УДК 621.391

АУТЕНТИФІКАЦІЯ КОРИСТУВАЧІВ НА ФІЗИЧНОМУ РІВНІ В РАДІОМЕРЕЖІ УПРАВЛІННЯ

А.М. Носик
(подав д.т.н., проф. Ю.В. Стасєв)

Проводиться аналіз аутентифікації користувачів в радіомережі управління з множинним доступом при використанні фазоманіпульованих сигналів.

Одним із головних елементів, що визначають механізм захисту інформації в радіомережі управління, є метод багатостанційного доступу, що забезпечує вирішення конфліктів та децентралізованого управління в радіомережі управління. Проте реалізація цього методу висуває на перший план проблему аутентифікації користувачів та інформації, що циркулює в каналі радіомережі управління.

Проведемо аналіз аутентифікації користувачів в радіомережі управління з множинним доступом на фізичному рівні при використанні фазоманіпульованих сигналів (ФМ).

Кількісно аутентифікація на фізичному рівні оцінюється імовірністю прийому хибного сигналу $\mathbf{P_x}$. Тоді, при використанні в радіомережі управління ФМ сигналів, імовірність прийому помилкового сигналу з обліком дії в радіомережі, шуму та сигналів, що перешкоджають, запишеться у вигляді

$$\mathbf{P_x = P_п P_c + (1 - P_п) P_м}, \qquad (1)$$

де $\mathbf{P_п}$ - імовірність постановки заважаючого сигналу;

$\mathbf{P_c}$ - імовірність помилки при дії заважаючого сигналу;

$\mathbf{P_м}$ - імовірність помилки при відсутності заважаючого сигналу.

Для обчислення $\mathbf{P_м}$ і $\mathbf{P_c}$ потрібно знайти щільність розподілу імовірностей випадкового розміру, що характеризує амплітуду напруги на вході вирішального пристрою в момент повної згортки сигналу [1]. Умовна щільність розподілу імовірностей на вході синфазного і квадратурного каналів некогерентного приймача, де діє корисний сигнал, що заважає сигнал і шум, є узагальнена релеєвська щільність, а щільність на виході каналу де діє шум є просто релеєвська щільність [1].

У результаті безумовна щільність розподілу імовірності на вході вирішального пристрою має вигляд

$$\varpi^{C}_{ВХВП}(y)=\int\limits_{0}^{1}\int\limits_{E_i-E_M R}^{E_i+E_M R}\varpi(\alpha/R)\int\limits_{a}^{\infty}\varpi(y/\alpha)dx\,d\alpha\,dR, \qquad (2)$$

де (α/R) - щільність розподілу імовірності випадкової величини α, що є функцією випадкових величин $(\varphi_c-\varphi_м)$ і ступеня кореляції сигналів R;

$\varpi(y/\alpha)$ - умовна щільність імовірності, що характеризує напругу на вході вирішального пристрою, при дії сигналу , що заважає; E_i і $E_м$ - енергія корисного і перешкоджаючого сигналів; $a = 0$, якщо $y > 0$ та $a = -y$, якщо $y > 0$.

У [1] показано, що розподіл косинуса різниці фаз, незалежних і рівномірно розподілених на інтервалі $[-\pi,\pi]$, еквівалентний розподілу косинуса рівномірно розподіленої на інтервалі $[-\pi,\pi]$ випадкової величини. Аналогічно позначимо $\xi=\cos(\varphi_c-\varphi_м)$. Функція розподілу випадкового величини ξ визначається як

$$\varpi_{\xi}(x)=\frac{1}{\pi}\sqrt{1-x^2}\,.$$

Звідси

$$\varpi_{\alpha}(y)=\varpi_{\xi}[\psi(y)]\frac{d\psi(y)}{dy}, \qquad (3)$$

де $x=\psi(y)$ - зворотна функція для $\alpha=\varphi(\xi)$.

З урахуванням (3) $\varpi(y/R)$ має вигляд

$$\varpi(y/R)=\frac{\alpha}{\pi E_i E_м R\sqrt{1-\left(\dfrac{\alpha^2-Ei^2-Eм^2R^2}{2EiEмR}\right)^2}}\,. \qquad (4)$$

Умовна щільність розподілу імовірності випадкової величини, що характеризує напругу на вході вирішального пристрою некогерентного приймача при дії на робочий сигнал заважаючого сигналу, має вигляд [1]:

$$\varpi(y/\alpha)=\int\limits_{a}^{\infty}\frac{x}{\sigma_0^{\,2}}\exp\left\{-\frac{x^2+\alpha^2}{2\sigma_0^{\,2}}\right\}I_0\left(\frac{x_0\alpha}{\sigma_0^{\,2}}\right)\frac{x+y}{\sigma_0^{\,2}}\exp\left\{-\frac{(x+y)^2}{2\sigma_0^{\,2}}\right\}dx, \qquad (5)$$

де $\sigma_0^{\,2}$ - дисперсія розподілу; I_0 - функція Беселя нульового порядку.

