Построенные модели ИК просты, наглядны и могут использоваться непосредственно с целью учета различий в результатах воздействия атаки на различные ИЭ при разработке новых СМ и повышения устойчивости уже существующих.

Список литературы

1. Ленков С.В. Методы и средства защиты информации: в 2 т. / С.В.Ленков, Д.А.Перегудов, В.А.Хорошко. — К.: Арий, 2008 — . —Т.2: Информационная безопасность. — 2008. — 344 с.

2. Кобозева А.А., Хорошко В.А. Анализ информационной безопасности.-К.:ДУИКТ, 2009.-250 с.

3. Ф. Харари. Теория графов.-М.:Мир,1973.-300 с.

4. Кобозєва А.А. Загальний підхід до оцінки властивостей стеганографічного алгоритму, заснованого на теорії збурень. - Информационные технологи и компьютерная инженерия, №1(11), 2008, с.164-171.

5. Джордж А. Численное решение больших разреженных систем уравнений / А.Джордж, Дж.Лю; пер. с англ. Х.Д.Икрамова. — М., Мир, 1984. — 333 с.

6. Гантмахер Ф.Р. Теория матриц / Ф.Р.Гантмахер. — М.: Наука, 1988. — 552 с.

7. Деммель Дж. Вычислительная линейная алгебра / Дж.Деммель; пер.с англ. Х.Д.Икрамова. — М.: Мир, 2001. — 430 с.

8. Борисенко И.И. Повышение помехоустойчивости стеганографического алгоритма – Сучасний захист інформації, №1, 2010, с.36-42.

Представлены две математические модели информационного контейнера (ИК), которые дают возможность оценить его устойчивость к предполагаемой атаке. В качестве инструмента для анализа реакции ИК на атаку в графовой модели используется спектр матрицы смежности графа «ИК-противник», а в геометрической модели – знаковая чувствительность векторов, которые являються математическим объектом ИК.

Запропоновані дві моделі інформаційного контейнера (ІК), які дають можливість оцінити його стійкість до ймовірного нападу. В якості інструмента для аналізу реакції ІК на напад в графовій моделі використовується спектр матриці суміжності графа «ІК - супротивник», а в геометричній моделі – знакова чутливість векторів, які є математичними об'єктами ІК.

Two mathematical models of information cove image (ICI) for estimate noise stability it to the assumption attack are presented in this paper. In the graph model is used spectrum of adjacency matrix of graph "ICI – adversary" for analysis a reaction ICI on the attack, but in the geometrical model is used sign sensibility of vectors that are mathematical object ICI.

Рецензент: Єрохін В.Ф.
Надіслано 04.11.2010

УДК 681.3:004.681

Опірський І.Р. (НУ «Львівська політехніка»)

ЕНТРОПІЯ ВОЛЗ ПРИ ВРАХУВАННІ ЗАВАД В ІНФОРМАЦІЇ, ЩО ПЕРЕДАЄТЬСЯ

Вступ

Зупинившись на понятті інформація в оптико-волокнній системі звязку, неможливо не торкнутися іншого суміжного поняття - ентропія. Вперше поняття ентропія і інформація зв'язав К.Шеннон в 1948р. З його подачі ентропія почала використовуватися як міра кількості інформації в процесах передачі сигналів по проводах. Слід підкреслити, що під інформацією Шеннон розумів сигнали потрібні, корисні для одержувача. Некорисні сигнали, з погляду Шеннона,- це шум і завади. Якщо сигнал на виході каналу зв'язку є точною копією сигналу на вході то, з погляду теорії інформації, це означає відсутність ентропії.

Питання визначення ентропії сигналу в оптичному волокні є досить важливим. При проходженні сигналу на великих відстання по волоконно-оптичній системі ми обовя'зково будемо мати деяку втрату сигналу саме через ентропію. Поняття ентропії вперше було введене в термодинаміці для визначення міри необоротного розсіювання енергії. При

проходженні інформаціїї через волоконно-оптичну систему зв'язку в якій існують завади, не можливо не враховувати і ентропію.

