УДК 004.8+65.05+681.5

А. В. ПАТРІКЕЙ, С. С. РОМАНЧУК, М. О. КАРПЕЦЬ, студенти,
Державний університет телекомунікацій, Київ

АНАЛІЗ МОЖЛИВИХ ЗАГРОЗ БЕЗПРОВОДОВИМ МЕРЕЖАМ НА БАЗІ МІКРОКОНТРОЛЕРА ESP8266

У статті виконано аналіз основних технічних засобів і систем, застосовуваних для організації атаки на Wi-Fi мережу. Розкрито структуру мікрочіпа та дано пояснення щодо призначення його компонентів. Наведено технічні характеристики приладу, який слугує для атак на Wi-Fi мережу. Запропоновано варіанти основних і допоміжних видів мікрочіпа. Проаналізовано можливості їх застосування як за допомогою комп'ютера, так і з використанням планшетів, смартфонів чи іншої мобільної техніки.

Ключові слова: інтернет; комп'ютер; мікрочіп; Wi-Fi мережа; захист інформації; атаки на безпроводові мережі.

Вступ

Сучасні технології дають змогу створювати деавтентифікатори мереж із залученням спеціальних драйверів і відповідного програмного забезпечення. Тому дедалі гостріше постає проблема захисту безпроводових мереж передавання даних, таких як Wi-Fi мережа. Для її розв'язання існує низка апаратних і технічних засобів, варіюванням та комбінуванням характеристик яких вдається поліпшити показники захищеності Wi-Fi мереж.

Головна мета статті — визначення технічного стану та налаштування засобів і обладнання, необхідних для проведення атаки на мережу Wi-Fi та її захисту з урахуванням динамічного розвитку сучасних комп'ютерних технологій.

Здійснення атаки на Wi-Fi мережу за допомогою мікрочіпа ESP8266 на базі Arduino

Основний технічний аспект щодо побудови захисту від атаки на безпроводову мережу полягає в тому, аби правильно визначити й описати загрозу. Це зрештою дасть змогу застосувати власні гаджети для забезпечення конфіденційності інформації, коли йдеться про інноваційний, популярний і бюджетний різновид атак, який із кожним роком зміцнює свої позиції серед наявних аналогів. Адже все більше й більше користувачів, переважно молодь, практикують різні види несанкціонованого доступу до безпроводових мереж.

Китайські виробники електронної техніки вже випускають нове покоління мікрочіпів згаданого призначення на базі Arduino.

Зауважимо, що з розвитком мобільних інтернет-технологій нові можливості для здійснення несанкціонованого доступу до Wi-Fi мереж з'являються в сучасних гаджетів — смартфонів й планшетів. Тому сьогодні безпроводовий захист невпинно актуалізується.

Так, за прогнозами аналітиків протягом найближчих чотирьох років світова абонентська база безпроводових мереж зросте в кілька разів. Один із головних чинників, який істотно сприятиме успіху безпроводових мереж, — стрімке зростання попиту користувачів на безпроводові пристрої (планшети, ноутбуки, смартфони).

Розглянемо докладніше прилад, на базі якого здійснюються особливо небезпечні атаки на безпроводові мережі. Ідеться про мікроконтролер ESP8266 китайського виробника Espressif (див. рисунок).

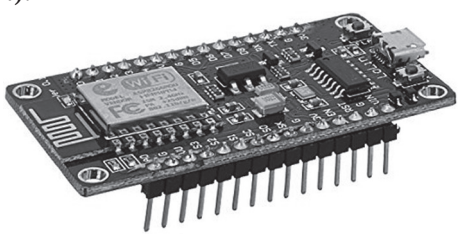

Рис. 1. Мікроконтролер ESP8266

ГОЛОВНІ ТЕХНІЧНІ ХАРАКТЕРИСТИКИ:

- 80 МГц. Можливий розгін до 160 МГц.
- 32-біт процесор Tensilica Xtensa L106.
- IEEE 802.11 b/g/n Wi-Fi. Підтримується WEP та WPA/WPA2.
- 14 портів входу-виходу (із них можливо використовувати 11), SPI, IC, IS, UART, 10-біт АЦП.
- Живлення — 2,2…3,6 В.
- Споживання до 215 мА у режимі передавання; 100 мА у режимі прийому; 70 мА у режимі очікування.
- Підтримуються три режими зниженого живлення, усі без збереження з'єднання з точкою доступу.
- Modem sleep (15 мА), Light sleep (0.4 мА), Deep sleep (15 мкА).
- Двохядерний 32-біт Tensilica Xtensa® LX6 з FPU і MAC. 240 МГц (600 DMIPS).
- 448 кбайт ПЗУ, 520 кбайт ОЗУ. Зовнішні ОЗУ/ПЗУ на SPI інтерфейсі, до 4·16 Мбайт. Зовнішня пам'ять може бути криптографічно захищена.
- Джерело живлення — 2,2…3,6 В.
- Wifi 802.11, Bluetooth v4.2 (у тому числі Low Energy).
- Збільшена кількість портів і периферії: ADC, DAC, 4 SPI, 2 I2S, 2 I2C, 3 UART, CAN. Інтерфейс SD карт (як майстер, так і слейв). Ethernet MAC.
- Корпус QFN-48.
- Інтегроване середовище розробки Arduino.

