

УДК 621.396

UDC 621.396

05.13.19 - Методы и системы защиты информации, информационная безопасность (технические науки)

05.13.19 - Methods and systems of information protection, information security (technical sciences)

**МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ
СИНХРОНИЗАЦИИ ДАТЧИКОВ ПСП НА
КАНАЛАХ НИЗКОГО КАЧЕСТВА**

**MATHEMATICAL MODELING OF PSP
SENSOR SYNCHRONIZATION ON LOW
QUALITY CHANNELS**

Ажмухамедов И.М.
д.т.н., профессор, заведующий кафедрой
информационной безопасности
*Астраханский государственный университет, г.
Астрахань, Россия*

Azhmukhamedov I.M.
Doctor of Technical Sciences, Professor, Head of
Information Security Department
Astrakhan state university, Astrakhan, Russia

Мельников Е.В.
соискатель
*Кубанский институт информзащиты, г.
Краснодар, Россия*

Melnikov E.V.
Applicant for degree
*Kuban Institute of Information Protection, Krasnodar,
Russia*

Целью данной работы является нахождение
граничной оценки синхронизации датчиков ПСП в
каналах низкого качества по методу зачетного
отрезка (ЗОТ), не зависящей от распределения
ошибок в канале

The purpose of this work is to find the boundary
estimate of the synchronization of PSP sensors in low-
quality channels according to the method of the test
segment (OST), independent of the distribution of
errors in the channel

Ключевые слова: СИНХРОНИЗАЦИЯ;
ПСЕВДОСЛУЧАЙНАЯ
ПОСЛЕДОВАТЕЛЬНОСТЬ; СИСТЕМЫ
СПЕЦИАЛЬНОЙ СВЯЗИ

Keywords: SYNCHRONIZATION; PSEUDO-
RANDOM SEQUENCE; SPECIAL
COMMUNICATION SYSTEMS

DOI: <http://dx.doi.org/10.21515/1990-4665-154-003>

Введение

Точные оценки вероятности синхронизации псевдослучайной последовательности (ПСП) в нестационарных каналах низкого качества затруднена из-за необозримого усложнения расчетов для достаточно больших периодов ПСП [1,2,3,4,5,6]. Известны приближенные оценки синхронизации ПСП для каналов с заданными законами распределения ошибок, которые не всегда удовлетворяют разработчиков специальных систем связи [3,4,5,6]. В данной работе находится граничная оценка синхронизации ПСП в каналах низкого качества по методу зачетного отрезка (ЗОТ), независящая от распределения ошибок в канале.

Постановка задачи

Передаваемый сигнал – зачетный отрезок, состоящий из " n " двоичных символов.

Условие на канал связи - канал биномиальный, двоичный с вероятностью ошибки символа P ; тактовая синхронизация имеется, а цикловая отсутствует, то есть неизвестно какому номеру символа ЗОТ соответствуют, принимаемые символы, однако, известно, что обработка символов на приеме начинается не позднее, чем придет первый символ ЗОТ.

Ограничение на сложность устройства обработки - на каждом такте работы можно запомнить не более, чем " n " принимаемых двоичных символов или результат их обработки (допустимы различные случаи: $n=n$, $n>n$ и $n<n$).

Задача обработки - приняв L символов канала вынести решение о расположении ЗОТ относительно принимаемых символов, т.е. определить в итоге начало (или конец) ЗОТ.

Критерий качества обработки - вероятность правильного приема ЗОТ (P_{mn}).

Формально эта задача сводится к следующему: Принято L двоичных символов $u_1 u_2 \dots u_L$ и известна длина ЗОТ из n двоичных символов $S_1 S_2 \dots S_n$. Требуется определить положение истинного ЗОТ относительно последовательности $u_1 u_2 \dots u_L$, если известно, что весь ЗОТ входит в последовательность $u_1 u_2 \dots u_L$.