Основна частина

Існують сім типів ентропії при врахуванні завад в інформації, що передається по ВОЛЗ:

1. Ентропія системи передачі з частотною характеристикою $G(j\omega) = 1$ при наявності завад;
2. Ентропія загального випадку (система $G(j\omega) = 1$);
3. Вхідна ентропія або ентропія джерела;
4. Вихідна ентропія;
5. Ентропія похибки перетворення-розсіювання або невизначеності інформації;
6. Загальна ентропія;
7. Апріорна ентропія.

Ентропія системи передачі з частотною характеристикою $G(j\omega) = 1$ за наявності завад. При припущенні про гаусовий розподіл сигналів і при відсутності кореляції вхідних сигналів можна визначити наступні значення ентропії:

1) Вхідну ентропію або ентропію джерела $I(n_в)$ [1].

$$I(n_в) = \frac{1}{2}\log\left[2\pi e\overline{n_в^2}(t)\right] + \lim_{\Delta x \to 0}\frac{1}{\Delta x}. \quad (1)$$

2) Невизначеність інформації, так звану також розсіюванням або ентропією, обумовленою завадами $I(z_а|n_в)$.

Для невизначеності інформації на вході ВОЛЗ набуває значення ентропія (умовна ентропія):

$$I(z_а|n_в) = \frac{1}{2}\log\left[2\pi e\overline{r_в^2}(t)\right] + \lim_{\Delta x \to 0}\frac{1}{\Delta x}. \quad (2)$$

3) Вихідну ентропію $I(z_а)$ (безумовну ентропію). За відсутності кореляції вхідних сигналів безпосередньо отримуємо:

$$I(z_а) = \frac{1}{2}\log\left\{2\pi e\left[\overline{n_в^2}(t) + \overline{r_в^2}(t)\right]\right\} + \lim_{\Delta x \to 0}\log\frac{1}{\Delta x}. \quad (3)$$

4) Дійсно передану інформацію $I(n_в; z_а)$.

Фізично передана інформація є ентропією, віднесеною в рівній мірі як до посланих, так і прийнятих сигналів. Отже, вихідна ентропія з вирахуванням ентропії, обумовленої завадами, якраз і дозволяє судити про передавану інформацію:

$$I(n_в; z_а) = N(z_а) - N(z_а|n_в). \quad (4)$$

З урахуванням виразів (2) і (3) за відсутності кореляції вхідних сигналів отримуємо:

$$I(n_в; z_а) = \frac{1}{2}\log\left[1 + \frac{\overline{n_в^2}(t)}{\overline{r_в^2}(t)}\right] \quad (5)$$

або, оскільки $z_а = r_в$, то

$$I(n_в; z_в) = \frac{1}{2}\log\left[1 + \frac{\int_0^\infty P_{nв}(\omega)d\omega}{\int_0^\infty P_{rв}(\omega)d\omega}\right]. \quad (6)$$

Передана інформація $I(n_в; z_в)$ є інформацією, що міститься в загальному сигналі $z_в(t)$ по відношенню до останнього сигналу $n_в(t)$. Отже, можна записати:

$$z_в(t) = n_в(t) + r_в(t) \quad (7)$$

де $r_в(t)$ – компонента завад.

Отже проведемо оцінку ентропії для загального випадку [система $G(j\omega) = 1$]. Як вже було показано, ентропію можна виразити безпосередньо через середні потужності сигналів, якщо припустити, що ці сигнали з гаусовим розподілом. Для такого випадку передачі інформації можна вирахувати наступні середні потужності [1]:

для похибки перетворення $\varepsilon(t,\tau)$

$$\overline{\varepsilon^2(t,\tau)_{min}} = \overline{z_a^2(t)}\left[1-\rho^2_{n_e z_a}(\tau\ )\right] \quad (8)$$

Для загального вихідного сигналу $z_a(t)$ – значення $\overline{z_a^2(t)}$ і для вихідного корисного сигналу $n_e(t)$ – середню потужність $\overline{n_e^2(t)}$. З їх допомогою можна визначити наступні види ентропії:

- вихідну ентропію або ентропію джерела $I(n_e)$;
- вихідну ентропію $I(z_a)$;
- ентропію похибки перетворення (ентропію обумовлену завадами) – розсіювання або невизначенність інформації $N(z_a|n_e)$;
- передавальну функцію $I(n_e; z_a)$;
- загальну ентропію $I(n_e, z_a)$;
- апріорну ентропію або невизначеність $I(n_e|z_a)$.