При створенні атаки зловмисник має насамперед визначитись із її видом, що, вочевидь, залежить від поставленої ним мети.

Існують три можливі види атак на Wi-Fi мережу за допомогою ESP8266. Розглянемо два з них.

Більшість сучасних пристроїв запам'ятовують назву Wi-Fi мережі, до якої вони успішно під'єдналися принаймні одного разу, і негайно з'єднуються з нею, якщо «побачать» її в безпроводвому ефірі. Цю вразливість безпроводових технологій дедалі активніше використовують зловмисники, створюючи rogue AP (підроблену точку доступу). Такі атаки з кожним роком стають все масштабніші, передусім через постійно зростаючий ринок безпроводових пристроїв і величезний обсяг критичної інформації, що міститься в них.

Ще один вид атак — це деавтентифікація, що реалізується на програмному рівні. Деавтентифікатор здійснює атаку типу «відмова в обслуговуванні», відправляючи на роутер фрейм деавтентифікації від імені під'єднаних до мережі пристроїв. Оскільки цей фрейм ніяк не шифрується, мікроконтролеру достатньо з'ясувати MAC-адреси пристроїв, перехопивши трафік у мережі.

Зазвичай деавтентифікація — це частина комплексної атаки на мережу. Вона використовується при створенні «злого двійника» точки доступу або для перехоплення хендшейка, що згодом дозволяє розшифрувати пароль. Проте мікроконтролер здатний створити атаку й сам по собі.

Атаки проводяться за допомогою установленого на мікроконтролері Web-сервера, яким можна користуватись через будь-який пристрій із Wi-Fi адаптером.

Тепер спинимось на питанні захисту від цих атак. Передусім ідеться про використання стандарту IEEE 802.11w-2009, який може підвищити безпеку шляхом конфіденційного пересилання даних кадрів управління, механізмів, що забезпечують цілісність даних та їхню автентичність. Можна також використовувати утиліту Waipds, призначену для виявлення атак на безпроводові мережі.

Висновки

♦ Безпроводові мережі передавання даних стрімко набувають популярності, чому сприяє високий розвиток комп'ютерних і мобільних технологій у поєднанні з величезним набором програм і пристроїв для організації Wi-Fi.

♦ Удосконалення апаратних характеристик і програмних вирішень створює нові можливості для несанкціонованого доступу в безпроводові мережі.

♦ Незабаром передавання інформації через безпроводові мережі буде основою для всієї мережі Інтернет, а тому вже сьогодні потрібно дбати про надійний захист у цій сфері.

♦ Розглянуті способи та методи захисту безпроводових мереж становлять значний практичний інтерес, що, безумовно, посприяє подальшому вдосконаленню Wi-Fi мережі.

♦ З огляду на небачені темпи розвитку сучасної апаратури та техніки є всі підстави стверджувати про необхідність подальшої роботи в цій сфері та її неодмінну успішність.

Список використаної літератури

1. ***Official*** *IEEE 802.11 Working Group Project Timelines (19 September 2016). 57c.*

2. ***Скуснов А.*** *Тестирование точек доступа: беспроводной интернет в каждую квартиру // Upgrade: компьютерный еженедельник. 2004. № 44(186). С. 49.*

3. ***Таненбаум Е.*** *Комп'ютерні мережі. 2018. 32 с.*

4. ***Standard*** *IEEE 802.1. September 2004. С. 4–5.*

5. ***Sidak J. Gregory.*** *The Antitrust Division's Devaluation of Standard. Essential Patents, 2017. 6 с.*

Рецензент: доктор техн. наук, доцент **С. І. Отрох**, Державний університет телекомунікацій, Київ.

А. В. Патрикей, С. С. Романчук, Н. А. Карпец

АНАЛИЗ ВОЗМОЖНЫХ УГРОЗ БЕСПРОВОДНОЙ СЕТИ НА БАЗЕ МИКРОКОНТРОЛЛЕРА ESP8266

В статье проведен анализ основных технических средств и систем, применяемых для организации атаки на Wi-Fi сеть. Раскрывается структура микрочипа и объясняется назначение его компонентов. Приведены технические характеристики прибора, применяющиеся для атак на Wi-Fi сеть. Представлены варианты основных и вспомогательных видов микрочипа. Проанализирована возможность их применения как при помощи компьютера, так и с использованием планшетов, смартфонов и другой мобильной техники.

Ключевые слова: интернет; компьютер; микрочип; Wi-Fi сеть; защита информации; атаки на беспроводные сети.