Для определения правила решения, обеспечивающего необходимую вероятность правильной синхронизации требуется знать функцию распределения различных положений ЗОТ. Если она равномерная или неизвестна, то очевидно оптимальным будет правило максимального правдоподобия, т.е. для каждого из $L-n$ допустимых сдвигов мы вычисляем

апостериорную вероятность того, что он соответствует истинному сдвигу и выбираем тот сдвиг, для которого эта вероятность максимальна.

Для того, чтобы ускорить процесс принятия решения, на каждом шаге необходимо производить сравнение с порогом и если он превышен, то сразу принимать решение о принятии ЗОТ. При хорошем соотношении параметров, появление двух и более превышений порога маловероятно и такой метод будет близок к оптимальному. Найдем вероятность неприема ЗОТ с использованием граничных оценок Бернштейна и Буля-Бонферрони.

Нахождение граничной оценки вероятности неприема ПСП на каналах низкого качества

Преимуществом границы Бернштейна состоит в том, что вероятность превышения порога взаимно-корреляционной функции экспоненциально зависит от числа слагаемых n или другими словами от длины ЗОТ. Кроме того, для применения этих границ требуется малая априорная информация [7]. Нет необходимости знать законы распределения, а достаточно знать лишь дисперсию и среднее значение СВ. Применим разработанное выше неравенство Бернштейна и границу Буля-Бонферрони для определения вероятности неприема ЗОТ в биномиальных каналах низкого качества.

Известно, что для случайной величины (СВ) ξ с нулевым математическим ожиданием и одинаковыми дисперсиями: $a_i=0$, $b_i=\sigma^2$ неравенства Бернштейна имеют вид [7]:

$$P\left\{\sum_{i=1}^n \xi_i \geq 2t\sigma\sqrt{n}\right\} < e^{-t^2},$$
$$P\left\{\sum_{i=1}^n \xi_i \leq -2t\sigma\sqrt{n}\right\} < e^{-t^2},$$
$$P\left\{\left|\sum_{i=1}^n \xi_i\right| \geq 2t\sigma\sqrt{n}\right\} < 2e^{-t^2},$$

где: $0 < t < \frac{\sigma\sqrt{n}}{2H}$,

$H > 0$ – для которого справедливо: $M\{\xi_i^k\} \leq \frac{\sigma^2}{2} H^{k-2} \cdot k!$, $k = 2, 3, \dots$.

Неравенство Бернштейна справедливы для любых случайных величин ξ_i , если для них математическое ожидание: $M\{e^{\gamma\xi_i}\} < \infty$, при $|\gamma| < \frac{1}{2H}$.

Из полученных неравенств видно, что если СВ ограничены $|\xi_i| < C - \text{const}$, $i = 1, 2, 3, \dots, n$, то неравенство Бернштейна можно использовать для любых t . Большинство физических величин всегда ограничены и даже если для них используются модели неограниченных величин (гауссовское распределение), то для самих случайных величин, а не моделей неравенства Бернштейна будут справедливы.

Используя неравенство Бернштейна и аддитивной границы Буля–Бонферрони, была получена оценка вероятности неприема пускового ПСП, приведенная ниже:

$$\bar{P}_n = (L - 2n) \left(e^{\frac{-[2P-1]^2}{4(4P(1-P)+1)}} + e^{\frac{-[(1-2P)(n+R(T))]^2}{16P(1-2P)(4d(T)+T)n}} \right), \tag{1}$$

где:

L - длина анализируемого участка ПСП;

n – длина ЗОТ;

$R(T)$ – аперидическая функция взаимной корреляции;

$d(T)$ -число несовпадений пускового и опорного сигналов на участке их взаимного пересечения, определяемое как:

$$d(T) = \begin{cases} 0 & \text{при } T=0; \\ \sum_{i=1}^{n-T} S_i \oplus S_{i+T} & \text{при } T=1, 2, \dots, n-1; \end{cases}$$

Разработанная математическая модель (1) на основе неравенств Бернштейна и аддитивной границы Буля-Бонферрони позволяет, в отличие от известных приближенных методов, получить строгую оценку вероятности синхронизации ПСП при любых как угодно больших периодах, используемых в специальных системах связи для защиты от организованных помех. В связи с этим, разработанная математическая модель, позволит за счет эффективных методов оценки синхронизации ПСП в каналах низкого качества ($P \geq 0.1$) повысить эксплуатационную надежность проектируемых специальных систем связи, что имеет важное значение при построении инновационных сетевых принципов управления в особых условиях мощных организованных помех.

