ISSN 0033-8486

РАДИОТЕХНИКА

6 1999

ЖУРНАЛ В ЖУРНАЛЕ

РАДИОСИСТЕМЫ

Выпуск 37 Радиотехнические и информационные системы охраны и безопасности, № 2

Выпуск 38 Информационный конфликт в спектре электромагнитных волн, № 5. Часть 1. Радиоэлектронные системы

ИПРЖР
Тел./факс: (095) 925-9241
Эл. почта: zaoiprzhr@glasnet.ru
http://www.glasnet.ru/~zaoiprzhr/

УДК 621.391

Оценка скрытности передачи информации при использовании рандомизированной импульсной несущей

А.П.Трифонов, М.Б.Беспалова

Методом локально-марковской аппроксимации найдена дисперсия квазиправдоподобной оценки периода следования рандомизированной импульсной несущей на фоне белого шума.

Method of locally-Markov approximation the quasilikelyhood estimate dispersion of random pulse carrier repetition period in additive white noise are founded.

В системах передачи информации в качестве несущего колебания часто используются периодические последовательности импульсов вида [1]

$$s_0(t,\theta)=\sum_{k=0}^{N-1} a_k I[(t-k\theta)/\tau], \tag{1}$$

где θ — период следования, посредством модуляции которого передается информация; a_k и τ — амплитуда и длительность k-го импульса; $I(x)=1$ при $|x|<\frac{1}{2}$ и $I(x)=0$ при $|x|>\frac{1}{2}$. В [2] для повышения скрытности передачи информации предложено рандомизировать импульсную несущую (1) введением мультипликативных стохастических гауссовских искажений. Тогда полезный сигнал представляет собой последовательность из N прямоугольных импульсов, искаженных модулирующей помехой

$$s(t,\theta)=\sum_{k=0}^{N-1} \xi_k(t) I[(t-k\theta)/\tau], \tag{2}$$

где $\xi_k(t)$ — стационарный гауссовский случайный процесс, обладающий моментами

$$\langle\xi_k(t)\rangle=a_k,\quad \langle\xi_k(t)\xi_k(t+\lambda)\rangle-a_k^2=K_k(\lambda). \tag{3}$$

Сторонний наблюдатель для реализации несанкционированного доступа к передаваемой информации должен определять оценку периода следования последовательности (2). В общем случае статистические характеристики (3) стохастических мультипликативных искажений рандомизированной несущей ему неизвестны. Поэтому будем полагать, что для синтеза алгоритма оценки периода следования по методу максимального правдоподобия сторонний наблюдатель использует некоторые ожидаемые (прогнозируемые) статистические характеристики рандомизации импульсной несущей

$$a_{1k},\quad K_{1k}(\lambda),\quad k=\overline{0,N-1}. \tag{4}$$

При этом в общем случае $a_{1k}\neq a_k$ и $K_{1k}(\lambda)\neq K_k(\lambda)$.

Цель работы — определить степень скрытности передачи информации при использовании рандомизированной импульсной несущей (2) вследствие отличия прогнозируемых (4) и истинных (3) статистических характеристик рандомизации.

Полагая случайные процессы $\xi_k(t)$ в различных периодах повторения статистически независимыми, имеем, что рандомизированная несущая (2) представляет собой нестационарный гауссовский случайный процесс, первые два прогнозируемые моменты которого

$$a_{1s}(t,\theta)=\sum_{k=0}^{N-1} a_{1k} I[(t-k\theta)/\tau], \quad K_{1s}(t_1,t_2,\theta)=\sum_{k=0}^{N-1} I[(t_1-k\theta)/\tau]\, I[(t_2-k\theta)/\tau] K_{1k}(t_1,t_2). \tag{5}$$

Таким образом, считаем, что сторонний наблюдатель для синтеза оценки периода следования рандомизированной импульсной несущей использует прогнозируемые (5) математическое ожидание и корреляционную функцию рандомизированной несущей.

