УДК 621.396.4; 656.13

# ПРИМЕНЕНИЕ ПОСЛЕДОВАТЕЛЬНОСТЕЙ ГОРДОНА-МИЛЛСА-ВЕЛЧА В ИНТЕЛЛЕКТУАЛЬНЫХ ТРАНСПОРТНЫХ СИСТЕМАХ

**В. А. Григорьев,**
заведующий кафедрой беспроводных телекоммуникаций Национального исследовательского университета ИТ, механики и оптики (НИУ ИТМО), д.т.н.

**В. Г. Стародубцев,**
начальник отдела ООО «Мультисервисные сети и телекоммуникации», к.т.н.

**В. О. Аксенов,**
аспирант СПбГУТ им. проф. М. А. Бонч-Бруевича; vladaksi@labics.ru

***Ключевые слова:*** *интеллектуальная транспортная система, беспроводные сети малого радиуса действия, технология DSRC (Dedicated Short Range Communication), последовательность Гордона-Миллса-Велча, эквивалентная линейная сложность, псевдослучайная последовательность.*

**Введение.** Современный уровень развития интеллектуальных транспортных систем (ИТС; Intelligent Transport Systems, ITS) в качестве телекоммуникационной основы предполагает использование технологий на базе стандартов 802.11p, IEEE 1609, Wireless Access in Vehicular Environment (WAVE) и др. [1, 2]. Применение оборудования, поддерживающего данные стандарты для целей повышения безопасности дорожного движения, планируется в диапазоне беспроводных сетей малого радиуса действия (Dedicated Short Range Communication, DSRC).

Стандарт 802.11p определяет взаимодействие Wi-Fi-оборудования, движущегося со скоростью до 200 км/ч мимо неподвижных точек доступа, удаленных на расстояние до 1 км. Составная часть стандарта — Wireless Access in Vehicular Environment (WAVE). Стандарты WAVE определяют архитектуру и дополнительный набор служебных функций и интерфейсов, которые обеспечивают безопасный механизм радиосвязи между движущимися транспортными средствами. Эти стандарты разработаны для таких приложений, как, например, организация дорожного движения, контроль безопасности движения, автоматизированный сбор платежей, навигация и маршрутизация транспортных средств и др. Таким образом, Wi-Fi-технология 802.11p — технология Wi-Fi, разработанная для беспроводной передачи информации между высокоскоростными транспортными средствами и объектами транспортной инфраструктуры с целью создания интеллектуальной транспортной системы. Используемый частотный диапазон — 5,855—5,925 ГГц [1, 2].

Группа для разработки стандарта IEEE 802.11p была сформирована в ноябре 2004 г., а версии стандарта появлялись с 2005 по 2009 г. [3]. В настоящее время семейство стандартов IEEE 1609 включает восемь документов: IEEE 1609.0–IEEE 1609.5, IEEE 1609.11, IEEE 1609.12. Они определяют как общую архитектуру технологии WAVE, так и протокол передачи коротких сообщений (WAVE short

message protocol, WSMP), которыми обмениваются объекты в сети, а также порядок осуществления многоканального взаимодействия на MAC-уровне и порядок обмена данными с верхними уровнями WAVE-архитектуры.

В перспективных ИТС, охватывающих транспортную структуру больших мегаполисов, существенно возрастают требования по обеспечению безопасности при обмене информацией внутри сети, по защите от возможных информационных атак, «прослушивания» сети, несанкционированного доступа, а также по соблюдению конфиденциальности.

Одним из возможных направлений повышения безопасности функционирования ИТС является применение псевдослучайных последовательностей (ПСП), обладающих хорошими автокорреляционными свойствами и высокой эквивалентной линейной сложностью. Такие последовательности могут использоваться на канальном уровне для скремблирования сигналов BPSK, QPSK, QAM, используемых в рассмотренных выше телекоммуникационных стандартах. Применение ПСП существенно затрудняет несанкционированный доступ к передаваемой информации и снижает возможность формирования и распространения ложных информационных сигналов в рамках ИТС.

В современных системах в качестве скремблирующих последовательностей используются М-последовательности, достоинством которых является одноуровневая периодическая автокорреляционная функция. К недостаткам М-последовательностей можно отнести низкую структурную скрытность, т.е. возможность быстрого вскрытия структуры сигнала для осуществления несанкционированного доступа к передаваемой информации.

