УДК 621.396.2

Залужний О.В. (ВІТІ)
к.т.н. Голь В.Д. (ІСЗЗІ КПІ)
к.т.н. Штаненко С.С. (ВІТІ)

МЕТОД ВИБОРУ ДОВЖИНИ КОДОВОГО СЛОВА ДЛЯ РАДІОЛІНІЙ З ВІДКЛАДЕНОЮ ПЕРЕДАЧЕЮ ПІДТВЕРДЖЕННЯ

Запропонований метод вибору довжини кодового слова для радіоліній з обмеженою смугою пропускання та відкладеною передачею підтвердження. Він дозволяє обчислювати оптимальну довжину кодової послідовності при заданих гранично допустимих значеннях ймовірності вірного і хибного спрацювання, в умовах постановки імітаційних завад.

Залужный О.В., Голь В.Д., Штаненко С.С. Метод выбора длины кодового слова для радиолиний с отложенной передачей подтверждения. *Предложен метод выбора длины кодового слова для радиолиний с ограниченной полосой пропускания и отложенной передачей подтверждения. Он позволяет вычислять оптимальную длину кодовой последовательности при заданных гранично допустимых значениях вероятности верного и ложного срабатывания, в условиях постановки имитационных помех.*

O. Zaluzhnyi, V. Gol, S. Shtanenko Codeword length selection metod radio lines with delayed acknowledgment. *In this article, the choose method of codeword length selection metod for radio lines with constrained bandwidth and delayed acknowledgement is proposed. It allows us calcule an optimal code sequence length at the given boundary acceptable probabilities of true and false operation, in conditions with simulated echo set.*

Ключові слова: *радіолінія з відкладеною передачею підтвердження, критерій Неймана-Пірсона, хибне спрацювання, ймовірність хибного спрацювання, ймовірність вірного прийому.*

Постановка завдання в загальному виді. В умовах ведення сучасних бойових дій широко використовуються системи радіоуправління, телеметрії, моніторингу віддалених об’єктів, оповіщення та ін.

Для покращення електромагнітної сумісності різних засобів, зменшення енергоспоживання, габаритних показників, затрат на розгортання та експлуатацію обладнання, а також, що особливо важливо, з метою приховати місце знаходження кореспондента, особливе місце у вказаних системах, як вітчизняного так і зарубіжного виробництва знаходять радіолінії з відкладеним підтвердженням (далі – РЛ з ВП).

Вони застосовуються з метою: передачі інформації про стан об’єкта в розвідувально-сигналізаційних і охоронних системах, передачі сигналів управління електронними пристроями перехоплення інформації (радіокерованими закладними пристроями для запису мови), передачі команд управління та сигналів оповіщення підводним човнам, надводному флоту, окремим тактичним групам, силам спеціального призначення (напр. – протокол ACP 142 (A), що передбачає роботу в режимі EMCON (Emission Control) – „радіомовчання”) [1, 2].

Недоліками таких радіоліній є відсутність інформації про факт посилки корисного сигналу і можливості адаптації до сигнально-завадової обстановки [1]. Обмеженим є вибір оптимальних методів модуляції і способів прийому та обробки сигналів, завадостійкого кодування, що зумовлено обмеженим частотним, часовим, енергетичним ресурсом та необхідністю функціонуванням в умовах високого насичення радіоефіру та впливу засобів радіоелектронної боротьби противника.

За протоколом ACP 142 або ACP 142 (A), швидкість передачі в радіоканалі, в окремих випадках, складає 75 біт/с [2]. Необхідна умова їх використання – забезпечення заданих та взаємопов’язаних показників надійності та достовірності доведення інформації, а саме – ймовірності правильного прийому повідомлення ($P_{\text{п}}$) та ймовірності прийому хибного повідомлення $P_{\text{х}}$ (хибного спрацювання) [3]. Останнє зумовлене впливом структурних завад та відбувається, коли корисний сигнал в каналі відсутній.

Результати проведеного аналізу наукових досліджень у даній предметній області свідчать про те, що для розв’язання подібних задач застосовується статистичний критерій Неймана-Пірсона. Відповідно до нього спочатку досягається задане і достатньо мале значення

$P_{\text{х}}$, після чого здійснюються всі можливі заходи для отримання максимального значення $P_{\text{п}}$ [4, 5, 6].

