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).

Слева и справа от этих двух кодов другие нормированные коды оказываются симметрично одинаковыми, с расходящимися вверх и вниз по порядковым номерам суммарных кодов остатками. На этом основании можно строить полипараметрические суммарные коды, ограничиваясь лишь параметрами кодов без кодовой комбинации, которую в конечном итоге легко восстановить по параметрам кодов. Формирование нормированных при $k = 7$ кодов иллюстрирует рис. 2, где $n = 85,\ldots,100$; $n = 1,\ldots,15$.

s_n	n
1	1
3	2
6	3
10	4
15	5
21	6
28	7
36	8
45	9
55	10
66	11
78	12
91	13
105	14
120	15

Рис. 1. Суммарные коды в первоначальном виде

$\frac{1}{7}s_n$	n	$\frac{1}{7}s_n$	n
522,143	85	0,143	1
534,429	86	0,429	2
546,857	87	0,857	3
559,429	88	1,429	4
572,143	89	2,143	5
585	90	3	6
598	91	4	7
611,143	92	5,143	8
624,429	93	6,429	9
637,857	94	7,857	10
651,429	95	9,429	11
665,143	96	11,143	12
679	97	13	13
693	98	15	14
707,143	99	17,143	15
721,429	100		

Рис. 2. Суммарные нормированные при $k = 7$ коды

Закономерности, имеющие место при $n = 25,\ldots,40$ в случае нормирования кодов при $k = 4; 5; 6$, отражает рис. 3.

$\frac{1}{4}s_n$	n	$\frac{1}{5}s_n$	n	$\frac{1}{6}s_n$	n
81,25	25	65	25	54,167	25
87,75	26	70,2	26	58,5	26
94,5	27	75,6	27	63	27
101,5	28	81,2	28	67,667	28
108,75	29	87	29	72,5	29
116,25	30	93	30	77,5	30
124	31	99,2	31	82,667	31
132	32	105,6	32	88	32
140,25	33	112,2	33	93,5	33
148,75	34	119	34	99,167	34
157,5	35	126	35	105	35
166,5	36	133,2	36	111	36
175,75	37	140,6	37	117,167	37
185,25	38	148,2	38	123,5	38
195	39	156	39	130	39
205	40	164	40	136,667	40

Рис. 3. Суммарные нормированные при $k = 4; 5; 6$ коды

Следует подчеркнуть, что параметры суммарного кода удобно использовать с целью обнаружения и исправления канальных ошибок. При этом достаточно ограничиться порядковым номером двойной кратности и значением нормирующего числа k.

Вместо суммарной кодовой комбинации в канал имеет смысл передавать порядковый номер дуальной кратности, выполняющий роль индекса в математических операциях, а также смещение по порядковым номерам суммарных кодов. Тогда все указанные номера суммарных кодов оказываются задействованными.

Важные в практическом плане случаи использования параметров рассмотрены далее.

Определение понятий

• **Норма:** число, на которое осуществляется деление каждого суммарного кодового слова для получения его модуля и остатка.

• **Нормированное суммарное кодовое слово:** модуль нормированного кодового слова с удаленным остатком.

• **Порядковый номер суммарного кодового слова:** количество слагаемых элементов натурального ряда, образующих данное суммарное кодовое слово.

Из структуры суммарных кодовых слов становится очевидным, что порядковые номера суммарных кодовых слов изменяются от единицы до заданного n.

• **Признак:** показатель (двоичный нуль или двоичная единица), по которому различается использование в контенте обычного суммарного кодового слова или его нормированного эквивалента.

• **Двойная (дуальная) кратность:** два подряд следующих друг за другом нормированных суммарных кодовых слова с нулевыми остатками.

• **Индекс кодового слова с двойной (дуальной) кратностью:** число, показывающее количество встречающихся до данного номера суммарных нормированных кодовых слов с нулевым остатком.

• **Смещение:** количество отклонений в сторону возрастания порядковых номеров кодовых слов от последних по порядку двух кодовых слов с двоичной кратностью.