Повысить безопасность функционирования ИТС можно, используя вместо М-последовательностей последовательности Гордона-Миллса-Велча (ГМВП) (Gordon-Mills-Welch, GMW). Эти псевдослучайные последовательности относятся к классу периодических последовательностей, автокорреляционные свойства которых аналогичны свойствам М-последовательностей [4—6], но обладают более высокой эквивалентной линейной сложностью [5].

**Алгоритм формирования последовательностей Гордона-Миллса-Велча.** ГМВП формируются над конечными полями с двойным расширением вида $GF[(p^m)^n]$, вследствие чего период данных последовательностей является составным числом, т.е. $N = p^{mn} - 1$, где $p$ — характеристика поля; $m$, $n$ — натуральные числа. В настоящее время широкое применение получили двоичные ГМВП над полями с двойным расширением вида $GF[(2^m)^n]$. Символы $d_i$ данных последовательностей периода $N = 2^{mn} - 1$ формируются в соответствии с выражением [7—9]:

$$d_i = tr_{m1}[(tr_{mn,m}(\alpha^i))^r],\ 1 \le r < 2^m - 1,\ (r, 2^m - 1) = 1, \quad (1)$$

где $tr_{mn,m}(\cdot)$ — след элемента из поля с двойным расширением $GF[(2^m)^n]$ в расширенном поле $GF(2^m)$; $tr_{m1}(\cdot)$ — след элемента из расширенного поля $GF(2^m)$ в простом поле $GF(2)$; $\alpha \in GF[(2^m)^n]$ — примитивный элемент поля с двойным расширением. Параметр $r$ является числом, взаимно простым с порядком мультипликативной группы расширенного поля $GF(2^m)$, равным $2^m - 1$.

При $r = 1$ согласно свойству функции следа выражение (1) описывает М-последовательность (МП):

$$d_i = tr_{m1}[(tr_{mn,m}(\alpha^i)] = tr_{mn,1}(\alpha^i). \quad (2)$$

При формировании ГМВ-последовательностей на основе выражения (1) необходимо построить расширенное поле $GF(2^m)$, поле с двойным расширением $GF[(2^m)^n]$ и вычислить следы всех элементов в расширенном и простом полях, что определяет значительную вычислительную сложность данной процедуры.

Целью статьи является разработка алгоритма формирования ГМВ-последовательностей, основанного на матричном представлении последовательностей составного периода и использовании структурных свойств проверочных полиномов.

Формирование ГМВ-последовательностей осуществляется на основе М-последовательностей аналогичного периода. Построение МП может быть реализовано с помощью проверочного полинома, определяемого из таблиц неприводимых полиномов [10, 11].

Для наглядности рассмотрим сначала процедуру формирования ГМВП на конкретном примере, а затем приведем формализованную запись алгоритма.

Пусть требуется сформировать ГМВП периода $N = 63$. Формируем МП данного периода. В качестве проверочного полинома выбираем произвольный примитивный полином 6-й степени, например $h_{МП}(x) = x^6 + x + 1$. Для начального состояния 000001 линейного регистра сдвига с обратными связями (ЛРСОС) длины $L = 6$ элементы искомой МП записываются построчно в виде матрицы размерности $[J \times S] = [7 \times 9]$:

$$\mathbf{F}_{МП} = \begin{vmatrix} 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ \mathbf{0} & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \end{vmatrix}. \quad (3)$$

Номера строк в матрице изменяются от нуля до $(J - 1)$, а номера столбцов — от нуля до $(S - 1)$.

Заметим, что столбцы матрицы, за исключением нулевого столбца, состоящего из одних нулей, представляют собой $S - 1 = 8$ некоторых сдвигов М-последовательности периода $J = 7$. Данная последовательность получила название характеристической последовательности (ХП). Последовательность, состоящая из нулей, называется нулевой последовательностью (НП) [12].

Таким образом, можно сделать вывод, что М-последовательность составного периода формируется на основе М-последовательности более короткого периода. НП необходима для выполнения условия сбалансированности МП.

Проверочным полиномом для полученной в рассматриваемом примере ХП периода $J = 7$ является полином $h_{ХП1}(x) = x^3 + x^2 + 1$. Сформируем все сдвиги этой ХП, произвольно выбрав в качестве нулевого сдвига третий столбец матрицы $\mathbf{F}_{МП}$ вида (3) — 0011101 (табл. 1).

