УДК 681.518.22

МЕТОД СИНХРОНИЗАЦИИ ПРОСТРАНСТВЕННО РАЗНЕСЕННЫХ УСТРОЙСТВ В СИСТЕМЕ ГЕНЕРАЦИИ И РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ ШИФРОВАНИЯ

А.В. Карпов, А.Д. Смоляков, И.Р. Лапшина, А.А. Галиев

Рассматривается система генерации и распределения ключей шифрования, в которой секретные ключи не передаются, а формируются в процессе измерений фазы сигнала. В статье описан метод беспроводной синхронизации пространственно разнесенных устройств системы генерации и распределения ключей, который учитывает параметры кратковременной и долговременной нестабильности частот опорных генераторов. Показано что частоты и фазы опорных генераторов можно свести с высокой точностью путем обмена тестовыми зондирующими сигналами между устройствами.

Ключевые слова: ключ шифрования, измерение, фаза сигнала, стандарт частоты, частотная нестабильность, фазовая расстройка стандартов, синхронизация.

АКТУАЛЬНОСТЬ

В настоящее время интенсивно развиваются физические методы получения ключевых последовательностей для решения задач шифрования с целью безопасной передачи данных. Одним из таких методов является получение ключей шифрования на основе использования свойств многолучевого радиоканала способом, предложенным в [1–3]. Взаимность многолучевого радиоканала позволяет сформировать идентичные ключи для обоих абонентов, находящихся на концах радиолинии [4].

Для реализации такого метода генерации ключей была разработана система, осуществляющая измерение фазы сигналов во встречном режиме и формирование ключей шифрования из полученных фазовых отсчетов, представленная в работе [5]. В материалах [6] представлены результаты экспериментов по получению случайных последовательностей при многолучевом распространении радиоволн в условиях городской застройки.

Идентичность фазовременных характеристик (ФВХ), которые устройства получают в результате встречного обмена зондирующими сигналами, напрямую зависит от точности синхронизации устройств между собой. Поэтому чем выше точность синхронизации опорных генераторов, тем более высокую скорость генерации ключей можно получить.

Основные принципы организации средств синхронизации в системе были изложены в работе [7], где описывался протокол беспроводной синхронизации с использованием в качестве единого тактового синхросигнала сигнала с выхода 1PPS приемника GPS/ГЛОНАСС [8]. Относительная кратковременная нестабильность данного сигнала (СКО = $1*10^{-9}$) хуже, чем у стандарта частоты FS725 [9] (СКО = $2*10^{-11}$), поэтому подстройка по внешнему сигналу 1 Гц осуществляется не менее 12 часов. Возникает необходимость провести начальную синхронизацию за приемлемое для возможного сеанса связи время. Кроме того, из-за значительной кратковременной нестабильности частоты опорного генератора за одну секунду,ошибка измерения фазы сигнала уже через 10 секунд после подстройки может достигнуть 130 градусов. Поэтому даже если частоты опорных генераторов сведены идеально, влияние нестабильности частоты опорного генератора на измерения фазы остается очень сильным, при этом ошибка измерения фазы растет со временем. Чтобы скомпенсировать отклонение частоты опорного генератора, необходимо контролировать в реальном времени погрешность измерения фазы и, при необходимости, подстраивать фазы тактовых сигналов, которые формирует блок синхронизации [10].

Целью данной работы является разработка методики синхронизации пространственно разнесенных устройств системы генерации и распределения ключей шифрования (СГРКШ). Для этого необходимо:

- Получить аналитическое выражение связывающее отклонение частоты опорных генераторов с измеряемой фазой зондирующего сигнала;
- Разработать алгоритм сведения частот опорных генераторов;
- Разработать алгоритм автоматической подстройки фазы.

ОПИСАНИЕ СИСТЕМЫ

На рисунке 1 представлена блок схема системы генерации и распределения ключей шифрования (СГРКШ). Она состоит из двух устройств (У1 и У2) приема и передачи зондирующих радиосигналов через многолучевой радиоканал, к которым подключены стандарты частоты FS725 и компьютер с установленной управляющей программой. К каждому стандарту частоты подключен GPS приемник, который обеспечивает начальную синхронизацию разнесенных в пространстве устройств.

