МОДЕЛИРОВАНИЕ СПЕЦИАЛИЗИРОВАННЫХ РАСПРЕДЕЛЕННЫХ СИСТЕМ ОБРАБОТКИ ИНФОРМАЦИИ С ПОВЫШЕННОЙ ПОМЕХОСТОЙЧИВОСТЬЮ

Кравец О.Я., Тупота А.В.

При построении беспроводных вычислительных машин, многопроцессорных и многомашинных систем используется Bluetooth технологии для обеспечения обмена данными между отдельными элементами этих машин и систем.

В Bluetooth-технологии сфокусированы лучшие на сегодняшний день достижения современной микроэлектроники как в области аппаратуры, так и в программном обеспечении. Bluetooth-системы относятся к классу взаимодействующих открытых систем. Bluetooth-устройства физически представляют собой микросхемы, обеспечивающие связь в диапазоне 2,4 ГГц В России к технологии Bluetooth проявляется огромный интерес. Наиболее перспективными являются те области промышленности и народного хозяйства, где требуется сбор и обработка большого количества одновременно измеряемых параметров, например, нефтепромыслы, металлургические заводы, жилищно-коммунальное хозяйство и так далее.

Основополагающим принципом построения систем Bluetooth является использование метода расширения спектра при скачкообразном изменении частоты . Весь выделенный для Bluetooth-радиосвязи частотный диапазон 2,402:2,480 ГГц разбит на 79 частотных каналов. Смена каналов производится по псевдослучайному закону с частотой 1600 Гц.

Несмотря на то, что смена частотных каналов производится по псевдослучайному закону с частотой 1600 Гц, устройства Bluetooth не всегда могут исключить проблемы связанные с воздействием помех в диапазоне 2,4 ГГц. При этом требуется разработка научных подходов, методов и алгоритмов символьной и специальной обработки информации для обеспечения надежности функциональной устойчивости и диагностики функционирования вычислительных машин и систем. Это достигается представлением и обработкой информации в конечном поле Fp, $p>2$ с использованием псевдослучайных последовательностей символов конечного поля для выбора каналов передачи информации устройств Bluetooth.

Для повышения быстродействия процессов обработки и обмена информации между отдельными устройствами машин и систем целесообразно в качестве характеристики конечного поля целесообразно выбрать простые числа $p=2^m+1$, $m\in 2,4,8,16$ [1].

Для того, чтобы получить псевдослучайную последовательность символов конечного поля Fp максимальной длины $N=p^k-1$, где k-целое, большее единицы, необходимо найти примитивный многочлен степени k и по его виду определить структуру регистра сдвига.

Поскольку нахождение примитивных многочленов степени k над полем Fp в общем случае представляет трудноразрешимую на практике задачу, то поступим следующим образом.

В поле F_2 определим структуру регистра сдвига, позволяющего вырабатывать двоичную псевдослучайную последовательность максимальной длины с периодом, равным N, а для того, чтобы на каждом такте работы регистра сдвига иметь не двоичные псевдослучайные числа, а числа соответствующие характеристике выбранного нами поля Fp $(p=2^m+1)$, $m\in 2,4,8,16$ необходимо информацию параллельным кодом снимать одновременно с m ячеек (линий задержки) регистра сдвига.

Порядок считывания информации с выбранных линий задержки регистра сдвига может быть выбран любой. При этом регистр сдвига будет генерировать псевдослучайную последовательность чисел (символов) $\{0,1,\ldots,p-2\}$ с периодом совпадающим с периодом псевдослучайной последовательности двоичных чисел.

В псевдослучайной последовательности символов конечного поля Fp, точно также как в псевдослучайной последовательности двоичных чисел, в пределах своего периода отсутствуют скрытые периодичности и обеспечивается статистическая равномерность используемых символов.

Поскольку псевдослучайные символы конечного поля Fp могут сниматься с различных ячеек (линий задержки) регистра сдвига и в разной последовательности, то могут использоваться различные псевдослучайные последовательности символов конечного поля, причём каждая из них будет нелинейной, так как не воспроизводит один символ конечного поля, равный $p-1$ и не будет являться циклически сдвинутой относительно других псевдослучайных последовательностей символов.

Для обеспечения функциональной устойчивости и надежности систем в условиях индустриальных и взаимных помех должна быть также сформирована перебирающая последовательность символов конечного поля. Сформированная перебирающая последовательность является последовательностью символов мультипликативной группы конечного поля Fp $\{1,2,\ldots,p-1\}$. Использование двух последовательностей позволяет формировать в поле Fp функцию для символьной обработки исходного текста α, включающую операцию умножение по модулю p символа исходного текста на символ перебирающей последовательности и операцию сложения по модулю p полученного результата с символом псевдослучайной последовательности.

Поскольку символы перебирающей последовательности x являются элементами мультипликативной группы конечного поля Fp, то могут быть вычислены обратные величины

$$x^{-1}\equiv x^{p-2}(\mathrm{mod}\ p),$$

а для символов псевдослучайной последовательности y, которые составляют аддитивную группу конечного поля Fp, могут быть вычислены сопряжённые элементы

$$y^*=p-y,$$

которые позволяют реализовать обратные преобразования в конечном поле Fp и восстановления символов исходного текста

$$(\beta+y^*)x^{-1}\equiv\alpha\ (\mathrm{mod}\ p).$$

Так как в преобразованиях в конечном поле используется две нелинейные последовательности символов конечного поля Fp, то обеспечивается функ-

циональная устойчивость системы в условиях промышленных и взаимных помех при обмене информации между её элементами.

