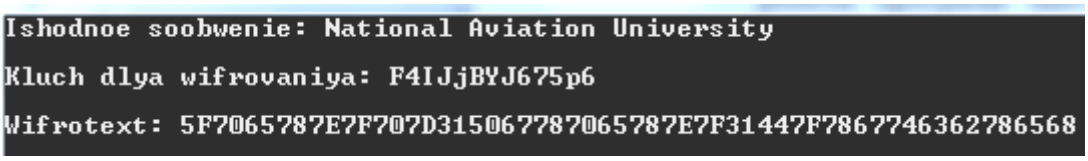
– початковий відкритий (інформаційне повідомлення) текст береться з визначеного файла;

– ключова послідовність відповідно до схеми шифрування WEP може становити або 5 або 13 символів відповідно (для більшої стійкості алгоритму довжину ключа встановимо рівною 13 символам за замовчуванням). Ключ може складатися з малих і великих букв латинського алфавіту, а також арабських цифр;

– згенерована ключова послідовність за допомогою генератора псевдовипадкових чисел заноситься у файл;

– вихідне повідомлення, закодоване за допомогою алгоритму RC4 для демонстрування роботи програми, заноситься у файл у двох форматах: символьному та шістнадцятковому;

– на дисплей результати виконання програми виводяться у шістнадцятковому вигляді (див. рисунок).



Результати виконання програми

Стандарт IEEE 802.11 забезпечує два механізми вибору ключа для шифрування та розшифрування кадрів. Перший механізм оснований на встановленні чотирьох ключів за замовчуванням. Ключі за замовчуванням мають бути відомі всім станціям бездротової підмережі. Перевага використання ключів за замовчуванням в тому, що якщо станція отримала ці ключі, то вона може вести обмін даними секретно з усіма іншими станціями підмережі.

Недолік використання такого механізму в тому, що ключі доступні всім станціям, а, отже, досить велика ймовірність їх «взлому» або несанкціонованого отримання.

Другий механізм, що забезпечується стандартом IEEE 802.11, дозволяє станції встановлювати зв'язок з кожною іншою за визначеними різними ключами («key mapping»). Це, імовірно, більш захищена форма роботи, оскільки меншій кількості станцій відомо ключ. Проте розподілення таких ключів проблематично, якщо кількість станцій у мережі досить велика [1].

IEEE 802.11 визначає два типи методів аутентифікації: відкрита система аутентифікації та аутентифікація з розподіленим (*shared*) ключем.

Вдале виконання фаз аутентифікації та з'єднання дозволяє вузлу бездротової мережі вдало увійти у робочий режим організації передачі даних з умов загальної карти вузлів бездротової мережі.

При аутентифікації з відкритим ключем весь аутентифікаційний процес проходить з відкритим текстом. Це означає, що клієнт може з'єднатися з точкою доступу з неправильним WEP-ключем або взагалі без нього. Але, як тільки клієнт спробує відправити чи прийняти дані, він не зможе цього зробити, оскільки для обробки кадрів необхідно знати правильний ключ.

Під час аутентифікації з розподіленим ключем у процесі аутентифікації використовуються зашифровані повідомлення. Якщо клієнт не має правильний ключ, то він пройде стадію аутентифікації і не зможе виконати з'єднання з точкою доступу.

У цьому випадку WEP-заголовок додається до тіла зашифрованного кадру. Номер ключа за замовчуванням, який потрібно використовувати для розшифрування кадру міститься в полі KeyID заголовка кадру разом з вектором ініціалізації. Кінцівка містить *Integrity Check Value* (ICV) для контролю правильності переданого кадру. Довжина ключа зазвичай розподіляється на довжину WEP-ключа та довжину вектора ініціалізації. Наприклад, 64-бітний ключ складається з 40-біт-ного WEP-ключа, що зберігається таємно, та 24-бітного вектора ініціалізації [3].

Недоліки захищеності IEEE 802.11 та можливі шляхи їх подолання. Найбільш вагомим недоліком стандарту 802.11 є відсутність оптимального способу розподілу ключів. Статистичний розподіл, що визначений у специфікації стандарту, не використовується у чистому вигляді для великих мереж і на великих проміжках часу. Виникає необхідність періодичної зміни ключів, а для мереж великих масштабів, і у разі відсутності зручних способів розподілу ключів, це становить доволі серйозну проблему для системного адміністратора. Також досить важко зберегти ключ у таємниці, якщо до мережі матимуть доступ неавторизовані користувачі.