В соответствии с табл. 1 определяем номера сдвигов ХП для всех столбцов матрицы (3). Тогда МП периода $N = 63$, записанную в виде матрицы $\mathbf{F}_{МП}$, можно представить как последовательность номеров сдвигов ХП периода $J = 7$ с одним

**Таблица 1. Сдвиги ХП для нулевого сдвига 0011101**

| Номер сдвига | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|---|
| Сдвиг МП | 0011101 | 1001110 | 0100111 | 1010011 | 1101001 | 1110100 | 0111010 |

**Таблица 2. Сдвиги ХП для нулевого сдвига 0010111**

| Номер сдвига | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|---|
| Сдвиг МП | 0010111 | 1001011 | 1100101 | 1110010 | 0111001 | 1011100 | 0101110 |

прочерком для обозначения НП. В результате получим правило формирования (ПФ) в виде вектора из $S = 9$ компонент:

$$\mathbf{I}_{\text{МП}} = \{-, 2, 6, 0, 0, 3, 2, 0, 2\}. \quad (4)$$

На основе полученного ПФ можно синтезировать ГМВ-последовательность. Для этого в качестве ХП необходимо выбрать другую МП периода $J = 7$. Для данного периода существует всего одна такая последовательность с проверочным полиномом $h_{\text{ХП2}}(x) = x^3 + x + 1$. Сформируем все сдвиги данной ХП для нулевого сдвига 0010111 (табл. 2).

ГМВП представляется в виде матрицы, аналогичной матрице (3), при подстановке сдвигов ХП из табл. 2 в соответствии с ПФ (4). Для удобства формирования последовательности данное ПФ приведено над матрицей $\mathbf{F}_{\text{гмв}}$:

$$\mathbf{I}_{\text{мп}} = \{-,\ 2,\ 6,\ 0,\ 0,\ 3,\ 2,\ 0,\ 2\}$$

$$\mathbf{F}_{\text{гмв}} = \begin{vmatrix} 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & \mathbf{0} & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \end{vmatrix}. \quad (5)$$

Возможность формирования ГМВП путем замены ХП в правиле формирования $\mathbf{I}_{\text{МП}}$ для МП можно пояснить следующим образом.

В выражении (1) значение внутренней функции следа $tr_{mn,m}a = tr_{6,3}a$ элемента $a$ поля с двойным расширением $GF[(2^3)^2]$ является элементом расширенного поля $GF(2^3)$. Если $r$ принимает значение больше единицы, то возведение в степень $(tr_{6,3}a)^r$ означает децимацию элементов поля $GF(2^3)$ по индексу $r$. При этом в каждом столбце матрицы (3) также происходит децимация символов ХП по индексу $r$. Если двоичное представление числа $r$ содержит одну единицу (числа 2, 4, 8 и т.д.), то в результате децимации получаем циклический сдвиг МП $\mathbf{F}_{\text{МП1}}$. Если двоичное представление числа $r$ содержит не менее двух единиц (числа 3, 5, 6), то в результате получаем другую «короткую» МП — $\mathbf{F}_{\text{МП2}}$. Таким образом, возведение в степень $r$ в выражении (1) эквивалентно замене в матричном представлении (3) МП $\mathbf{F}_{\text{МП1}}$ на последовательность $\mathbf{F}_{\text{МП2}}$. В результате вместо МП периода $N = 63$ формируется ГМВП.

**Формализованная запись алгоритма формирования ГМВП:**

1. По таблицам неприводимых полиномов выбирается примитивный полином $h_{\text{мп}}(x)$ степени $k = mn$, которая определяется в соответствии с требуемым периодом ГМВП из равенства $N = p^k - 1$.

2. На основании полинома $h_{\text{мп}}(x)$ формируется МП периода $N$, которая записывается в виде матрицы $\mathbf{F}_{\text{МП}}$ размерности $[J \times S]$.

3. Для произвольного ненулевого столбца, являющегося ХП1 в виде МП1 периода $J = 2^m - 1$, определяется проверочный полином $h_{\text{ХП1}}(x)$ степени $m$. Формируются все циклические сдвиги ХП1.

4. Определяются номера сдвигов ХП1 для всех столбцов матрицы $\mathbf{F}_{\text{МП}}$. Данная последовательность номеров сдвигов называется правилом формирования $\mathbf{I}_{\text{МП}}$ и является вектором, содержащим $S$ компонент.

5. По таблицам неприводимых полиномов выбирается примитивный полином $h_{\text{ХП2}}(x)$ степени $m$. Формируются все циклические сдвиги ХП2, являющейся МП2 периода $J = 2^m - 1$.

6. В соответствии с правилом формирования $\mathbf{I}_{\text{МП}}$ в столбцы матрицы $\mathbf{F}_{\text{МП}}$ заносятся требуемые циклические сдвиги ХП2. В результате получается матрица $\mathbf{F}_{\text{ГМВ}}$, в которой искомая ГМВП записана по строкам.

