УДК 621.391

Ю. В. СТАСЕВ, канд. техн. наук

АУТЕНТИФИКАЦИЯ ПАКЕТНОЙ СЕТИ С МНОЖЕСТВЕННЫМ ДОСТУПОМ

Особенности передачи информации в пакетных сетях с множественным доступом предопределяют необходимость рассмотрения проблемы аутентификации информации, циркулирующей в сети. Проведенные к настоящему времени исследования показывают [1], что проблему аутентификации сообщений целесообразно рас-

сматривать, используя трехуровневую модель: аутентификацию на уровне передаваемых пакетов, аутентификацию на уровне кодовых слов и аутентификацию на уровне сигналов.

Проводится оценка аутентификации пакетной сети с множественным доступом на уровне сигналов. Пусть в пакетной сети с множественным доступом используются сложные сигналы с псевдослучайной перестройкой рабочей частоты (ППРЧ), фазоманипулированные (ФМ) сигналы или ППРЧ-ФМ сигналы. Количественно аутентификация оценивается вероятностью приема ложного сигнала $P_л$.

Тогда, при использовании в пакетной сети с множественным доступом ППРЧ сигналов, вероятность приема ложного сигнала с учетом действия в радиоканале шума и мешающих сигналов запишется в виде

$$P_л = P_п (P_м + P_с) + (1 - P_п) P_ш. \qquad (1)$$

Здесь $P_п$ — априорная вероятность попадания мешающего сигнала в разрешенный в данный момент времени частотный диапазон; $P_м$ — условная вероятность приема ложного сигнала при воздействии мешающего сигнала в канале, где сигнал отсутствует; $P_с$ — условная вероятность переименования сигнала при воздействии на него мешающего сигнала и шума; $P_ш$ — вероятность ошибки из-за действия шума.

Для вычисления $P_м$ и $P_с$, как показано в работе [2], требуется найти плотность распределения вероятностей случайной величины, характеризующей амплитуду напряжений на входе решающего устройства в момент полной свертки сигнала. Условная плотность распределения вероятностей напряжений на выходе синфазного и квадратурного каналов некогерентного приемника, где действует полезный сигнал, мешающий сигнал и шум, есть обобщенная рэлеевская плотность, а плотность на выходе канала, где действует шум, есть просто рэлеевская плотность [2].

В результате безусловная плотность распределения вероятности напряжения на входе решающего устройства имеет вид

$$\omega^{c}_{\text{вх.ру}}(y) = \int_0^1 \int_{E_i - E_м R}^{E_i + E_м R} \omega(\alpha/R) \cdot \int_a^{\infty} \omega(y/\alpha)\, dy\, d\alpha\, dR, \qquad (2)$$

где $\omega(\alpha/R)$ — плотность распределения вероятности случайной величины α, являющейся функцией случайных величин ($\varphi_с - \varphi_м$) и степени корреляции сигналов R; $\omega(y/\alpha)$ — условная плотность вероятности, характеризующая напряжение на входе решающего устройства при действии мешающего сигнала; E_i и $E_м$ — энергии полезного и мешающего сигналов; $a = \begin{cases} 0 & \text{при } y > 0, \\ -y & \text{при } y < 0. \end{cases}$

В работе [3] показано, что распределение косинуса разности фаз, независимых и равномерно распределенных на интервале $[-\pi, \pi]$, эквивалентно распределению косинуса равномерно распределенной на интервале $[-\pi, \pi]$, случайной величины. Анало-

гично [3] обозначим $\xi = \cos(\varphi_c - \varphi_м)$. Функция распределения случайной величины ξ как

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

Отсюда

$$\omega_\alpha(y) = \omega_\xi[\psi(y)]\frac{d\psi(y)}{d(y)}, \tag{3}$$

где $x = \psi(y)$ — обратная функция для $\alpha = \varphi(\xi)$.