Если одна ошибка произойдет на интервале, соответствующем смене порождающих элементов перебирающей последовательности, то такая ошибка будет обнаружена и скорректирована. Для этого на передающей стороне формируется суммарный символ исходного текста в виде двоичного вектора путем сложения в конечном поле *Fp*, символа исходного текста со всеми предыдущими символами исходного текста, аналогично вычисляется суммарный символ преобразованного текста, меняется порождающий элемент перебирающей последовательности при появлении в ее составе символа 1 на символ суммарного исходного текста. При этом суммарные символы исходного и преобразованного текста передаются по линии связи, а на приемной стороне корректируется искаженные символы. Для этого:

-вычисляют расхождение $\Delta\alpha$ в суммарных символах переданного исходного текста $C\alpha$ и вычисленного $C^*\alpha$ на приемной стороне

$$\Delta\alpha \equiv C_\alpha - C_\alpha^* (\mathrm{mod}\ p)$$

- вычисляют расхождение $\Delta\beta$ в суммарных символах переданного преобразованного текста C_β и вычисленного C^*_β на приемной стороне

$$\Delta\beta \equiv C_\beta - C_\beta^* (\mathrm{mod}\ p)$$

- вычисляют символ перебирающей последовательности, используемый для корректировки искаженного при приеме символа

$$x \equiv \Delta\beta \cdot \Delta\alpha^{-1} (\mathrm{mod}\ p)$$

где $\Delta\alpha^{-1} \equiv (\Delta\alpha)^{p-2} (mod\ p)$ - обратный элемент по отношению к символу $\Delta\alpha$ в поле *Fp*;

- корректируют искаженный символ исходного текста по формуле

$$\alpha \equiv \alpha + \Delta\alpha (mod\ p)$$

Возможность обнаружения и корректировки символов исходного текста на приемной стороне приводит к повышению помехоустойчивости передаваемой информации.

Формирование символов *x* перебирающей последовательности в виде двоичных векторов на каждом такте работы регистра сдвига можно осуществить за счет вычисления порожденных элементов конечного поля *Fp* путем умножения предыдущего символа этой последовательности на порождающий элемент x_n:

$$x_i \equiv x_{i-1} x_n (mod\ p).$$

Если в процессе вычислений на каком-то *i*-ом такте работы регистра сдвига окажется, что $x=1$, то в этом случае меняется порождающий элемент x_n поля *Fp*. При этом в качестве нового порождающего элемента x_n принимается сформированный на данном такте работы регистра сдвига суммарный символ исходного текста C_α конечного поля *Fp*, $x_n = C_\alpha$, если $C_\alpha < 2$, то $x_n = 2$.

Сформированные последовательности конечного поля *Fp* используются символьного преобразования потока данных:

$$\alpha \cdot x + y \equiv \beta (mod\ p)$$

Так как в перебирающей последовательности конечного поля элементы формируются за счёт возведения в степень порождающего элемента x_n, имеющего порядок *k*, то все элементы $x_n, x_n^2, x_n^3, \ldots, x_n^k$ будут различны на интервале *k* тактов работы регистра сдвига. В силу того, что порождающие элементы x_n могут быть разного порядка в конечном поле *Fp*, то смена порождающих элементов будет осуществляться по псевдослучайному закону. При этом обеспечивается статистическая равномерность символов преобразованного текста на интервале, равном *p-1* тактов работы регистра сдвига, что обеспечивает равномерное использование каналов устройств Bluetooth.

Поскольку для данной символьной обработки информации ошибки в отдельных каналов устройства Bluetooth могут быть обнаружены и исправлены, то обеспечивается контроль функционирования системы и своевременная смена каналов устройства Bluetooth, подверженных сильным индустриальным и взаимным помехам. В этом случае повышается скорость передачи информации между отдельными устройствами, так как исключается её повторная передача при возникновении ошибки в отдельных каналах передачи информации.

СПИСОК ЛИТЕРАТУРЫ

1. Тупота В.И. Адаптивные средства защиты информации в вычислительных сетях // Радио и связь. – М., 2002. -176 с.

СРЕДСТВА ПОЛУНАТУРНОЙ ВЕРИФИКАЦИИ АЛГОРИТМОВ ФУНКЦИОНИРОВАНИЯ СИСТЕМЫ УПРАВЛЕНИЯ

Кравец О.Я., Севидов В.В.
Международный университет компьютерных технологий

Полунатурное моделирование целесообразно применять в ситуации, когда необходимо осуществить верификацию - проверить правильность самого процесса управления. Аналитических и имитационных средств для решения задачи верификации, как правило, недостаточно вследствие наличия значительных нестационарностей в процессе функционирования системы.

Одна из задач, поставленных в работе, сформулирована следующим образом: создать средства, обеспечивающие верификацию сформированного варианта управления методами полунатурного моделирования, позволяющими учесть факторы нестационарности. Рассмотрим методы решения поставленной задачи на примере системы управления (СУ) автоматизированной транспортно-складской системой (АТСС) интегрированного производства (ИП).

Основное внимание будет уделено вопросам моделирования системы управления автоматизированной транспортно-складской системы ИП на базе ЛВС. Решение проблемы адекватного моделирования СУ АТСС ИП позволяет получить достаточную гибкость производства при условии синхронизации информационных и материальных потоков. В сложном кон-