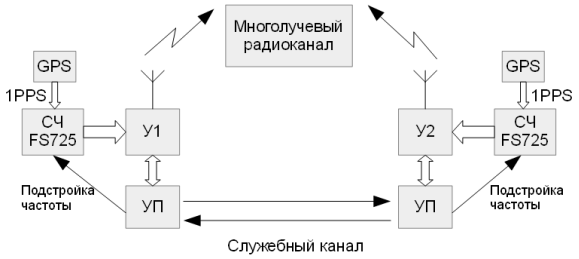

Рисунок 1 – Блок схема СГРКШ

Для обмена данными между устройствами используется дополнительный служебный канал передачи данных (internet). Работа системы начинается с этапа начальной синхронизации стандартов частоты по сигналам точного времени от подключенных к ним приемников GPS. После чего происходит тестовый обмен ЗС для корректировки начальных фаз опорных генераторов. На следующем этапе устройства переходят в режим обмена ЗС для измерения их фазы. Накопленные измерения поступают в управляющую программу, которая сначала производит процедуру «чистки» выборки по набору критериев: отношение сигнал/шум ЗС; коэффициент автокорреляции. Затем происходит создание ключей шифрования и сверка их между устройствами.

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ СИНХРОНИЗАЦИИ В СГРКШ

Для того чтобы получить выражения связывающие отклонение частоты опорных генераторов с измеряемой фазой зондирующего сигнала (ЗС), необходимо подробно рассмотреть процесс формирования и приема ЗС устройствами СГРКШ.

На рисунке 2 представлена блок-схема формирования зондирующего сигнала передатчика. С выхода опорного генератора сигнал поступает на вход синтезатора частот, который формирует сигнал несущей частоты с полной фазой:

$$\Phi_{сч1} = N_{tr} * (t * (\omega_{ог1} + \Delta\omega_{ог1}) + \varphi_{ог1}), \quad (1)$$

где N_{tr} – коэффициент умножения частоты.

Далее сигнал подается на модулятор, на выходе которого формируется передаваемый радиоимпульс, который излучается, пройдя через антенный коммутатор и антенну.

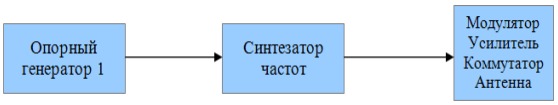

Рисунок 2 – Формирование зондирующего сигнала в устройстве 1

Приемник устройства 2 принимает зондирующий сигнал (рисунок 3) с полной фазой. Сигнал переносится на промежуточную частоту с помощью смесителя. Фазометр измеряет разность фаз между сигналом промежуточной частоты $\Phi_{пч2}$ и сигналом от опорного генератора.

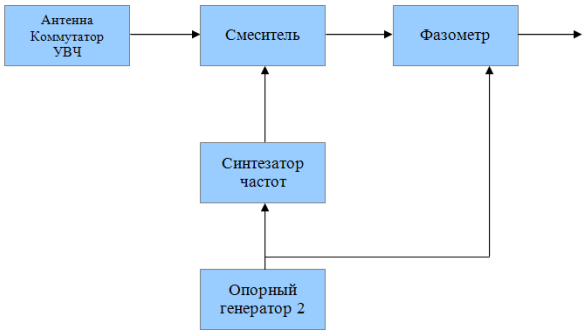

Рисунок 3 – Измерение фазы принятого сигнала в устройстве 2

На выходе фазометра 2-го устройства будет сигнал с полной фазой:

$$\Phi_{фм2} = 90 * t * (\omega_{ог2} - \omega_{ог1}) + 90 * t * (\Delta\omega_{ог2} - \Delta\omega_{ог1}) + 90 * (\varphi_{ог2} - \varphi_{ог1}) - \varphi_{канал12} \quad (2)$$

где:

$\omega_{\text{ог}1}$ – частота сигнала с выхода опорного генератора 1-го устройства;

$\Delta\omega_{\text{ог}1}$ – нестабильность частоты опорного генератора 1-го устройства;

$\omega_{\text{ог}2}$ – частота сигнала с выхода опорного генератора 2-го устройства;

$\Delta\omega_{\text{ог}2}$ – нестабильность частоты опорного генератора 2-го устройства;

t – время;

$\varphi_{\text{ог}1}$ – начальная фаза сигнала опорного генератора 1- го устройства;

$\varphi_{\text{ог}2}$ – начальная фаза сигнала опорного генератора 2-го устройства;