В соответствии с методом максимального правдоподобия [4] для получения оценки периода следования необходимо формировать логарифм функционала отношения правдоподобия. Положим, что рандомизированная импульсная несущая (2) наблюдается в течение интервала времени $[0,T]$ на фоне гауссовского белого шума $n(t)$ с односторонней спектральной плотностью N_0; интервал наблюдения больше длительности всей последовательности, т.е. $T > N\theta$; скважность последовательности не слишком мала и длительность τ импульсов последовательности значительно больше времени корреляции процессов $\xi_k(t)$, так что

$$\mu_k >> 1, \quad \mu_{1k} >> 1, \quad \mu_k = \tau\, \Omega_k / 4\pi, \quad \mu_{1k} = \tau\, \Omega_{1k} / 4\pi, \tag{6}$$

где $\Omega_k = \int_{-\infty}^{\infty} G_k^2(\omega)\, d\omega / \max_\omega G_k^2(\omega)$ — эквивалентная полоса частот стохастической модуляции; $\Omega_{1k} = \int_{-\infty}^{\infty} G_{1k}^2(\omega)\, d\omega / \max_\omega G_{1k}^2(\omega)$; $G_k(\omega)$ и $G_{1k}(\omega)$ — истинная и прогнозируемая спектральные плотности соответственно.

При выполнении (6) и перечисленных условий, порторяя выкладки [3] для нестационарного гауссовского процесса, обладающего моментами (5), член логарифма функционала отношения правдоподобия, зависящий от оцениваемого параметра, можно записать как

$$L(\theta) = \frac{1}{N_0} \sum_{k=0}^{N-1} \int_{k\theta-\tau/2}^{k\theta+\tau/2} \left[y_{1k}^2(t) + \frac{2a_{1k}}{1+q_{01k}} x(t) \right] dt. \tag{7}$$

Здесь $y_{1k}(t) = \int_{-\infty}^{\infty} x(t') h_{1k}(t-t')dt'$ — отклик фильтра с передаточной функцией $H_{1k}(\omega)$ на реализацию наблюдаемых данных; $q_{01k} = 2G_{1k}(0)/N_0$; $x(t) = s(t,\theta_0) + n(t)$ — реализация наблюдаемых данных. Передаточная функция фильтра выбирается из условия $|H_{1k}(\omega)|^2 = 2G_{1k}(\omega) / [N_0 + 2G_{1k}(\omega)]$. Искомая оценка $\widetilde{\theta}$ определяется как положение наибольшего максимума функции $L(\theta)$ (7). Реализация наблюдаемых данных $x(t)$ содержит рандомизированную импульсную несущую (2), статистические характеристики которой (3) отличаются от статистических характеристик (4), (5) прогнозируемой несущей, для которой найден логарифм функционала отношения правдоподобия (7). Поэтому оценка $\widetilde{\theta}$ не является оценкой максимального правдоподобия. Получаемую с помощью (7) оценку $\widetilde{\theta}$ можно назвать квазиправдоподобной, поскольку она совпадает с оценкой максимального правдоподобия при $a_{1k} \equiv a_k$ и $K_{1k}(\lambda) \equiv K_k(\lambda)$, $k=\overline{0,N-1}$.

Для определения характеристик квазиправдоподобной оценки периода следования представим (7) в виде суммы сигнальной и шумовой функций [4]

$$L(\theta)=S(\theta)+N(\theta)+C, \tag{8}$$

где сигнальная функция

$$S(\theta)=\langle L(\theta)\rangle-C, \tag{9}$$

$C=\dfrac{\tau}{4\pi}\sum\limits_{k=0}^{N-1}\int\limits_{-\infty}^{\infty}\dfrac{2G_{1k}(\omega)}{N_0+2G_{1k}(\omega)}d\omega$ — несущественная постоянная.