Визначемо вхідну ентропію або ентропію джерела $I(n_e)$. Для цієї, так само як і для $G(j\omega) = 1$ справедливе співвідношення:

$$I(n_e) = \frac{1}{2}\log\left[2\pi e\overline{n_e^2(t)}\right] + \lim_{\Delta x\to 0}\log\frac{1}{\Delta x} \quad (9)$$

або

$$I(n_e) = \frac{1}{2}\log\left[2\pi e\int_0^\infty P_{ne}(\omega)d\omega\right] + \lim_{\Delta x\to 0}\log\frac{1}{\Delta x}\ . \quad (10)$$

Визначемо вихідну ентропію $I(z_a)$. За аналогією з рівнянням (9) ентропія вихідного сигналу, або вихідна ентропія $I(z_a)$ виразиться рівнянням:

$$I(z_{ae}) = \frac{1}{2}\log\left[2\pi e\overline{z_e^2(t)}\right] + \lim_{\Delta x\to 0}\log\frac{1}{\Delta x} \quad (11)$$

або

$$I(z_a) = \frac{1}{2}\log\left[2\pi e\int_0^\infty\{P_{ne}(\omega) + P_{ze}(\omega)\}|G(j,\omega)|^2 d\omega\right] + \lim_{\Delta x\to 0}\log\frac{1}{\Delta x}. \quad (12)$$

Визначемо ентропію похибки перетворення (ентропію обумовлену завадами) – розсіювання або невизначенність інформації $I(z_a|n_e)$. З урахуванням рівняння (8) і (9) для цієї ентропії отримаємо:

$$I(z_a|n_e) = \frac{1}{2}\log\left[2\pi e\overline{\varepsilon^2(t,\tau)_{min}}\right] + \lim_{\Delta x\to 0}\log\frac{1}{\Delta x} \quad (13)$$

або

$$I(z_a|n_e) = \frac{1}{2}\log\left[2\pi e\overline{z_e^2(t)}\left(1-\rho^2_{n_e z_a}(\tau)\right)\right] + \lim_{\Delta x\to 0}\log\frac{1}{\Delta x}\ . \quad (14)$$

Визначемо передавальну функцію $I(n_e; z_a)$. За аналогією з рівнянням (4) для власне переданої інформації безпосередньо отримуємо:

$$I(n_e, \tau; z_a) = \frac{1}{2}\log\frac{\overline{z_a^2(t)}}{\overline{\varepsilon^2(t,\tau)_{min}}} \quad (15)$$

або з урахуванням рівняння (8):

$$I(n_e, \tau; z_a) = \frac{1}{2}\log\frac{1}{1-\rho^2_{n_e z_a}(\tau).} \quad (16)$$

Передана інформація $I(n_e, \tau; z_a)$ в принципі є інформацією, що міститься в загальному вихідному сигналі по відношенню до вхідного корисного сигналу при заздалегідь заданій системі передачі. Слід вказати [2,3], що розкладаючи сигнал на корельовану з іншими сигналами і не корельовану з ним компонентами, приходять до того ж результату, який отриманий нами в рівнянні (7).

Тоді як у ідеальної системи $G(j\omega) = 1$ загальний сигнал $z_a(t) = z_e(t)$ містить лише компоненту сигналу завади, в даному загальному випадку [система $G(j\omega)$] в похибці перетворення повинні враховуватися також лінійні спотворення корисного сигналу. Як витікає з рівнянь (15) і (16), для обчислення переданої інформації необхідно знати так звану

середньо-квадратичну відносну похибку перетворення 2-го роду $\overline{\varepsilon^2(t,\tau)_{min}}/\overline{z_a^2(t)}$ і нормовану кореляційну функцію $\rho_{n_в z_a}(\tau)$.