$\varphi_{\text{канал}12}$ – набег фазы при распространении радиосигнала от 2-го устройства к 1-у устройству;

На выходе фазометра 1-го устройства будет аналогичный сигнал:

$$\Phi_{фм1} = 90 * t * (\omega_{ог1} - \omega_{ог2}) + 90 * t * (\Delta\omega_{ог1} - \Delta\omega_{ог2}) + 90 * (\varphi_{ог1} - \varphi_{ог2}) - \varphi_{канал21} \quad (3)$$

Анализ выражений (2) и (3) показывает, что измерения разности фаз зависят не только от $\varphi_{\text{канал}12}$, $\varphi_{\text{канал}21}$, которые, при условии взаимности канала, будут равны, но и от параметров опорных генераторов. Нужно отметить, что нельзя свести частоты двух опорных генераторов точнее, чем величина кратковременной нестабильности частоты. Так как в выражениях (2) и (3) входит время, то со временем фазовая невзаимность будет нарастать и из-за влияния кратковременной нестабильности случайно отклоняться. Например, подставив в формулу (2) значение относительной нестабильности частоты опорного генератора FS725 равным 10^{-11} за одну секунду, получим, что за это же время измерения фаз, полученные устройствами 1 и 2, могут отличаться не более чем на 13 градусов.

Таким образом, алгоритм сверки шкал времени должен состоять из двух этапов:

1. Сведение частот опорных генераторов;
2. Периодическая подстройка фаз опорных генераторов.

АЛГОРИТМ СВЕДЕНИЯ ЧАСТОТ ОПОРНЫХ ГЕНЕРАТОРОВ

Полная фаза принятого сигнала при $\Delta\omega_{ог1} = \Delta\omega_{ог2} = 0$:

$$\Phi_{\Delta\varphi} = 90 * t * (\omega_{ог1} - \omega_{ог2}) - \varphi_{канал21}. \quad (4)$$

Пренебрегая влиянием канала, получаем:

$$(\omega_{ог1} - \omega_{ог2}) = \frac{\Phi_{\Delta\varphi}}{90*\text{t}}. \quad (5)$$

Так как ФВХ представляет собой последовательность измерений фазы с периодом снятия измерений $t_{изм}$, и длиной последовательности N, то разность отклонения частот опорных генераторов будет равна:

$$\Delta\text{f} = \frac{1}{90*\text{t}_{изм}*\text{n}}, \quad (6)$$

где n – число отсчетов, в течение которых фаза изменилась на 2π.

Для вычисления Δf проводятся тестовые сеансы обмена зондирующими сигналами между синхронизируемыми устройствами. После завершения сеанса зондирования устройства получают ФВХ радиоканала в отсчетах. Эти измерения поступают на модуль быстрого преобразования Фурье, а после него в виде массива амплитуд гармоник подаются в функцию поиска гармоники максимальной амплитуды. Номер отсчета гармоники будет прямо пропорционален Δf. Далее для компенсации сдвига частоты ОГ величина Δf поступает по COM-порту на стандарт частоты FS725.

АЛГОРИТМ АВТОМАТИЧЕСКОЙ ПОДСТРОЙКИ ФАЗЫ ОПОРНОГО ГЕНЕРАТОРА

После каждого тестового сеанса зондирования 2-ое устройство пересылает по служебному каналу все измерения фазы 1-му устройству, которое сравнивает их со своими измерениями фазы. По результатам сравнения 1-ое устройство корректирует начальную фазу своего опорного генератора. Тестовые сеансы зондирования повторяются до тех пор, пока невзаимность измерений фазы не станет меньше заданного порога. Не все измерения фазы используются для подстройки, так как отношение сигнал/шум в реальных условиях постоянно меняется, а значит и меняется погрешность оценки фазы.

ВЛИЯНИЕ ШУМОВ КАНАЛА НА ОШИБКУ СИНХРОНИЗАЦИИ

В любом канале действуют шумы и помехи. В приемопередатчиках существуют помехи, наведенные на вход усилителей, а также внутренние шумы электронных компонентов и тепловые шумы антенн.