Заключение

Полученная формула (1) достаточно удобная для расчетов. Сравнительный анализ проведенных расчетов показывает, что при одинаковых параметрах канала и длины ЗОТ разработанная математическая модель с использованием неравенств Бернштейна и аддитивной границы Буля-Бонферрони дает выигрыш в помехоустойчивости, по сравнению известными методами, в каналах низкого качества более чем на 1 порядок.

Использованная литература

1. Хисамов Ф.Г. Проблемы применения псевдослучайных последовательностей в системах защиты информации Известия Таганрогского радиотехнического университета \ №2, 2003 г., С.201-205
2. Лосев В.В. Методы синхронизации по задержке (обзор)./ Радиотехника и электроника, 1979, т.ХХII, №1, сс.49-61
3. Скворцов В.С. К вопросу о вероятности неприема комбинации сигнала синхронного запуска./ Радиотехника, 1969, т.24, №10, сс.37-45.
4. Финк Л.М. Теория передачи дискретных сообщений. - М.: Сов. радио, 1970. - 728с.

5. Золотуев А. Д. Подоптимальный метод синхронизации ПСП для когнитивных систем специальной связи, Перспективы развития информационных технологий: сборник материалов XXV Международной научно-практической конференции / Под общ.ред. С.С. Чернова. – Новосибирск: Издательство ЦРНС, 2015. – с. 54-62

6. Khisamov F., Zolotuev A., Sobachkin D., Bobilev M., Simulink Modelling of the Majority Pseudo-noise Sequence Acquisition Method for Multi-Carrier CDMA // International Conference on Innovative Trends in Electronics Communication and Applications, India, с. 138-142

7. Бернштейн С. Н., в кн.: Собр. соч., т. 2, М., 1954, с. 130-40.

References

1. Xisamov F.G. Problemy` primeneniya psevdosluchajny`x posledovatel`nostej v sistemax zashhity` informacii Izvestiya Taganrogskogo radiotexnicheskogo universiteta \ №2, 2003 g., S.201-205

2. Losev V.V. Metody` sinxronizacii po zaderzhke (obzor)./ Radiotexnika i e`lektronika, 1979, t.XXII, №1, cc.49-61

3. Skvorczov V.S. K voprosu o veroyatnosti nepriema kombinacii signala sinxronnogo zapuska./ Radiotexnika, 1969, t.24, №10, cc.37-45.

4. Fink L.M. Teoriya peredachi diskretny`x soobshhenij. - M.: Sov. radio, 1970. -728s.

5. Zolotuev A. D. Podoptimal`ny`j metod sinxronizacii PSP dlya kognitivny`x sistem special`noj svyazi, Perspektivy` razvitiya informacionny`x texnologij: sbornik materialov XXV Mezhdunarodnoj nauchno-prakticheskoy konferencii / Pod obshh.red. S.S. Chernova. – Novosibirsk: Izdatel`stvo CzRNS, 2015. – s. 54-62

6. Khisamov F., Zolotuev A., Sobachkin D., Bobilev M., Simulink Modelling of the Majority Pseudo-noise Sequence Acquisition Method for Multi-Carrier CDMA // International Conference on Innovative Trends in Electronics Communication and Applications, India, с. 138-142

7. Bernshtejn S. N., v kn.: Sobr. soch., t. 2, M., 1954, s. 130-40.