Абарона кадаванага сігналу ад перахопу

А. І. Міцюхін
Беларускі дзяржаўны ўніверсітэт інфарматыкі і радыёэлектронікі,
Інстытут інфармацыйных тэхналогій, Мінск, Беларусь
mityuhin@bsuir.by

У артыкуле аналізуюцца неабходныя характарыстыкі сістэмы сувязі, якія павышаюць ўзровень памехаабароненасці і утойлівасці.

Ключевые словы: сувязь, памехаабароненасць, радыёўціск, кадаванне, белы шум, памылка, імавернасць, нявызначанасць.

У спецыяльных сістэмах сувязі найважнейшае значэнне маюць такія характарыстыкі як памехаабароненасць і ўтойлівасць работы. Гэта абумоўліваецца тым, што такія сістэмы павінны працаваць у каналах з актыўным радыёсупрацівам (радыёэлектронным ўціскам) і радыётэхнічнай выведкай з мэтай выяўлення сігналу, вызначэння структуры сігналу і дэкадавання інфармацыі, якая перадаецца.

Сродкам радыёўціску перашкаджае памехаабароненасць работы сістэмы сувязі. Паспяховым дзеянням радыёперахопу перашкаджае утойлівая работа сістэмы. У артыкуле аналізуюцца неабходныя характарыстыкі сістэмы сувязі, якія павышаюць ўзровень памехаабароненасці і утойлівасці.

Вядома, што павышэнне надзейнасці сувязі вырашаецца за кошт выкарыстання метаду пашырэння спектру інфармацыйнага сігналу (Ипатов, 2007), кадавання інфармацыі кодам, статыстычныя і спектральныя характарыстыкі, якога набліжаюцца да характарыстык фонавага выпраменьвання тыпу белага шуму. На мал. 1 паказана матэматычная мадэль канала, па якім перадаецца i-е кадаванае паведамленне $\boldsymbol{X}^i, i = 1,...,n, M, M$ — магутнасць мноства $\{\boldsymbol{X}\}$. Кодар фарміруе словы $[n, M, d_{\min}]$-кода даўжынёй n знакаў; $d_{\min} = 2t + 1$ — мінімальная адлегласць Хэмінга, t — кратнасць памылак, выпраўленых кодам; ДСК — двайковы сіметрычны канал (канал перахопу). Код можа выпраўляць t памылак. Як у асноўным канале, так і ў канале перахопу фарміруецца адытыўная сумесь (вектар) віду

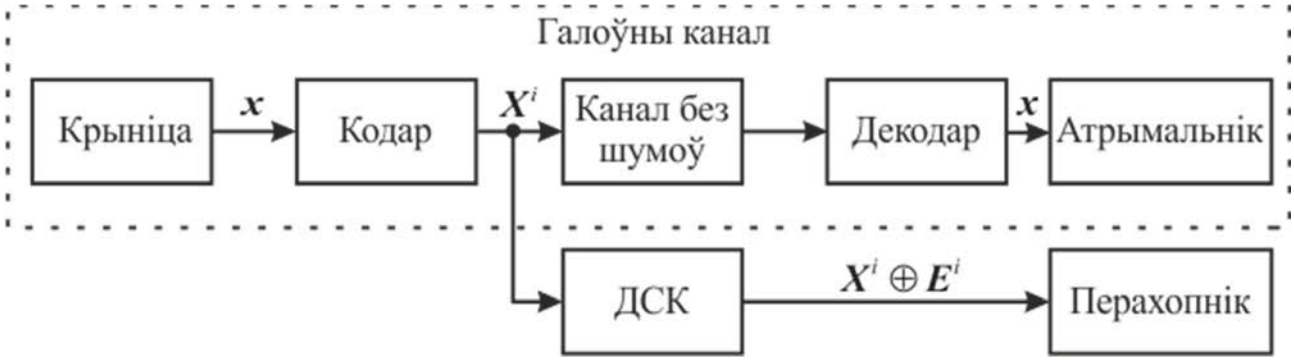
$$\boldsymbol{Y} = \boldsymbol{X} + \boldsymbol{E},$$

дзе $\boldsymbol{E} = (e_0,...,e_{n-1})$ — выпадковы вектар памылак (шумавы вектар), $\boldsymbol{X} = (x_0,...,y_{n-1}), \boldsymbol{Y} = (y_0,...,y_{n-1})$.