Підставивши (4), (5) у (2) визначимо вірогідність P_c наступним виразом:

$$P_c=\int_0^1\int_a^\infty \frac{x}{\sigma_0^2}\exp\left\{-\frac{x^2+\alpha^2}{2\sigma_0^2}\right\}I_0\left(\frac{x_\alpha}{\sigma_0^2}\right)\int_0^\infty \frac{x+y}{\sigma_0^2}\exp\left\{-\frac{x^2+\alpha^2}{2\sigma_0^2}\right\}dx\times$$
$$\times\int_{E_i-E_м R}^{E_i+E_м R}\frac{\alpha}{\pi E_i E_м R\sqrt{1-\left(\frac{\alpha^2-E_i^2-E_м^2R^2}{2E_iE_мR}\right)^2}}dxdrdyda \qquad (6)$$

У [1] показано, що подвійний інтеграл по **x**, **y** дорівнює $0{,}5\exp\left\{-\alpha^2/4\sigma_0^2\right\}$. Отже, P_c має вигляд

$$P_c=\int_0^1\int_{E_i-E_м R}^{E_i+E_м R}0{,}5\exp\left\{-\frac{\alpha^2}{4\sigma_0^2}\right\}\frac{\alpha}{\pi E_i E_м R\sqrt{1-\left(\frac{\alpha^2-E_i^2-E_м^2R^2}{2E_iE_мR}\right)^2}}d\alpha dr. \qquad (7)$$

Використовуючи [2] перетворимо вираз (7) до вигляду

$$P_c=\frac{\sqrt{2\pi}}{4\pi h_i h_м}\exp^{-0{,}5h_i^2}\left\{(h_i+h_м)\Phi(h_м+h_i)-(h_м-h_i)\Phi(h_м-h_i)+\right.$$
$$\left.+\frac{2}{\sqrt{2\pi}}\left\{e^{-0{,}5(h_м+h_i)^2}-e^{-0{,}5(h_м-h_i)^2}\right\}\right\}, \qquad (8)$$

де $\Phi(Z)$ - функція Крампа;

$h_j=\sqrt{\frac{E_j}{N_0}}$; N_0 - спектральна потужність шуму.

Для обчислення $P_м$ необхідно знайти щільності розподілу на виході каналу, де діє корисний сигнал і шум, та каналу, де діє перешкоджаючий сигнал і шум. Обидва ці розподіли є узагальнені релеєвські розподіли.

Імовірність прийому помилкового сигналу $P_м$ визначається інтегралом аналогічним (6):

$$P_м=\int_0^1\int_0^\infty\frac{x}{\sigma_0^2}\exp\left\{-\frac{x^2+Ei^2}{2\sigma_0^2}\right\}I_0\left(\frac{xEi}{\sigma_0^2}\right)\int_0^\infty\frac{(x+y)}{\sigma_0^2}\times$$
$$\times\exp\left\{-\frac{(y+x)^2+E_мR}{2\sigma_0^2}\right\}I_0\left\{\frac{(x+y)+E_мR}{\sigma_0^2}\right\}dydxdr. \qquad (9)$$

Інтеграл (9) за аналогією з [1] може бути приведений до виду

$$P_м = 1 - \left(\frac{e^{-0.5 h_i^2}}{3\sqrt{2\pi} h_i h_м} \right) \Big\{ (h_м + h_i)^3 \Phi(h_м + h_i) - (h_м - h_i)^2 \times \Phi(h_м - h_i) + \tag{10}$$

$$+ \frac{2}{2\pi} \left\{ (h_м + h_i)^2 e^{-0,5(h_м + h_i)^2} - (h_м - h_i)^2 e^{-0,5(h_м - h_i)^2} \right\} \Big\}.$$

Імовірність помилки через дію шуму $P_ш$ дорівнює

$$P_ш = 0.5 e^{-0.5 h_i} . \tag{11}$$

Імовірність постановки хибного ФМ сигналу з заданим ступенем кореляції визначаться виразом [3]:

$$P_п = \frac{1}{0.125L \left[(1+R)^{1+R} (1-R)^{1-R} \right]^{0.5L}} ; \tag{12}$$

$$P_х = \frac{1}{0.125L \left[(1+R)^{1+R} (1-R)^{1-R} \right]^{0.5L}} \frac{\sqrt{2\pi}}{4\pi h_i h_м} e^{-0.5 h_i^2} \{ (h_i + h_м) \times$$

$$\times \Phi(h_м + h_i) - (h_м - h_i) \Phi(h_м - h_i) + \frac{2}{\sqrt{2\pi}} x [e^{-0.5(h_м + h_i)^2} - \tag{13}$$

$$- e^{-0.5(h_м - h_i)^2}] \} + 0.5 \frac{1}{0.125L \left[(1+R)^{1+R} (1-R)^{1-R} \right]^{0.5L}} e^{-0.5 h_i} .$$

З використанням виразу (13) був проведений аналіз імовірності нав'язування хибного сигналу. Отже імітостійкість і перешкодозахищеність радіомережі може бути підвищена за рахунок розширення ансамблю використовуваних сигналів, збільшення ступеня невизначеності конкретної форми сигналу, а також зменшення ступеня кореляції між сигналами.

ЛІТЕРАТУРА

1. Пышкин И.М. Теория кодового разделения сигналов. – М.: Связь, 1980. – 208 с.

2. Бейтман Г., Эрдели А. Таблицы интегральных преобразований. – М.: Наука, 1969. – 582 с.

3. Варакин Л.Е. Теория систем сигналов. – М.: Сов. радио, 1978. – 304 с.

Надійшла до редколегії 5.09.2000