Проте невирішеним залишається завдання забезпечення одночасного виконання вимог по ймовірності правильного прийому ($P_{\text{п}} \geq P_{\text{п}}^{*}$, де $P_{\text{п}}^{*}$ – мінімально необхідне значення ймовірності правильного прийому повідомлення) та хибного спрацювання ($P_{\text{х}} \leq P_{\text{х}}^{*}$, де $P_{\text{х}}^{*}$ – максимально допустиме значення ймовірності хибного спрацювання). В такому випадку необхідно знайти такий (мінімально необхідний) об'єм випадкової вибірки X_N (N – кількість розрядів (довжина) двійкового кодового слова), при якому відповідний оптимальний критерій Неймана-Пірсона забезпечить **задані** значення ймовірностей $P_{\text{х}}$ та $P_{\text{п}}$ [7].

Метою статті є розробка методу вибору мінімально необхідної довжини кодового слова з використанням оптимального критерію Неймана-Пірсона при заданих вимогах до ймовірності правильного прийому повідомлення та хибного спрацювання.

Загальна частина. У вказаних вище системах, рішення про прийом повідомлення (кодового слова) приймається тоді, коли загальна кількість правильно прийнятих його символів n_N – не менше ніж деяке значення $N_{\text{пор}}$ (далі – поріг) [5, 8]. Число n_N є випадковою величиною, а її розподіл відповідає біноміальному закону (схема Бернуллі). Відповідно, ймовірність правильного прийому повідомлення з першої спроби (ймовірність появи випадкової величини n_N такої, що $n_N \geq N_{\text{пор}}$ в N незалежних випробуваннях), описується виразом [3]:

$$P_{\text{п1}} = \sum_{i=0}^{N-N_{\text{пор}}} C_N^i \cdot p_{\text{біт}}^i \left(1-p_{\text{біт}}\right)^{N-i}, \quad \text{або} \quad P_{\text{п1}} = 1 - \sum_{i=0}^{N_{\text{пор}}-1} C_N^i \cdot p_{\text{біт}}^{N-i} \left(1-p_{\text{біт}}\right)^i, \tag{1}$$

де $p_{\text{біт}}$ – ймовірність помилкового прийому символу повідомлення (ймовірність бітової помилки).

Оскільки РЛ з ВП відомчого призначення функціонують в складних завадових умовах, варто враховувати, що в процесі очікування повідомлення може виникнути ситуація, коли канал відсутній, а через вплив завади, яка складається із послідовності статистично незалежних рівномірних символів приймається якесь хибне повідомлення. У цьому випадку $p_{\text{біт}} = 0{,}5$ [3, 9].

Ймовірність хибного прийому кодового слова з першої спроби при впливові структурних завад різного походження (постановці імітаційних завад) задається наступним співвідношенням [3]:

$$P_{\text{х1}} = \sum_{i=0}^{N-N_{\text{пор}}} C_N^i \cdot \left(p_{\text{біт}}^{*}\right)^i \left(1-p_{\text{біт}}^{*}\right)^{N-i} = 2^{-N} \sum_{n=0}^{N-N_{\text{пор}}} C_N^i \text{, або } P_{\text{х1}} = 1 - 2^{-N} \sum_{n=0}^{N_{\text{пор}}-1} C_N^i \tag{2}$$

Відомо, що коли, наприклад, час роботи радіолінії дорівнює ΔT, то атакуючій стороні досить нескладно підібрати таке значення розрядності регістра зсуву n (розрядність регістра для формування послідовності максимальної довжини), за допомогою якого можна буде сформувати імітуючу послідовність загальної довжини $L = 2^n - 1$, що не повторюватиметься за структурою впродовж часу ΔT на довжині n при будь-якому місці його розташування [9].