Варианты представления параметров суммарных кодов

Комбинируя параметры и общий вид суммарных кодовых слов, получаем различные алгоритмы борьбы с канальными ошибками. Приведем несколько наиболее полезных алгоритмов.

Вариант 1. *Суммарное кодовое слово–признак–индекс:* по такому алгоритму формируются обычные суммарные кодовые слова либо нормированные с нулевой двойной кратностью.

Пример. В канал посылается двоичная последовательность цифр с разделением 13-1-2 либо 97-0-2. Согласно рис. 2 первый набор цифр соответствует нормированному коду с порядковым номером 13 и нулевым остатком. Вторая последовательность отображает тот же самый, но не нормированный $k = 7$ суммарный код.

Вариант 2. *Признак–индекс с двойной (дуальной) кратностью.* По такому алгоритму формируются обычные либо нормированные с двойной кратностью суммарные кодовые слова.

Пример. В канал посылается двоичная последовательность цифр с разделением 1-2 либо 0-2, которая повторяется для обнаружения и исправления канальных ошибок. Конечный результат должен быть таким же, как и в предыдущем примере.

Вариант 3. *Суммарное кодовое слово–признак–индекс–смещение.* Как и в предыдущих случаях, по такому алгоритму формируются обычные суммарные кодовые слова либо нормированные с двойной кратностью. Правомерность такого алгоритма определяется тем фактом, что, как можно показать, суммарных кодов с двойной кратностью существует не более 5% из общего их числа. Однако после любой пары кодов двойной кратности остатки нормированных кодов одинаковы в обе стороны по их множеству до очередной повторяемой двойной кратности. Эту особенность можно наблюдать на рис. 2 и 3.

Пример. В канал посылается двоичная последовательность цифр с разделением 4-0-1-2 или 21-0-1-2. В этом случае в канал кроме нормированного либо обычного кода поступают признак, индекс и смещение, по которым можно проверить правильность суммарного кода на приемном конце.

Вариант 4. *Признак–индекс–смещение с повторением.* Аналогичен варианту 3 за исключением смещения. Рассматривался при изложении варианта 2. Как и в том случае, повторение при передаче данной числовой последовательности дает возможность выявить и устранить канальные ошибки.

Выводы

♦ Суммарные коды являются полипараметрическими, что может служить важным фактором для их идентификации.

♦ Посредством выбора значений делителей k получаются различные версии нормированных по этому делителю суммарных кодов.

♦ Совместное одновременное использование нескольких параметров суммарных кодов позволяет достаточно верно осуществлять обмен данными.

♦ Один отдельный параметр суммарного кода позволяет оценить верность суммарного кодового слова. Дополнительное использование других параметров позволяет восстановить его правильность.

♦ Возможны различные методы реализации кодовых параметров.

♦ Полипараметричность суммарных кодов удобно использовать при реализации защиты информации от несанкционированного доступа.

Список использованной литературы

1. ***Дикарев А. В.*** *Фрактальная структура сжатого натурального ряда / Зв'язок. 2017. №3(127). С. 34–38.*
2. ***Дикарев А. В.*** *Сжатие двоичных блочных кодов // Зв'язок. 2017. №1(125). С. 40–42.*
3. ***Алгоритми*** *створення проріджувальних кодів / В. Г. Сайко, О. В. Дікарєв, Л. М. Грищенко [та ін.] // Зв'язок. 2017. №2(126). С. 33–38.*
4. ***Фракталы*** *в физике: под ред. Л. Пьетронеро, Э. Тозатти. Москва, 1988.*
5. ***Берлекэмп Э.*** *Алгебраическая теория кодирования. Москва. 1971. 477 с.*