Учитывая (6) и пренебрегая ошибками измерения периода следования порядка времени корреляции стохастической модуляции, аналогично [3] для сигнальной функции (9) получаем

$$S(\theta)=A_s-B_s|\theta-\theta_0|. \tag{10}$$

Шумовая функция $N(\theta)=L(\theta-\langle L(\theta)\rangle$ в (8) является реализацией асимптотически (при $\mu_k\to\infty$ и $\mu_{1k}\to\infty$) гауссовского случайного процесса, причем

$$\langle N(\theta)\rangle=0,\quad B(\theta_1,\theta_2)=\langle N(\theta_1)N(\theta_2)\rangle=A_N-B_N|\theta_1-\theta_2|-C_N[\max(\theta_0,\theta_1,\theta_2)-\min(\theta_0,\theta_1,\theta_2)]. \tag{11}$$

В (10), (11) обозначено

$$A_s=\sum_{k=0}^{N-1}\left\{\frac{\tau}{4\pi}\int_{-\infty}^{\infty}\frac{\beta_k q_k^2\rho_k(\omega)\rho_{1k}(\omega)}{1+\beta_k q_k\rho_{1k}(\omega)}d\omega+Z_{0k}^2\frac{2\alpha_k+\beta_k q_{0k}}{2(1+\beta_k q_{0k})}\right\},$$

$$B_s=\sum_{k=0}^{N-1}\left\{\frac{1}{4\pi}\int_{-\infty}^{\infty}\frac{\beta_k q_k^2\rho_k(\omega)\rho_{1k}(\omega)}{1+\beta_k q_k\rho_{1k}(\omega)}d\omega+Z_{0k}^2\frac{2\alpha_k+\beta_k q_{0k}}{2\tau(1+\beta_k q_{0k})}\right\}k, \tag{12}$$

$$A_N=\sum_{k=0}^{N-1}\left\{\frac{\tau}{4\pi}\int_{-\infty}^{\infty}\frac{\beta_k^2 q_k^2\rho_{1k}^2(\omega)[1+q_k\rho_k(\omega)]^2}{[1+\beta_k q_k\rho_{1k}(\omega)]^2}d\omega+Z_{0k}^2\frac{(\alpha_k+\beta_k q_{0k})^2+q_{0k}(\alpha_k^2+2\beta_k q_{0k}+q_{0k})^2}{(1+\beta_k q_{0k})^2}\right\},$$

$$B_N=\sum_{k=0}^{N-1}k\left\{\frac{1}{4\pi}\int_{-\infty}^{\infty}\frac{\beta_k^2 q_k^2\rho_{1k}^2(\omega)}{[1+\beta_k q_k\rho_{1k}(\omega)]^2}d\omega+\frac{Z_{0k}^2\alpha_k^2}{\tau(1+\beta_k q_{0k})^2}\right\},$$

$$C_N=\sum_{k=0}^{N-1}k\left\{\frac{1}{4\pi}\int_{-\infty}^{\infty}\frac{\beta_k^2 q_k^3\rho_k(\omega)\rho_{1k}^2(\omega)[2+q_k\rho_k(\omega)]}{[1+\beta_k q_k\rho_{1k}(\omega)]^2}d\omega+Z_{0k}^2 q_{0k}\frac{\beta_k q_{0k}(q_{0k}+\beta_k+2)+\alpha_k(\alpha_k+2\beta_k)}{\tau(1+\beta_k q_{0k})^2}\right\},$$

$$\alpha_k=a_{1k}/a_k,\ \beta_k=\max_\omega G_{1k}(\omega)/\max_\omega G_k(\omega),\ \rho_k(\omega)=G_k(\omega)/\max_\omega G_k(\omega),\ \rho_{1k}(\omega)=G_{1k}(\omega)/\max_\omega G_{1k}(\omega),$$

$$q_k=2\max_\omega G_k(\omega)/N_0,\ q_{0k}=2G_k(0)/N_0,\ Z_{0k}^2=2a_k^2\tau/N_0.$$

При выводе сигнальной (10) и корреляционной (11) функций предполагалось, что $\max(|\theta-\theta_0|, |\theta_0-\theta_1|, |\theta_0-\theta_2|, |\theta_1-\theta_2|) < \min(\theta_0, \theta_1, \theta_2)/(N-1)$. Поэтому (10), (11) описывают центральные пики соответствующих функций [4].