С учетом (3) $\omega(\alpha/R)$ имеет вид

$$\omega(\alpha/R) = \frac{\alpha}{\pi E_i E_м R\sqrt{1-\left(\frac{\alpha^2 - E_i^2 - E_м^2 R^2}{2E_i - E_м R}\right)^2}}. \tag{4}$$

Условная плотность распределения вероятности случайной величины, характеризующей напряжение на входе решающего устройства некогерентного приемника при действии на рабочий сигнал мешающего сигнала имеет вид [2]

$$\omega(y/\alpha) = \int_a^\infty \frac{x}{\sigma_0}\exp\left\{-\frac{x^2+\alpha^2}{2\sigma_0^2}\right\} I_0\left(\frac{x\alpha}{\sigma_0^2}\right)\frac{x+y}{\sigma_0^2}\exp\left\{-\frac{(x+y^2)}{2\sigma_0^2}\right\} dx, \tag{5}$$

где σ_0^2 — дисперсия распределения; I_0 — функция Бесселя нулевого порядка. Подставив (4), (5) в (2), определим вероятность P_c:

$$P_c = \int_0^1\int_0^\infty \frac{x}{\sigma_0^2}\exp\left\{-\frac{x^2+\alpha^2}{2\sigma_0^2}\right\} I_0\left(\frac{x\alpha}{\sigma_0^2}\right)\int_0^\infty \frac{x+y}{\sigma_0^2}\exp\left\{-\frac{x^2+\alpha^2}{2\sigma_0^2}\right\}\int_{E_i-E_м R}^{E_i+E_м R}\alpha :$$

$$: \pi E_i E_м R\sqrt{1-\left(\frac{\alpha^2 - E_i^2 - E_м^2 R^2}{2E_i E_м R}\right)^2}\, dR\, dx\, dy\, d\alpha, \tag{6}$$

В работе [2] показано, что двойной интеграл по x, y равен $0{,}5\exp\{-\alpha^2/4\sigma_0^2\}$. Следовательно, P_c имеет вид

$$P_c = \int_0^1\int_{E_i-E_м R}^{E_i+E_м R} 0{,}5\exp\left\{-\frac{\alpha^2}{4\sigma_0^2}\right\} \times$$

$$\times \frac{\alpha}{\pi E_i E_м R\sqrt{1-\left(\frac{\alpha^2 - E_i^2 - E_м^2 R^2}{2E_i E_м R}\right)^2}}\, d\alpha\, dR. \tag{7}$$

Используя [4], преобразуем выражение (7) к виду

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

$$\left. + \frac{2}{\sqrt{2\pi}}\{e^{-0{,}5(h_м+h_i)^2} - e^{-0{,}5(h_м-h_i)^2}\}\right\}, \tag{8}$$

где $\Phi(z)$ — функция Крампа; $h_i = \sqrt{\frac{E_i}{N^0}}$; N_0 — спектральная мощность шума.

Для вычисления $P_м$ необходимо найти плотности распределения на выходе канала, где действует полезный сигнал и шум, и канала, где действует мешающий сигнал и шум. Оба эти распределения — обобщенные рэлеевские распределения.

Вероятность приема ложного сигнала $P_м$ определяется интегралом, аналогичным (6)

$$P_м = \int_0^1 \int_0^\infty \frac{x}{\sigma_0^2} \exp\left\{-\frac{x^2 + E_i^2}{2\sigma_0^2}\right\} I_0\left(\frac{xE_i}{\sigma_0^2}\right) \int_0^\infty \frac{(y+x)}{\sigma_0^2} \exp\left\{-\frac{(y+x)^2 + E_м R}{2\sigma_0^2}\right\} \times$$

$$\times I_0\left\{\frac{(y+x)E_м R}{\sigma_0^2}\right\} dy\, dx\, dR, \qquad (9)$$

Интеграл (9) после громоздких преобразований по аналогии с работой [2] может быть приведен к виду

$$P_м = 1 - \left(\frac{e^{-0,5h_i^2}}{3\sqrt{2\pi}h_i h_м}\right)\left\{(h_м + h_i)^3 \Phi(h_м + h_i) - (h_м - h_i)^3 \Phi(h_м - h_i) + \right.$$

$$\left. + \frac{2}{\sqrt{2\pi}}\{(h_м + h_i)^2 e^{-0,5(h_м+h_i)^2} - (h_м - h_i)^2 e^{-0,5(h_м-h_i)^2}\}\right\}. \qquad (10)$$