Представленный алгоритм формирования ГМВП может быть использован для построения как двоичных, так и недвоичных последовательностей.

В качестве примера реализации разработанного алгоритма рассмотрим процедуру формирования троичной ГМВП периода $N = 80$.

1. По таблицам неприводимых полиномов [10, 13] над полем характеристики $p = 3$ $GF[(3^2)^2]$ выбираем примитивный полином $h_{\text{МП}}(x) = x^4 + 2x^3 + 2$ степени $k = mn = 4$, которая определяется в соответствии с требуемым периодом ГМВ-последовательности из равенства $N = 80 = 3^k - 1$.

2. На основании полинома $h_{\text{МП}}(x) = x^4 + 2x^3 + 2$ формируем троичную МП периода $N = 80$. Формирование выполняем с помощью рекуррентного выражения для символов МП вида $C_{4+i} = C_{3+i} + C_{0+i}$, $(i = 0, 1, \ldots, 75)$, которое получаем из полинома $h_{\text{МП}}(x)$ [14]. В качестве начального состояния выберем последовательность 0001. Полученную троичную МП записываем в виде матрицы $\mathbf{F}_{\text{МП}}$ размерности $[J \times S] = [8 \times 10]$ последовательно по строкам:

$$\mathbf{F}_{\text{МП}} = \begin{vmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 & 2 & 0 & 1 \\ 2 & 1 & 1 & 2 & 1 & 2 & 0 & 2 & 0 & 2 \\ 2 & 1 & 1 & 0 & 2 & 0 & 1 & 1 & 0 & 0 \\ 1 & 2 & 2 & 2 & 0 & 2 & 1 & 0 & 0 & 2 \\ 0 & 0 & 0 & 2 & 2 & 2 & 2 & 1 & 0 & 2 \\ 1 & 2 & 2 & 1 & \mathbf{2} & 1 & 0 & 1 & 0 & 1 \\ 1 & 2 & 2 & 0 & 1 & 0 & 2 & 2 & 0 & 0 \\ 2 & 1 & 1 & 1 & 0 & 1 & 2 & 0 & 0 & 1 \end{vmatrix}. \quad (6)$$

3. Для произвольного ненулевого столбца, являющегося характеристической последовательностью в виде троичной МП периода $J = 3^m - 1 = 8$, определяем проверочный полином $h_{\text{ХП1}}(x) = x^2 + 2x + 2$ степени $m = 2$. Формируем все циклические сдвиги этой ХП1, в качестве нулевого сдвига выберем нулевой столбец матрицы $\mathbf{F}_{\text{МП}}$ вида (6) (табл. 3).

4. Определяем номера сдвигов ХП1 для всех столбцов матрицы $\mathbf{F}_{\text{МП}}$. МП периода $N = 80$ представляется в виде последовательности номеров сдвигов ХП периода $J = 8$ с одним прочерком для обозначения нулевой последова-

**Таблица 3. Сдвиги ХП для нулевого сдвига 02210112**

| Номер сдвига | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|---|
| Сдвиг МП | 02210112 | 20221011 | 12022101 | 11202210 | 01120221 | 10112022 | 21011202 | 22101120 |

**Таблица 4. Циклические сдвиги ХП 2 для произвольно выбранного нулевого сдвига**

| Номер сдвига | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|---|
| Сдвиг МП | 02110122 | 20211012 | 22021101 | 12202110 | 01220211 | 10122021 | 11012202 | 21101220 |

тельности. В результате получим правило формирования в виде вектора из $S = 10$ компонент:

$$\mathbf{I}_{\text{МП}} = \{0, 4, 4, 2, 3, 2, 5, 7, —, 2\}. \quad (7)$$

5. По таблицам неприводимых полиномов выбираем примитивный полином $h_{\text{ХП2}}(x) = x^2 + x + 2$ степени $m = 2$, отличный от полинома $h_{\text{ХП1}}(x)$. Заметим, что существует всего два примитивных полинома степени 2 над полем $GF(3^2)$. Формируем все циклические сдвиги этой ХП2 для произвольно выбранного нулевого сдвига, например 02110122 (табл. 4).