Ще одним недоліком статистичного розподілення ключів є те, що при пасивному спостереженні потоків даних у мережі досить довго, можливо накопичити достатньо інформації про ключ, що дасть змогу безперешкодно дешифрувати повідомлення. Усунення цього недоліку потребує створення схеми динамічного розподілу ключів, їх постійного оновлення і прив'язки ключів не до вузла мережі, а до користувача (щоб неавторизований користувач знав лише свій особистий ключ, і у випадку його поширення третій стороні був доступний лише його трафік). Іншим суттєвим недоліком є те, що в стандарті 802.11 існує лише процес аутентифікації клієнта, а аутентифікація сервера відсутня. Це дає можливість атакувати мережу шляхом введення в неї несанкціонованих серверів і перенаправлення потоку даних на них. Для усунення цього недоліку необхідно ввести схему взаємної аутентифікації, в якій обидві сторони повинні доводити свою легітимність. Якщо ж вузол не зміг зробити цього за відповідно відведений час, то він повинен бути ізольований як несанкціонований користувач.

Наступним недоліком є те, що не відбувається аутентифікації кожного пакету, і можливі підміни або генерація неіснуючих пакетів. Однак це доволі складно реалізувати з технічного погляду. Для подолання цього недоліку необхідно частіше змінювати ключі та вектор ініціалізації. Ще одним вразливим місцем стандарту IEEE 802.11 є власне алгоритм шифрування RC4, що реалізований у WEP. І хоча компанія RSA *Data Security* заявляла, що шифр володіє імунітетом до методів лінійного та диференційного криптоаналізу, а також що він високо нелінійний і в його алгоритмі не використовуються короткі цикли, його надійність була поставлена під сумнів через несанкціоноване розголошення тексту програми, що використовувала даний шифр. Такі події загрожують безпеці бездротових мереж, що використовують WEP технологію як схему шифрування [1].

У роботі Й. Голіча, що стосувалась аналізу криптостійкості вказаного алгоритму, відмічалось, що для послідовностей, згенерованих RC4, не підходять методи статистичного аналізу. Але, з іншого боку, для блоків, розмір яких перевищує розмір внутрішньої пам'яті генератора, завжди існує лінійна статистична слабкість або так звана «лінійна модель».

Таку модель можна ефективно визначити за допомогою методу апроксимації лінійною послідовною схемою (АЛПС). Лінійна статистична слабкість – це лінійне співвідношення між бітами гамми, що виконується із імовірністю, відмінною від 1/2. З практичного погляду лінійна модель Й. Голіча може бути використана для виділення по шифротексту генератора RC4 серед інших криптосистем, а також для визначення розміру слова алгоритму.

В 2000 р. була опублікована стаття С. Флюера та Д. Мак-Грі, присвячена статистичному аналізу потокового генератора RC4, у котрій були використані результати роботи Й. Голіча для знаходження значення компонент S-боксу. Приблизний час роботи цього методу становить 2^{6n}, де n — порція бітів у вихідному потоці, довжина вихідної послідов-ності, що потрібна для визначення статистичної слабкості RC4, приблизно становить 2^{30}.

Отриманий результат вказує на істотну слабкість генератора і можливість відновлення параметрів i та n. Можливими способами підвищення стійкості RC4 до зламування є збільшення довжини ключа до максимального значення у 256 байт і реалізації його динамічної зміни, що використовується для шифрування повідомлень, але це, у свою чергу, негативно вплине на пропускну здатність бездротового каналу передачі даних. Іншим методом подолання слабкостей у схемі шифрування WEP є використання тунелювання через бездротову мережу з використанням протоколів IPSec і SSL/TLS. Проте існують рішення, що роблять бездротову мережу безпечною (WPA, WPA2) [3].

Висновки

Проведено аналіз стандартів і методів, що забезпечують захист інформаційних ресурсів бездротових мереж з умови використання технології шифрування WEP (*Wired Equivalent Privacy*).

В роботі досліджено ефективність системи захисту інформації, що забезпечує технологія шифрування WEP; розглянуто питання продуктивності WEP залежно від методів його реалізації та визначення подальших напрямів і можливостей їх підвищення; надано загальну оцінку криптостійкості симетричного потокового алгоритму RC4; розглянуто подальші шляхи підвищення рівня захищеності інформації в бездротових мережах із використанням протоколів WEP.

ЛІТЕРАТУРА

1. *Пролетарский А. В.* Беспроводные сети Wi-Fi/ А. В. Пролетарский, И. В. Баскаков, Д. Н. Чирков, Р. А. Федотов [и др.]. — М. : Бином. Лаборатория знаний, 2007. — 216 с.

2. *Бехроуз А*. Криптография и безопасность сетей: учеб. пособие / А. Бехроуз. — М. : Бином. Лаборатория знаний, 2010. — 784 с.

3. *Максим М.* Безопасность беспроводных сетей / М. Максим, Д. Полино. — М. : Компания АйТи; ДМК Пресс, 2004. — 288 с.

4. *НД ТЗІ 1.1-003-99*. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу.

5. НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу.

Стаття надійшла до редакції 25.06.2012.