Тоді, вираз для ймовірності хибного спрацювання хоча б один раз за час ΔT, при швидкості передачі V записується наступним чином [9]:

$$P_{\text{х}L} = \sum_{i=1}^{L-N+1} C_{L-N+1}^i \cdot P_{\text{х1}}^i \left(1-P_{\text{х1}}\right)^{L-N+1-i},$$

що рівнозначно:

$$P_{\text{х}L} = 1 - \left(1-P_{\text{х1}}\right)^{L-N+1}, \quad \text{де } L = \Delta T \cdot V. \tag{3}$$

Вихідними даними для розрахунку є значення $P_{\text{п}}^{*}$, $P_{\text{х}}^{*}$, час роботи радіолінії в режимі EMCON (ΔT); $p_{\text{біт}}$ – імовірність бітової помилки; V – швидкість передачі в радіоканалі.

Необхідно врахувати наступні *обмеження:* максимальна довжина повідомлення $N_{\max}$ обмежується часовими вимогами до системи.

Можливі припущення: атакуючій стороні відомі неінформаційні параметри сигналу та час роботи радіолінії; двійкові стани елементів імітаційної кодової послідовності є рівноймовірними ($p_{\text{біт}} = 0{,}5$) та взаємонезалежними.

Цільова функція, що має за мету мінімізацію довжини N, має вигляд:

$$N = F\left[P_{\text{п}}^{*}, P_{\text{xL}}^{*}\right] \to \min .$$

Знаючи вимоги до хибного спрацювання $P_{\text{x}L}^{*}$ та використавши формулу (3) розраховуються вимоги до ймовірності хибного спрацювання з першої спроби: $P_{\text{x1}}^{*} = 1 - \sqrt[L+N-1]{1-P_{\text{xL}}^{*}}$. Так як вважається, що РЛ працює в режимі EMCON впродовж тривалих проміжків часу (1 год та більше) то при обчисленнях сумою $N+1$ можна знехтувати, оскільки $L >> N$.

Відповідно до загальної теорії перевірки статистичних гіпотез [7] ймовірності помилки 1-го роду відповідає значення P_{x1}, оскільки хибне кодове слово буде прийнято тоді, коли за даними реалізації $\vec{x}_N$ випадкової вибірки $\vec{X}_N$ (де N – довжина кодового слова) з генеральної сукупності випадкової величини X (правильний прийом символу повідомлення) приймається рішення про те, що повідомлення передавалось тоді, коли корисний сигнал в прийнятій реалізації відсутній. Ймовірність появи випадкової величини X є невідомою до початку експерименту.

Потужності статистичного критерію відповідає ймовірність правильного прийому повідомлення $P_{\text{п}}$, який відбувається тоді, коли вірно прийняте рішення, що повідомлення передавалось. Звідки ймовірність пропуску кодового слова $P_{\text{проп}} = 1 - P_{\text{п}}$ – ймовірність помилки другого роду. Таким чином, задача прийняття рішення про наявність, чи відсутність корисного сигналу в прийнятій реалізації зводиться до задачі перевірки статистичних гіпотез між двома можливими діями: відхилити кодове слово – дія 1, чи прийняти – дія 2.

Оскільки РЛ працює в режимі відкладеної передачі підтвердження і факт посилки корисного сигналу апріорі невідомий, то невідомим параметром, який впливатиме на правильність прийняття рішення є ймовірність бітової помилки $p_{\text{біт}}$ в РЛ. Тоді доцільно сформулювати наступні гіпотези:

основна – H_0: $p_{\text{біт}} \geq p_{\text{біт0}}$;

альтернативна – H_1: $p_{\text{біт}} \leq p_{\text{біт1}}$, де $p_{\text{біт0}} = 0.5$, а $p_{\text{біт1}} = const$ – деяке прогнозоване значення ймовірності помилки на біт в точці прийому, $p_{\text{біт0}} > p_{\text{біт1}}$.

Дія „1” здійснюється тоді, коли у прийнятому кодовому слові відносна кількість помилково прийнятих символів $p_{\text{біт}} \geq p_{\text{біт0}}$ (приймається рішення, що справедлива гіпотеза H_0).

Дія „2” здійснюється тоді, коли у прийнятому кодовому слові відносна кількість помилково прийнятих символів $p_{\text{біт}} \leq p_{\text{біт1}}$ (приймається рішення, що справедлива гіпотеза H_1).