A. V. Patrikei, S. S. Romanchuk, M. O. Karpets

ANALYSIS OF POSSIBLE THREATS OF WIRELESS NETWORK BASED ON THE MICROCONTROLLER ESP8266

The article analyzes the main technical means and systems used to organize an attack on the Wi-Fi network. The structure of the microchip is revealed and the purpose of its components is explained. The technical characteristics of the device used for attacks on the Wi-Fi network are given. The variants of main and secondary types of microchips are presented. The possibility of application, for the help of the computer, and tablets, smartphones and other mobile equipment, is analyzed.

This device is so tiny you can fit into pocket and carry it anywhere. It can powered through your power bank or 3.7v Lithiumion battery. You can select which Wi-Fi network you want to jamming and attack on it. The 802.11 Wi-Fi protocol contains a so called deauthentication frame. It is used to disconnect clients safely from a wireless network. Because these packets are unencrypted, you

just need the mac address of the Wi-Fi router and of the client device which you want to disconnect from the network. You don't need to be in the network or know the password, it's enough to be in its range.

You can perform multiple attacks on this device such as you can jamming any particular wifi network or you can do beacon spam or random beacon spam or you can simple deauthorize all.

This software allows you to easily perform a variety of actions to test 802.11 wireless networks by using an inexpensive ESP8266 Wi-Fi SoC (System On A Chip). The main feature, the deauthentication attack, is used to disconnect devices from their Wi-Fi network.

No one seems to care about this huge vulnerability in the official 802.11 Wi-Fi standard, so I took action and begin to study this device with a price less than 10 USD to spare to recreate this project.

I hope it raises more attention on the issue. In 2009 the Wi-Fi Alliance actually fixed the problem (see 802.11w), but only a few companies implemented it into their devices and software.

To effectively prevent a deauthentication attack, both client and access point must support the 802.11w standard with protected management frames (PMF).

While most client devices seem to support it when the access point forces it, basically no Wi-Fi access point has it enabled.

Keywords: Internet; computer; microchip; Wi-Fi network; information security; attacks on wireless networks.

УДК 681.32

Ю. А. МИЛОВА, аспирантка,
Государственный университет телекоммуникаций, Киев

ПАРАМЕТРЫ СУММАРНЫХ КОДОВ

В статье рассмотрены важнейшие свойства параметров суммарных кодов. Отмечено, что наряду с кольцевыми и фрактальными кодами суммарные коды являются полипараметрическими. Полипараметричность суммарных кодов позволяет использовать их для защиты конфиденциальной информации от несанкционированного доступа. Описан способ построения суммарных кодов. Даны определения понятий, применяемых при вводе параметров суммарных кодов. Показано, что параметры суммарного кода могут служить его эквивалентом и полностью заменить такой код. Раскрыт смысл нормирования суммарных кодовых слов, в результате которого возникают двойные нормированные коды с нулевыми остатками (дуальные кратности). Приведены понятия, необходимые для описания алгоритмов построения суммарных кодовых слов. Предложены варианты комбинаций параметров и видов суммарных кодовых слов, при помощи которых можно получить различные алгоритмы борьбы с канальными ошибками. Ввиду того, что суммарные коды являются полипараметрическими, одновременное использование отдельных их параметров обеспечивает точность обмена данными. Всего по одному параметру суммарного кода можно оценить его верность. Привлечение дополнительных параметров позволяет правильно восстановить суммарный код. Предложенный метод дает возможность реализовать различные сочетания кодовых параметров. Указана область использования суммарных кодов.

Ключевые слова: натуральный ряд; суммарные коды; полипараметрические коды; модуль; сумма элементов натурального ряда; двойные нормированные коды; норма; нормированное суммарное кодовое слово; порядковый номер суммарного кодового слова; признак; индекс кодового слова с двойной (дуальной) кратностью; смещение; полипараметрические суммарные коды; представление параметров суммарных кодов; искаженные кодовые комбинации; параметры кода; остаток; дуальная кратность.

Введение

Кодовые слова рассматриваемых в статье полипараметрических суммарных кодов формируются как суммы

$$s_n = 1 + 2 + \ldots + n = \sum_{i=1}^{n} a_i$$

последовательных натуральных чисел от единицы до n.

Значение такой суммы определяется по формуле

$$s_n = \frac{n(n+1)}{2}.$$

Например, значения s_n при $n = 1,2,\ldots,15$ иллюстрирует рис. 1.

Главная особенность полипараметрических кодов заключается в том, что параметры каждого такого кода могут служить его эквивалентом и полностью заменить первоначальный код. Это позволяет, варьируя параметры кода и их сочетания, восстанавливать искаженные кодовые комбинации.

Исходные суммарные коды напрямую связаны с их порядковыми номерами, представляющими собой сумму $s(n)$ членов натурального ряда, построенную по указанному ранее способу.

Основная часть

Суммарные коды после их формирования могут быть нормированы. Нормирование осуществляется делением порядкового номера кода, т. е. суммы s_n, на некоторое небольшое целое число k. В результате возможно появление двойных нормированных кодов с нулевыми остатками (дуальных кратностей).