6. В соответствии с правилом формирования $\mathbf{I}_{\text{МП}}$ вида (7) в столбцы матрицы $\mathbf{F}_{\text{МП}}$ заносим требуемые циклические сдвиги ХП2. В результате получаем матрицу $\mathbf{F}_{\text{ГМВ}}$, в которой искомая ГМВП записана по строкам:

$$\mathbf{F}_{\text{ГМВ}} = \begin{vmatrix} 0 & 0 & 0 & 2 & 1 & 2 & 1 & 2 & 0 & 2 \\ 2 & 1 & 1 & 2 & 2 & 2 & 0 & 1 & 0 & 2 \\ 1 & 2 & 2 & 0 & 2 & 0 & 1 & 1 & 0 & 0 \\ 1 & 2 & 2 & 2 & 0 & 2 & 2 & 0 & 0 & 2 \\ 0 & 0 & 0 & 1 & 2 & 1 & 2 & 1 & 0 & 1 \\ 1 & 2 & 2 & 1 & 1 & 1 & 0 & 2 & 0 & 1 \\ 2 & 1 & 1 & 0 & 1 & 0 & 2 & 2 & 0 & 0 \\ 2 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 \end{vmatrix}. \quad (8)$$

Таким образом, в статье разработан алгоритм формирования как двоичных, так и недвоичных ГМВ-последовательностей.

**Заключение.** Использование ГМВ-последовательностей в качестве скремблирующих последовательностей для применяемых на канальном уровне сигналов позволит значительно повысить безопасность функционирования ИТС, а значит, затруднит как несанкционированный доступ к передаваемой информации, так и возможность информационных атак и «прослушивания» сети.

Данные последовательности, обладая хорошими автокорреляционными свойствами, могут быть использованы также в качестве синхросигналов как в перспективных ИТС, так и в системах мобильной связи стандарта GSM. При этом выигрыш в структурной скрытности по сравнению с применением М-последовательностей, обладающих аналогичными корреляционными свойствами, составляет не менее 3 дБ.

Разработанный алгоритм позволяет существенно уменьшить вычислительную сложность процедуры формирования ГМВП (на 3—6 дБ для двоичных последовательностей периода $N = 63$; 255; и для троичных последовательностей периода $N = 80$), так как при этом отсутствует необходимость производить вычисления в конечных расширенных полях.

*ЛИТЕРАТУРА*


1. IEEE 1609 — Family of Standards for Wireless Access in Vehicular Environments (WAVE). U.S. Department of Transportation (January 9, 2006).
2. **Григорьев В.А., Хворов И.А., Кузнецов В.И., Аксенов В.О.** Применение беспроводных технологий при реализации ИТС // Электросвязь.— 2013.— № 10.
3. Status of Project IEEE 802.11 Task Group p: Wireless Access in Vehicular Environments. IEEE (2004—2010).
4. **Варакин Л.Е.** Системы связи с шумоподобными сигналами.— М.: Радио и связь, 1985.
5. **Ипатов В.П.** Периодические дискретные сигналы с оптимальными корреляционными свойствами.— М.: Радио и связь, 1992.
6. **Свердлик М.Б.** Оптимальные дискретные сигналы.— М.: Сов. радио, 1975.
7. **Блейхут Р.Э.** Быстрые алгоритмы цифровой обработки сигналов / Пер. с англ.— М.: Мир, 1989.
8. **Прокис Дж.** Цифровая связь / Пер. с англ.; Под ред. Д.Д. Кловского.— М.: Радио и связь, 2000.
9. **Скляр Б.** Цифровая связь: теоретические основы и практическое применение / Пер. с англ.; 2-е изд.— М.: Вильямс, 2003.
10. **Питерсон У., Уэлдон Э.** Коды, исправляющие ошибки / Пер. с англ.; Под ред. Р.Л. Добрушина и С.И. Самойленко.— М.: Мир, 1976.
11. **Стародубцев В.Г., Павлов О.А.** Помехоустойчивые коды в телекоммуникационных и информационных системах / Вып. 1. Конечные поля Галуа: элементы теории и практики: учеб. пособие.— СПб.: ВКА им. А.Ф. Можайского, 2003.
12. **Стародубцев В.Г.** Алгоритм формирования и свойства дискретных редецимированных последовательностей для помехозащищенных систем связи // Сб. ст. НТК «Радио- и волоконно-оптическая связь, навигация, локация».— Воронеж, 1997.
13. **Кларк Дж., Кейн Дж.** Кодирование с исправлением ошибок в системах цифровой связи / Пер. с англ.— М.: Радио и связь, 1987.
14. **Блейхут Р.Э.** Теория и практика кодов, контролирующих ошибки / Пер. с англ.— М.: Мир, 1986.


*Получено 31.10.13*