В дальнейшем полагаем, что выходное отношение сигнал-шум достаточно велико, поэтому квазиправдоподобная оценка периода следования обладает высокой апостериорной точностью [4]. Согласно (10), (11) у сигнальной и корреляционной функций не существует второй производной по оцениваемому параметру при $\theta=\theta_1=\theta_2=\theta_0$, так что рандомизированная импульсная несущая (2) является разрывной по периоду следования [5]. Найти дисперсию оценки периода следования в этом случае можно с помощью метода локально-марковской аппроксимации [6]

$$D(\widetilde{\theta})=26\tau^2\left[\sum_{k=0}^{N-1}k\left\{\frac{\tau}{4\pi}\int_{-\infty}^{\infty}\frac{\beta_k^2q_k^2\rho_{1k}^2(\omega)\left\{1+[1+q_k\rho_k(\omega)]^2\right\}}{[1+\beta_kq_k\rho_{1k}(\omega)]^2}d\omega+Z_{0k}^2\frac{\alpha_k[\alpha_k(2+q_{0k})+2\beta_kq_{0k}]+\beta_kq_{0k}^2(q_{0k}+\beta_k+2)}{(1+\beta_kq_{0k})^2}\right\}\right]\times$$

$$\times\left[2\sum_{k=0}^{N-1}k\left\{\frac{\tau}{4\pi}\int_{-\infty}^{\infty}\frac{\beta_kq_k^2\rho_k(\omega)\rho_{1k}(\omega)}{1+\beta_kq_k\rho_{1k}(\omega)}d\omega+Z_{0k}^2\frac{2\alpha_k+\beta_kq_{0k}}{2(1+\beta_kq_{0k})}\right\}\right]^{-4}. \qquad (13)$$

Отметим, что квазиправдоподобная оценка периода следования условно несмещенная, поэтому дисперсия (13) оценки совпадает с ее рассеянием [4].

Описать количественно скрытность рандомизированной импульсной несущей можно, сравнивая дисперсию квазиправдоподобной оценки периода следования с дисперсией оценки максимального правдоподобия, которая используется для санкционированного доступа к передаваемой информации.

Обозначим $D(\hat{\theta})$ — дисперсия оценки максимального правдоподобия периода следования. Согласно [3] $D(\hat{\theta})$ определяется (13), где следует полагать $\alpha_k \equiv 1$, $\beta_k \equiv 1$, $\rho_{1k}(\omega) \equiv \rho_k(\omega)$, $k=\overline{0,N-1}$. Сравнивая $D(\widetilde{\theta})$ и $D(\hat{\theta})$, можем охарактеризовать скрытность рандомизированной импульсной несущей отношением $\chi=D(\widetilde{\theta})/D(\hat{\theta})$, которое назовем параметром скрытности. Очевидно, чем больше величина параметра скрытности, тем выше степень скрытности рандомизированной импульсной несущей для стороннего наблюдателя, который реализует несанкционированный доступ к передаваемой информации на основе статистических характеристик (4) стохастической модуляции и приемника (7).

- Найдено общее выражение для параметра скрытности, величина которого характеризует степень скрытности передачи информации посредством модуляции периода следования рандомизированной импульсной несущей.

Приведенные результаты получены при поддержке Российского фонда фундаментальных исследований.

Литература

1. *Трифонов А.П., Беспалова М.Б.* Эффективность оценки периода следования прямоугольных импульсов. — Радиотехника, 1992, №10/11.
2. *Трифонов А.П., Беспалова М.Б.* Влияние рандомизации импульсной несущей на скрытность передачи информации. — Прикладные вопросы защиты информации. — Воронеж, ВВШ МВД РФ, 1996.
3. *Трифонов А.П., Беспалова М.Б.* Эффективность оценок периода следования прямоугольных импульсов при наличии модулирующих помех. — Радиотехника, 1998, №1.
4. *Куликов Е.И., Трифонов А.П.* Оценка параметров сигналов на фоне помех. — М.: Сов.радио, 1978.
5. *Ибрагимов И.А., Хасьминский Р.З.* Асимптотическая теория оценивания. — М.: Наука, 1979.
6. *Трифонов А.П., Шинаков Ю.С.* Совместное различение сигналов и оценка их параметров на фоне помех. — М.: Радио и связь, 1986.

Поступила 19 апреля 1999 г.