Хибне спрацювання з першої спроби відбувається тоді, коли прийнята гіпотеза H_1, а вірна – H_0. Ймовірність такої події описується виразом:

$$P_{\text{x1}}(p_{\text{біт}}) = P\left\{\left(X_1 + \ldots + X_N\right) \geq N_{\text{пор}} \mid H_0\right\}. \qquad (4)$$

Повідомлення є прийнятим правильно, коли рішення про справедливість гіпотези H_1 – вірне. Ймовірність такої події описується виразом:

$$P_{\text{п}}(p_{\text{біт}}) = P\{(X_1 + \ldots + X_N) \geq N_{\text{пор}} \mid H_1\}. \quad (5)$$

Таким чином, критична множина для оптимального критерію Неймана-Пірсона в даному випадку матиме вигляд:

$$\sum_{i=1}^{N} n_N \geq N_{\text{пор}}.$$

Для вирішення задачі пошуку мінімально необхідної довжини кодового слова, при якій відповідний оптимальний критерій Неймана-Пірсона забезпечить задані значення ймовірностей $P_{\text{х1}}$ та $P_{\text{п}}$, необхідно розв'язати систему нерівностей:

$$\begin{cases} P\{(X_1 + \ldots + X_n) \geq N_{\text{пор}} \mid H_0\} \leq P^*_{\text{х1}}(p_{\text{біт}}) \\ P\{(X_1 + \ldots + X_n) \geq N_{\text{пор}} \mid H_1\} \geq P^*_{\text{п}}(p_{\text{біт}}) \end{cases}. \quad (6)$$

З цією метою можна використати метод, який запропонований в [7] для визначення об'єму випадкової вибірки при заданих значеннях ймовірностей помилки першого та другого роду, коли загальна кількість „успіхів" експерименту розподілена за біноміальним законом і ймовірність появи такої події в кожному із випробувань є невідомою до завершення експерименту.

Тоді, відповідно до відомої теореми Муавра-Лапласа, при достатньо великих значеннях довжини кодового слова N, випадкова величина n_N має асимптотично-нормальний розподіл з математичним очікування $\mu = N \cdot (1 - p_{\text{біт}})$ і дисперсією $\sigma^2 = N \cdot (1 - p_{\text{біт}}) \cdot p_{\text{біт}}$.

Використовуючи вказаний розподіл приходимо до системи рівнянь для пошуку необхідного значення довжини кодового слова (N^*) і відповідного йому порогу ($N^*_{\text{пор}}$).

$$\begin{cases} 1 - \Phi\left(\dfrac{N^*_{\text{пор}} - N^* \cdot (1 - p_{\text{біт0}})}{\sqrt{N^* \cdot (1 - p_{\text{біт0}}) \cdot p_{\text{біт0}}}}\right) = P^*_{\text{х1}}(p_{\text{біт}}) \\ 1 - \Phi\left(\dfrac{N^*_{\text{пор}} - N^* \cdot (1 - p_{\text{біт1}})}{\sqrt{N^* \cdot (1 - p_{\text{біт1}}) \cdot p_{\text{біт1}}}}\right) = P^*_{\text{п}}(p_{\text{біт}}) \end{cases}, \quad (7)$$

де $\Phi(x)$ – функція нормального розподілу з параметрами (0, 1) [10].

Нерівність (7) може бути представлена у наступному вигляді:

$$\begin{cases} \dfrac{N^*_{\text{пор}} - N^* \cdot (1 - p_{\text{біт0}})}{\sqrt{N^* \cdot (1 - p_{\text{біт0}}) \cdot p_{\text{біт0}}}} = u_{1-\alpha} \\ \dfrac{N^*_{\text{пор}} - N^* \cdot (1 - p_{\text{біт1}})}{\sqrt{N^* \cdot (1 - p_{\text{біт1}}) \cdot p_{\text{біт1}}}} = u_{\beta} = -u_{1-\beta} \end{cases},$$

де u – квантіль стандартного нормального закону розподілу; $\alpha = P^*_{\text{х1}}(p_{\text{біт}})$, $\beta = 1 - P^*_{\text{п}}(p_{\text{біт}})$.