Вибравши правильно компенсаційну систему m, можна визначити при постійному параметрі τ мінімальну для даного τ похибку $\overline{\varepsilon^2(t,\tau)_{min}}$ або нормовану взаємно кореляційну функцію $\rho_{n_в z_a}(\tau)$. При досягненні $\tau=\tau_{опт}$ виходить мінімальна для вхідних сигналів, а також для заданої системи передачі, похибка перетворення $\varepsilon^2(t,\tau_{опт})_{min}$ і одночасно максимальна взаємно кореляційна функція $\rho_{n_в z_a}(\tau_{опт})$. Таким чином, при заданій ВОЛЗ можна визначити інформацію, яка міститься в загальному вихідному сигналі по відношенню до вихідного корисного сигналу. Отже, для визначення переданої інформації важливим є вибір оптимального параметра $\tau_{опт.}$. Цей час відповідає середньому часу затримки, або середньому часу проходження сигналу через лінію зв'язку. Якщо між вхідними сигналами не існує статистичної залежності і припускається, що вхідним корисним сигналом є білий шум, справедливе [4] співвідношення:

$$\psi n_в z_a(\tau) = const\ g(\tau), \tag{17}$$

де $g(\tau)$ – вагова функція ВОЛЗ.

В цьому випадку можна встановити пряму залежність між похибкою і ваговою функцією. Оскільки білий шум фізично не реалізовується, слід прийняти верхнє обмеження смуги пропускання. В цьому випадку рівняння (17) виявляється справедливим лише приблизно, але воно виконується тим точніше, чим вища верхня гранична частота системи передачі. При цьому можна припустити:

$$\overline{\varepsilon^2(t,\tau)_{min}} \approx \overline{z_a^2(t)}\left\{1-\left[\frac{const}{\sqrt{n_в^2(\tau)z_a^2(t)}}\right]^2 g^2(\tau)\right\} . \tag{18}$$

Отже, для цього випадку похибка $\varepsilon^2(t,\tau)$ буде приблизно мінімальною, коли вагова функція $g(\tau)$ досягне максимуму, тобто після часу $\tau_{опт}$.

$I(n_в,\tau_{опт};z_a)$ відповідає інформації, переданій при заданих сигналах, якщо не вводиться кореляція.

Очевидно, оцінку кількості передаваної за допомогою ВОЛЗ інформації

$$I(n_в,\tau_{опт};z_a)=\frac{1}{2}\log\frac{1}{1-\rho^2_{n_в z_a}(\tau_{опт})} \tag{19}$$

використовують лише у разі кореляційного аналізу, зокрема при визначенні максимального значення взаємно кореляційної функції. Якщо представити рівняння (19) у формі, аналогічній (15), можна записати

$$I(n_в,\tau_{опт};z_a)=\frac{1}{2}\log\frac{\overline{z_a^2(\tau)}}{\overline{\varepsilon^2(t,\tau_{опт})_{min}}} . \tag{20}$$

За допомогою кореляційного аналізу можна зменшити середньоквадратичну похибку перетворення, при цьому для даної системи граничне значення виражається рівнянням:

$$\overline{\varepsilon^2(t,\tau_{опт})_{min}}=z_a^2(t)\left[1-\rho^2_{n_в z_a}(\tau_{опт})\right] \tag{21}$$

Але тим самим для заданої системи перетворення максимальним буде також відношення $\overline{z_a^2(t)}/\overline{\varepsilon^2(t,\tau)_{min}}$.

Частка інформації, яка відбирається з вихідного сигналу по відношенню до вхідного корисного сигналу, значною мірою залежить від виду обробки.

Кореляційний аналіз, що робиться з метою визначення оцінюваної інформації, можна назвати депозируванням з пам'яттю [5]. Оскільки кількість передаваної інформації для даної системи відома або її можна обчислити згідно рівняння (19), можна оцінити, чи дає підвищення технічних витрат при обробці (кореляційному аналізі) помітне збільшення кількості оброблюваної інформації. Проте при цьому не можна перевершити значення, визначуване рівнянням (19), оскільки в цьому випадку передавана системою і отримана інформація будуть ідентичними.