Мяркуецца, што ў канале перахопу апрыёры могуць быць вядомымі алгарытмы кадавання-дэкадавання. Прымаем, што імавернасці $\{P^1,...,P^M\}$ фарміравання кодавых словаў $\{\boldsymbol{X}\}$ аднолькавыя. Калі ўсе значэнні імавернасцяў роўныя

$$P^i = \frac{1}{M}$$

структура кода, вектары памылак $\boldsymbol{E} = \left(e_0, \ldots, e_{n-1}\right)$ адказваюць ўласцівасці псеўдавыпадковасці (вядомыя правілы крыптазасцярогі), то энтрапія крыніцы імкнецца да максімальнага значэння. Тым самым дасягаецца максімальная нявызначанасць інфармацыйнай крыніцы для перахопніка.



Мал. 1. Абагульненая матэматычная мадэль канала

Памылкі $\boldsymbol{E}$ робяць больш складаным выяўленне і дакладнае дэкадаванне інфармацыі ў канале перахопу. У асноўным канале вектар $\boldsymbol{E}$ выступае ў якасці ключа. Стратэгія абароны павінна грунтавацца на тым, што пасля атрымання $\boldsymbol{Y}$, веды перахопніка адносна $\boldsymbol{X}$ заставаліся б нявызначанымі. Калі прыём вектара $\boldsymbol{Y}$ адбываецца ва ўмовах, калі на прыёмную прыладу дзейнічае адытыўны белы гаўсаўскі шум (АБГШ), працэс дэкадавання носіць імавернасны характар.

Колькаснай мерай паспяховага перахопу можа служыць значэнне імавернасці $P(\boldsymbol{X} \mid \boldsymbol{Y})$ атрымання інфармацыі крыніцы $\boldsymbol{x} \to \boldsymbol{X}$. У адпаведнасці з тэарэмай Баеса імавернасць перахопу i-га словы $\boldsymbol{X}^i$, па прынятаму працэсу $\boldsymbol{Y}$ вызначаецца значэннем апастэрыёрнай імавернасці

$$P(\boldsymbol{X}^i \mid \boldsymbol{Y}) = \frac{P(\boldsymbol{Y} \mid \boldsymbol{X}^i) P(\boldsymbol{X}^i)}{P(\boldsymbol{Y}^i)},$$

дзе $P(\boldsymbol{X}^i)$ і $P(\boldsymbol{Y}^i)$ — адпаведна, апрыёрныя значэнні імавернасцяў ўваходу і выхаду канала (крыніц), $P(\boldsymbol{Y} \mid \boldsymbol{X}^i)$ — пераходная імавернасць, якая характарызуе канал перахопу. Паколькі імавернасці $P(\boldsymbol{X}^i)$ і $P(\boldsymbol{Y}^i)$ вядомыя, дачыненне $\frac{P(\boldsymbol{X}^i)}{P(\boldsymbol{Y}^i)}$ роўна пастаяннай велічыні K. Тады маем значэнне

$$P(\boldsymbol{X}^i \mid \boldsymbol{Y}) = K P(\boldsymbol{Y} \mid \boldsymbol{X}^i) \qquad (1)$$

Паколькі выпадковы вектар $\boldsymbol{E} = \boldsymbol{Y} - \boldsymbol{X}$ не залежіць ад слова $\boldsymbol{X}$ функцыю

$P(\boldsymbol{Y}\,|\,\boldsymbol{X})$ адлюструем як

$$P(\boldsymbol{Y}\,|\,\boldsymbol{X}) = P\left(\boldsymbol{Y}-\boldsymbol{X}=\boldsymbol{E}\,|\,\boldsymbol{X}\right) = P\left(\boldsymbol{E}\right) \qquad (2)$$

дзе велічыня $P\left(\boldsymbol{E}\right)$ — імавернасць узнікнення наўмыснага шумавога вектара.