Уровень шума на входе приемника в общем случае складывается из помех на канале N(t) и шумов аппаратуры $U_{app_{noise}}(t)$:

$$U_{noise}(t) = N(t) + U_{app_{noise}}(t). \quad (7)$$

На практике уровень шумов на входе в любой момент времени остается почти постоянным. Изменяется уровень сигнала передатчика. При различных значениях отношения «сигнал-шум» SNR на входе приемника получаем различную фазовую ошибку подстройки стандартов частоты.

На рисунке 4 приведена экспериментально полученная зависимость фазовой ошибки от SNR.

Анализируя полученную зависимость, приходим к выводу, что начиная с SNR = 35 дБ, можно добиться того, что максимальная фазовая ошибка синхронизации опорных генераторов будет около 2 градусов, то есть только аппаратурные шумы будут влиять на полученную фазовую ошибку.

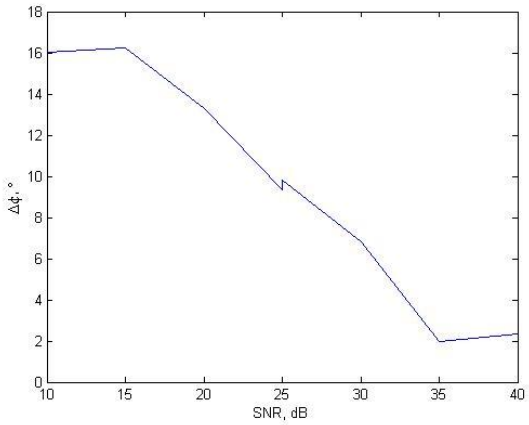

Рисунок 4 – Ошибка измерения фазы от отношения «сигнал-шум»

НЕОБХОДИМАЯ ПЕРИОДИЧНОСТЬ СЕАНСОВ СИНХРОНИЗАЦИИ

На рисунке 5 показано как меняется количество бит ключа шифрования, которые можно получить от одного измерения фазы ЗС в зависимости от величины расстройки частоты опорных генераторов и от длительности наблюдений.

Зависимость получена при условии, что кратковременная нестабильность частоты опорного генератора (рубидиевый стандарт частоты FS725) составляет $2*10^{-11}$ за одну секунду и в начальный момент времени сдвиг фаз между сигналами опорных генераторов отсутствует, а уровень шума равен нулю.

Из графика видно, что с увеличением расстройки частоты и длительности работы устройств количество полученных бит ключевой последовательности уменьшается. Уменьшение количества бит, получаемой из одного измерения, объясняется прогрессирующей неидентичностью ФВХ из-за влияния нестабильности частоты ОГ. Необходимо отметить что, как бы точно мы не свели частоты ОГ, скорость генерации ключей со временем уменьшится до нуля. Поэтому требуется периодически повторять сеансы обмена тестовыми ЗС для того чтобы по измерениям ФВХ оценить ошибку измерения фазы ЗС и при необходимости скорректировать её. По графику можно определить через какое время нужно повторять сеанс синхронизации. Стандарт частоты FS725 позволяет корректировать выходную частоту сигнала с шагом 10^{-5} Гц с управлением через COM-порт, поэтому на практике выходные частоты двух стандартов частоты можно свести с точностью близкой к 10^{-5} Гц. Если минимальное количество бит информации принять равным 1 бит от одного измерения фазы, тогда сеанс синхронизации нужно повторять каждые 10 секунд.

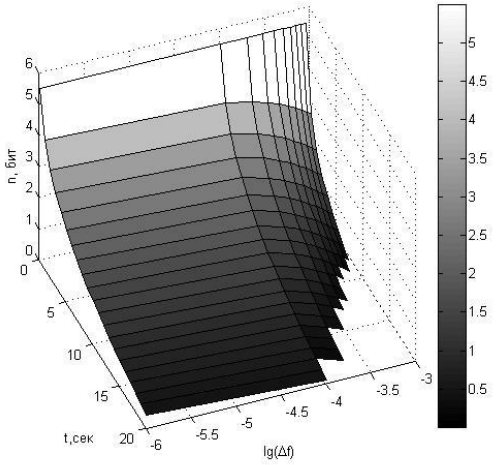

Рисунок 5 – График, показывающий количество бит информации, получаемых от одного измерения, в зависимости от расстройки стандартов частоты и длительности наблюдений

ВЫВОДЫ

Создана математическая модель синхронизации системы генерации и распределения ключей, на основе которой определены условия уменьшения фазовой ошибки. Разработаны и реализованы методы начальной синхронизации и фазовой автоподстройки частоты стандартов. Дана оценка влияния шума на канале на точность синхронизации. Получена экспериментальная зависимость скорости генерации ключей от времени и расстройки частоты. Показано, что для стандарта частоты FS725 сеанс синхронизации нужно повторять каждые 10 секунд.