Ю. О. Мілова

ПАРАМЕТРИ СУМАРНИХ КОДІВ

У статті розглянуто найважливіші властивості параметрів сумарних кодів. Зазначено, що поряд із кільцевими та фрактальними кодами сумарні коди належать до поліпараметричних. Поліпараметричність сумарних кодів можна застосовувати для реалізації захисту конфіденційної інформації від несанкціонованого доступу. Описано формування сумарних кодів. Подано визначення основних понять, використовуваних при введенні параметрів сумарних кодів. Показано, що параметри сумарних кодів можуть слугувати еквівалентом коду та повністю його замінити. Розкрито сенс нормування сумарних кодових слів, у результаті якого з'являються випадки подвійних нормованих кодів із нульовими остачами (дуальних кратностей). Сформульовано визначення понять, використовуваних для опису алгоритмів формування сумарних кодових слів. Наведено кілька варіантів комбінацій параметрів і видів сумарних кодових слів, за допомогою яких можна отримати різні алгоритми боротьби з канальними помилками. Завдяки тому, що сумарні коди є поліпараметричними, одночасне використання окремих їхніх параметрів дозволяє підвищувати точність обміну даними. Лише за одним параметром сумарного коду можна оцінити правильність коду. За додатковими параметрами дозволяється відновити правильність сумарного коду. Даний метод дає можливість реалізувати різні методи кодових параметрів. Наведено область застосування сумарних кодів.

Ключові слова: натуральний ряд; сумарні коди; поліпараметричні коди; модуль; сума елементів натурального ряду; подвійні нормовані коди; норма; нормоване загальне кодове слово; порядковий номер сумарного кодового слова; ознака; індекс кодового слова з двійковою (дуальною) кратністю; зсув; поліпараметричні сумарні коди; подання параметрів сумарних кодів; спотворені кодові комбінації; параметри коду; остача; дуальна кратність.

Yu. A. Milova

PARAMETERS OF CUMULATIVE CODES

This article presents the properties and features of digital cumulative codes parameters where the code words are created by adding the elements of natural sequence. It should be noted that along with circular and fractal codes, the cumulative codes are poliparametric ones. The formation of digital cumulative codes is described in the article. The article gives the definition of the main concepts used to enter the parameters of cumulative codes. It is shown that the parameters of cumulative codes can serve as their equivalent and entirely replace them. The demonstrated regulation of cumulative codes is produced at the expense of correlation of code words to another natural number, and as a result, there are cases of pair normalized codes with zero residues (dual multiplicity).The concepts used for description of cumulative codes algorithms are formulated in the article. The described variants of parameters combinations and the types of cumulative codes make it possible to receive various algorithms of fight against the channel errors. According to one parameter (variable) of cumulative code it is possible to identify it and evaluate its fidelity. In terms of additional parameters (advanced options) it is possible to restore the correctness of cumulative code. It has been demonstrated that the use of separate cumulative codes parameters simultaneously increases data exchange fidelity that allows to apply them for protection of confidential information from non-authorized admission. The proposed method gives an opportunity to apply received cumulative codes for both compression of information while its transfer and for protection of information distortion transmitted on communication channels and the control of access to confidential information using various methods of code parameters.

Keywords: natural series; cumulative codes; polyparametric codes; module; the sum of elements of the natural numbers; the double of the normalized codes; the rate; normalized cumulative code word; sequence number of the cumulative code word; the index of the codeword with the binary (dual) magnification; offset; polyparametric cumulative codes; represent the parameters of the cumulative codes; the distorted code combination; code parameters; remainder; dual multiplicity.

ЗВ'ЯЗОК

Наукове видання

Редакційна обробка та коректура
О. П. Бондаренко, Т. В. Ількевич

Комп'ютерна верстка та дизайн
Г. С. Тимченко

Відповідальний за випуск
І. І. Тищенко

Формат 60×84/8. Папір друкарський.
Гарнітура SchoolBookC, EuropeCond. Зам. 115
Наклад 300 прим.

Державний університет телекомунікацій
03110, м. Київ, вул. Солом'янська, 7
Тел. (044) 249-25-75
E-mail: *zviaz-ok@ukr.net*