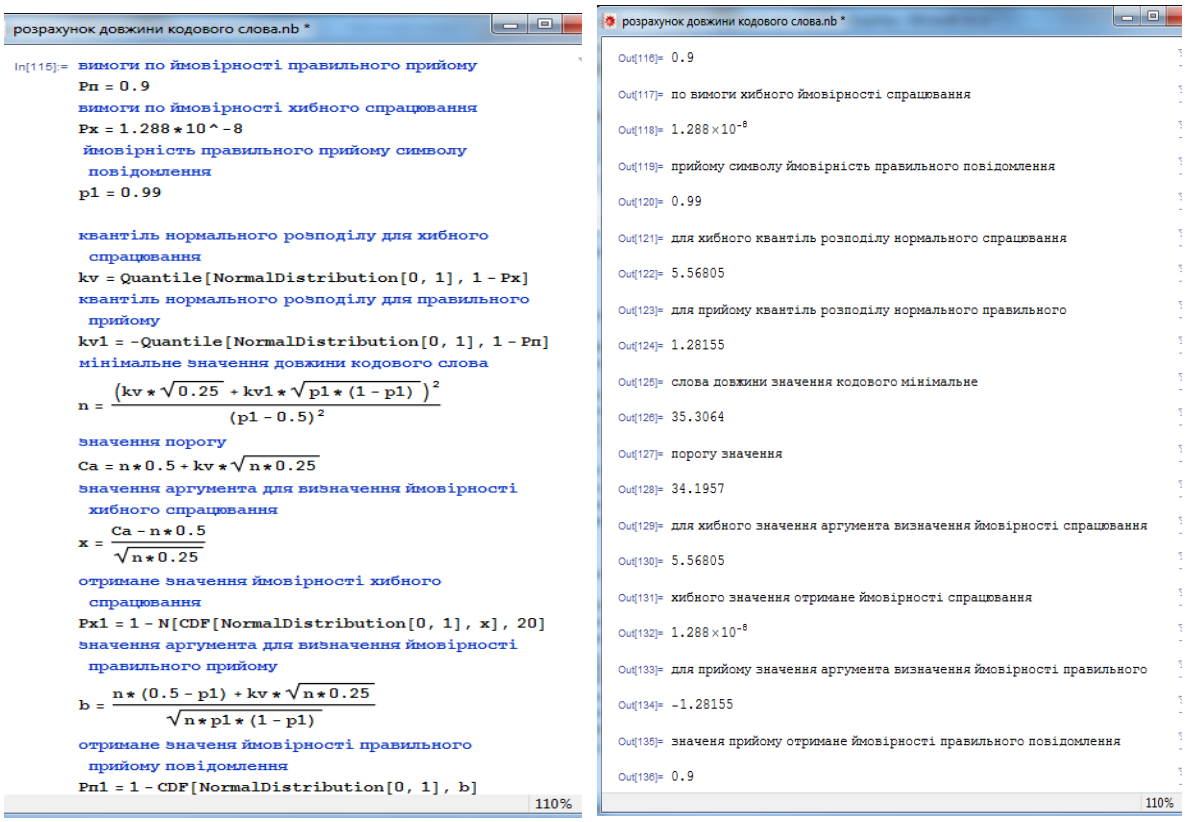
Вирішуючи цю систему знаходимо :

$$N^* = \frac{\left(u_{1-\alpha} \cdot \sqrt{(1 - p_{\text{біт0}}) \cdot p_{\text{біт0}}} + u_{1-\beta} \cdot \sqrt{(1 - p_{\text{біт1}}) \cdot p_{\text{біт1}}}\right)^2}{(p_{\text{біт0}} - p_{\text{біт1}})^2}$$

Звідки значення $N_{\text{пор}}$, яке задовольнятиме оптимальному критерію Неймана-Пірсона при $N = N^*$, визначається наступною рівністю:

$$N^*_{\text{пор}} = N^* p_{\text{біт0}} + u_{1-\alpha} \cdot \sqrt{N^* p_{\text{біт0}} \cdot (1 - p_{\text{біт0}})}.$$

Відповідно до розробленого методу в середовища програми Wolfram Mathematica 9.0. було здійснено обчислення мінімально необхідної довжини кодового слова при наступних вимогах: $P_{\text{п}} \geq 0{,}9$, $P_{\text{х1}} \leq 1{,}288 \cdot 10^{-8}$ та коли $p_{\text{біт}} = 1 - 0{,}99 = 10^{-2}$. На рис. 1 представлено скріншот вікна програми з вихідними даними та результатами розрахунків. Вони свідчать про адекватність та функціональну придатність розробленого методу для вирішення таких задач.