СПИСОК ЛИТЕРАТУРЫ

1. Джейкс, У. К. Связь с подвижными объектами в диапазоне СВЧ / У. К. Джейкс. – М. : Связь, 1979, – 384 с.

2. Пат. 2423800 Российская Федерация, МПК H 04 L 9/18. Способ защиты информации / Сидоров В. В., Шерстюков О. Н., Сулимов А. И. ; патентообладатель Федеральное государственное автономное образовательное учреждение высшего профессионального образования «Казанский (Приволжский) федеральный университет» (RU). – № 2008152523/09 ; заявл. 29.12.2008 ; опубл. 10.07.2011, Бюл. № 19. – 9 с.

3. Пат. 2527734 Российская Федерация, МПК H 04 L 9/00. Способ защиты информации / Сулимов А. И., Шерстюков О. Н., Карпов А. В., Каю-

мов И. Р., Смоляков А. Д. ; патентообладатель Общество с ограниченной ответственностью "Научно-производственное предприятие "СэйвТелеком" (ООО "НПП "СэйвТелеком") (RU). – № 2012112893/08 ; заявл. 04.04.2012 ; опубл. 10.09.2014, Бюл. № 25. – 11 с.

4. Madiseh, M. G. Verification of secret key generation from UWB channel observations / M. G. Madiseh, S. He, M. L. McGuire, S. W. Neville, X. Dong // Proc. of the IEEE Int. Conf. on Comm. (ICC'09). – 2009. – P. 593–597.

5. Карпов, А. В. Разработка макета устройства динамической генерации ключей шифрования для криптографической системы связи / А. В. Карпов, И. Р. Каюмов, А. Д. Смоляков // Ползуновский вестник. – 2011. – № 3. – С. 210–213.

6. Smolyakov, A. D. Experimental verification of possibility of secret encryption keys distribution with a phase method in a multipath environment / A. D. Smolyakov, A. I. Sulimov, A. V. Karpov, O. N. Sherstyukov // Proceedings of X International IEEE Siberian Conference on Control and Communications (SIBCON-2013). – Krasnoyarsk, Russia. – 2013. – P. 1–5.

7. Карпов, А. В. Беспроводная синхронизация устройств системы генерации секретных ключей в многолучевом радиоканале / А. В. Карпов, Р. Р. Фатыхов, А. Д. Смоляков // Ползуновский вестник. – 2014. – №. 2-1. – С. 238–241.

8. GPS-приемник TrimbleR3. Руководство пользователя // Версия 1.00. – Редакция А. – 2005 г. – 133 с. URL: - http://www.stp-rus.com/wp-content/uploads/2015/Documents/GPS%20Trimble%20R3.pdf.

9. FS725 Rubidium frequency standard. Operation and service manual / Stanford Research Systems // Version 1.3 – 2005. – 115 p. URL: http://www.thinksrs.com/downloads/PDFs/Manuals/FS725m.pdf.

10. Карпов, А. В. Разработка средств синхронизации устройств в системе генерации и распределения ключей в многолучевом радиоканале / А. В. Карпов, А. Д. Смоляков, И. Р. Туктарова, А. А. Галиев // Измерение, контроль, информатизация : сборник международной научно-практической конференции. – Барнаул : Изд-во АлтГТУ, 2015. – Т. 2. – С. 200–203.

***Карпов А.В.**, д.ф.-м.н., профессор кафедры радиофизики Института Физики Казанского Федерального Университета, e-mail: Arcadi.Karpov@kpfu.ru.*

***Смоляков А.Д.**, ассистент кафедры радиофизики Института Физики Казанского Федерального Университета, e-mail: alex9975@gmail.com.*

***Лапшина И.Р.**, ассистент кафедры радиофизики Института Физики Казанского Федерального Университета, e-mail: rica1991@mail.ru.*

***Галиев А.А.**, магистрант кафедры радиофизики Института Физики Казанского Федерального Университета, e-mail: ggalievv@mail.ru.*