Выраз

$$\boldsymbol{Y}-\boldsymbol{X}^i = \left\|\boldsymbol{Y}-\boldsymbol{X}^i\right\| = d(\boldsymbol{Y},\boldsymbol{X}^i)$$

з (2) вызначае эўклідаву адлегласць паміж вектарам $\boldsymbol{Y}$ на выхадзе канала і i-м словам кода. З пазіцыі неабходнасці абароны інфармацыі ад перахопу, адлегласць Еўкліда $d(\boldsymbol{Y},\boldsymbol{X}^i)$ паказвае, колькі каардынат словы трэба сказіць з выкарыстаннем шумавого вектара $\boldsymbol{E}$, каб перавесці (трансфармаваць) адно, дазволенае для перадачы кодавае слова, ў іншае дазволенае. Заўважым, у адрозненне ад канала з АБГШ, у выпадку з ДСК эквівалентам адлегласці Еўкліда з'яўляецца адлегласць Хэмінга $d_{\min}$. З выразу (1) вынікае, што працэдура перахопу (дэкадавання) заключаецца ў знаходжанні такога значэння нумара i кодавага слова, пры якім значэнне апастэрыёрнай імавернасці $P(\boldsymbol{X}^i\,|\,\boldsymbol{Y})$ дасягае максімума. Няхай ўжываецца алгарытм аптымальнага дэкадавання вектара $\boldsymbol{Y}$ бліжайшы вектар $\boldsymbol{X}$ $\left[n,M,d_{\min}\right]$-кода па адлегласці Хэмінга (Митюхин, 2015). Тады, калі

$$d_{\min} \geq t = \frac{d_{\min}-1}{2},$$

не існуе канфігурацый вектараў $\boldsymbol{E}$ з t або менш памылак, якія маглі б здзейсніць трансфармацыю. З (2) і апошняга сцвярджэння вынікае, што колькасць ненулявых сімвалаў у шумавога вектара $\boldsymbol{E}$ або ўзровень наўмыснага шуму вызначаецца значэннем імавернасцяў

$$P(\boldsymbol{Y},\boldsymbol{X}^i) \to P(\boldsymbol{E}) \to P$$

Задача павышэння ўзроўню памехаабароненасці і утойлівасці сістэмы сувязі патрабуе, каб у канале перахопу значэнне імавернасці P набліжалася да велічыні $P \to 0,5$. Задаваная вялічыня P адлюстроўвае ступень нявызначанасці адносна перахопленага паведамлення. Практычны развязак гэтага задання грунтуецца на ўжыванні мноства кодавых вектараў $\left\{\boldsymbol{X}\right\}$, WT-мернай прасторы, дзе $WT = \dfrac{1}{\tau}$ — вялічыня спектральнай паласы кадаванага сігналу, τ — працягласць элементарнага дискрэта (чыпа) слова $\boldsymbol{X}$, T — часавы інтэрвал перадачы i-га сігналу. Развязак задання перахопу закадаванай інфармацыі патрабуе ведаў

$$2^n = 2^{\frac{T}{\tau}} = 2^{WT}$$

законаў мадуляцыі (кадавання) і неабходнасці апрацоўкі сігналаў у зашумленым канале.

Перахоп інфармацыі робіцца цяжка здзяйсняльным з-за значных часавых, вылічальных і энергетычных выдаткаў.

Высновы. Выкарыстанне шумавога вектара у сістэмах з пашырэннем спектру, якія характарызуюцца значным частотна-часовым здабыткам WT дазваляе забяспечыць энергетычную ўтойлівасць перадачы закадаванай інфармацыі.

Спіс литаратуры

Ипатов, В. (2007). *Широкополосные системы и кодовое разделение сигналов. Принципы и приложения.* Москва: Техносфера.

Митюхин, А. И., & Якубенко, П. Н (2015). Корреляционные спектры и кодовые расстояния мажоритарныхпоследовательностей. *Доклады БГУИР, 4*(90), 5—9.