Для випадку $\rho_{n_в z_а} = 1$, тобто для строгої функціональної залежності між загальним вихідним сигналом $z_а(t)$ і вихідним корисним сигналом $n_в(t)$, передана інформація є великою, що також легко зрозуміти з функції процесів. При зникаючій залежності між $n_в(t)$ і $z_а(t)$ вихідний сигнал складається тільки з сигналу завади, тобто від джерела до приймача по ВОЛЗ не передається ніякої інформації. З цих розглядів знов виходить, що передана інформація має основоположні значення при перетворенні і передачі її по ВОЛЗ.

З рівняння (16) безпосередньо можна отримати рівняння (6), якщо прийняти $z_а(t) = z_в(t)$ і припустити відсутність кореляції вхідних сигналів.

Визначемо загальну ентропію $I(n_в; z_а)$. Загальну ентропію переданих і прийнятих сигналів можна отримати підсумовуючи ентропію джерела $I(n_в)$ і обумовлену завадами ентропію $I(z_а|n_в)$:

$$I(n_в, z_а) = I(n_в) + I(z_а|n_в) \tag{22}$$

або

$$I(n_в, z_а) = \frac{1}{2}\log\left[(2\pi e)^2 \overline{n_в^2(t) z_а^2(t)}\left\{1 - \rho^2_{n_в z_а}(\tau)\right\}\right] + 2\lim_{\Delta x \to 0}\log\frac{1}{\Delta x} \tag{23}$$

Висновки

Отримані результати і досліджені типи ентропії інформації при наявності завад в оптико-волоконних системах зв'язку дозволять покращити ефективність передачі інформації в ВОЛЗ, крім того створять передумови для проектування засобів захисту інформації в системах передачі інформації з використанням ВОЛЗ, а також можуть використовуватись для оцінки захищеності інформації.

Список літератури

1. Краус М. Измерительные информационные системы Краус М., Вошни. Э. – М.: Изд. Мир, 1975 – 310с.

2. Гельфанд И.М. О вычислении количества информации о случайной функции, содержащейся в другой такой функции/ Гельфанд И.М., Яглом А.М.// Успехи математической науки, 12, № 1, 1957. – с.3-52.

3. Гельфанд И.М. К общему определению количества информации/ Гельфанд И.М., Колмогоров А.Н., Яглом И.М. – ДАН СССР, 111, 1956. – с.743-745.

4. Ланге Ф. Корреляционная электроника. Основы и применение корреляционного анализа в современной технике связи, измерений и регулировании/ Ланге Ф. – Л.: Судпромгиз, 1963. – 346 с.

5. Фриман Р. – Оптические системы связи/ Фриман Р. –М.:Техносфера, 2003.

6. Гринфилд Д. – Оптические сети/ Гринфилд Д. –К.:ООО «Тид «ДС»,2002.- 256с.

7. Шеннон К.Е. – Математическая теория связи. Теория передачи электрических сигналов при наличии помех./ Шеннон К.Е.– М.:, ИЛ, 1953. – 253 с.

В роботі наводяться відомості про ентропії інформації в волоконно-оптичних лініях зв'язку. Проведено більш детальний аналіз різних типів ентропій, а саме: ентропії системи передачі з частковою характеристикою при наявності завад, ентропії загального випадку, ентропії джерела, вихідної ентропії тощо.

В работе наводятся сведения об энтропиях информации в волоконно-оптических линиях связи. Проведен более детальный анализ разных типов энтропий, а именно: ентропии системы передачи с частичной характеристикой при наличии помех, энтропии общего случая, энтропии источника, исходной энтропии и других видов энтропий.

Information is in-process pointed about entropii of information in optical-fibre flow lines. More detailed analysis of different types of entropiy is conducted, namely: entropy of the system of transmission is with partial description at presence of hindrances, entropy of general case, entropy of source, initial entropy and others like that.

Рецензент: Козловський В.В.
Надійшла 17.04.2010