вихідні дані результати розрахунку

Рис. 1 Скріншот вікна програми Wolfram Mathematica 9.0 при розрахунку мінімально необхідної довжини кодового слова

Таким чином, в роботі розроблено метод вибору мінімально необхідної довжини кодового слова для радіоліній з відкладеною передачею підтвердження. Враховано можливість виникнення хибних спрацювань в результаті впливу структурних завад впродовж усього часу знаходження системи в режимі радіомовчання (EMCON).

У процесі синтезу методу використаний відомий метод визначення об’єму випадкової вибірки, при якій оптимальний статистичний критерій Неймана-Пірсона забезпечує виконання заданих вимог по ймовірності помилки першого та другого роду.

З використанням середовища програми Wolfram Mathematica 9.0 за розробленим методом проведені обчислення, які свідчать про його функціональну придатність.

Запропонований метод дозволяє розраховувати значення мінімально необхідної довжини кодового слова при заданих вимогах до ймовірності правильного прийому повідомлення та хибного спрацювання.

Подальшим напрямком досліджень є вивчення можливості використання розробленого методу в комплексі з різними методами підвищення достовірності передачі дискретних повідомлень у радіолініях з відкладеним підтвердженням.

ЛІТЕРАТУРА

1. Military Messaging over HF Radio and Satellite using STANAG 4406 Annex E. Published by Isode Limited. – Режим доступу:
https://www.isode.com/whitepapers/military-messaging-stanag-4406.html

2. ACP 142(A), P_MUL – a protocol for reliable multicast in bandwidth constrained and delayed acknowledgement (EMCON) environments. Unclassified CCEB publication. – 2008. – 58 P. – Режим доступу:
https://pdfs.semanticscholar.org/087e/4c721b38d66a83a813f519cb6126c0615b1c.pdf

3. Ерохін В.Ф. Методика оцінки завадостійкості односторонньої передачі команд і повідомлень / В.Ф.Ерохін, О.В.Залужний, В.М. Раєвський // Спеціальні телекомунікаційні системи та захист інформації. – 2012. – Випуск 2 (22). – С. 67 – 72.

4. Васильев К.К. Теория электрической связи: учебное пособие / К.К. Васильев, В.А. Глушков, Дормидонтов, А.Г. Нестеренко; под общ. ред. К.К. Васильева. – Ульяновск: УлГТУ, 2008. – 452 с.

5. Ашимов Н. М. Поэлементная обработка и обработка в целом двоичных сигналов относительной фазовой телеграфии / Н.М. Ашимов, А.С. Карпов, Ю.П. Апарина, В.С. Миронов, Р.В. Синицын // Спецтехника и связь. – 2011. – № 3. – С. 20 – 25.

6. Левин Б.Р. Теоретические основы статистической радиотехники / Б.Р. Левин. – [3-е изд., перераб. и доп.]. – М.: Радио и связь, 1989. – 656 с.

7. Математическая статистика: Учеб. для вузов / [В.Б. Горяинов, И.В. Павлов, Г.М. Цветкова и др.]; под ред. В.С. Зарубина, А.П. Крищенко. – М.: МГТУ им. Н.Э. Баумана, 2001. – 424 с. (Сер. Математика в техническом университете; Вып. XVII).

8. Мальцев Г. Н. Кодирование сообщений в системах радиоуправления без обратного информационного канала / Г. Н. Мальцев, Е. В. Чернявский // Информационно-управляющие системы. – 2011. – № 4. – С. 60 – 65.

9. Ерохин В. Ф. Методика расчета длины кодограммы для асимптотически надежной радиолинии управления / В. Ф.Ерохин, О. В.Залужный // Вісник Національного технічного університету України „КПІ”, серія – Радіотехніка. Радіоапаратобудування. – 2013. – № 54. – С. 44 – 53.

10. Большев Л. Н. Таблицы математической статистики / Л. Н. Большев, И. В. Смирнов – М.: Наука, – 1983. – 416 с. – (Главная редакция физико-математической литературы).