Вероятность $P_ш$ ошибки из-за действия шума равна [2] $P_ш = 0,5e^{-0,5h_i^2}$ (11). После подстановки (8), (10), (11) в (1) получим

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

$$+ \frac{2}{\sqrt{2\pi}}\{e^{-0,5(h_м+h_i)^2} - e^{-0,5(h_м-h_i)^2}\} + \left\{1 - \left(\frac{e^{-0,5h_i^2}}{3\sqrt{2\pi}h_i h_м}\right) \times \right.$$

$$\times \left\{(h_м + h_i)^3 \Phi(h_м + h_i) - (h_м - h_i)^3 \Phi(h_м - h_i) + \frac{2}{\sqrt{2\pi}}[(h_м + h_i)^2 \times \right.$$

$$\left.\left.\left. \times e^{-0,5(h_м+h_i)^2} - (h_м - h_i)^2 e^{-0,5(h_м-h_i)^2}]\right\}\right\} + 0,5(1 - P_п) e^{-0,5h_i^2} \qquad (12)$$

При использовании в пакетной сети с множественным доступом ФМ сигналов вероятность приема ложного сигнала равна

$$P_л = P_п P_с + (1 - P_п) P_ш. \qquad (13)$$

Выражение для вычисления $P_с$ для случая использования в пакетной сети с множественным доступом ФМ сигналов совпадает с (8). Однако надо помнить, что $h_м$ в $\sqrt{L}$ раз меньше $h_м$ при использовании ППРЧ сигналов, где L — число элементов ФМ сигнала.

Вероятность постановки ложного ФМ сигнала с заданной степенью корреляции определяется выражением [5]:

$$P_п = \frac{1}{0,125L\,[(1+R)^{1+R}(1-R)^{1-R}]^{0,5L}} \qquad (14)$$

С учетом высказанных замечаний выражение для $P_л$ запишется в виде

$$P_л = \frac{1}{0{,}125L\,[(1+R)^{1+R}(1-R)^{1-R}]^{0{,}5L}} \frac{\sqrt{2\pi}}{4\pi h_i h_м} e^{-0{,}5h_i^2} \left\{ (h_i + h_м)\,\Phi \times \right.$$

$$\times (h_м + h_i) - (h_м - h_i)\,\Phi (h_м - h_i) + \frac{2}{\sqrt{2\pi}} [e^{-0{,}5(h_м+h_i)^2} - e^{-0{,}5(h_м-h_i)^2}] \Big\} +$$

$$+ 0{,}5 \left[1 - \frac{1}{0{,}125L\,[(1+R)^{1+R}(1-R)^{1-R}]^{0{,}5L}} \right] e^{-0{,}5h_i^2}. \qquad (15)$$

При использовании ППРЧ-ФМ сигнала вероятность приема ложного сигнала запишется как

$$P_л = P_{\text{ппрч}} [P_{\text{пфм}} (P_м + P_с) + (1 - P_{\text{пфм}}) P_ш] + (1 - P_{\text{ппрч}}) P_ш. \qquad (16)$$

Подставив значения переменных, входящих в выражение (16), получим

$$P_л = P_{\text{ппрч}} \left\{ \frac{1}{0{,}125L\,[(1+R)^{1+R}(1-R)^{1-R}]^{0{,}5L}} \times \right.$$

$$\times \left\{ 1 - \frac{e^{-0{,}5h_i^2}}{3\sqrt{2\pi} h_i h_м} \left\{ (h_м + h_i)^3\,\Phi (h_м + h_i) - (h_м - h_i)^3\,\Phi (h_м - h_i) + \right. \right.$$

$$+ \frac{2}{\sqrt{2\pi}} [(h_м + h_i)^2 e^{-0{,}5(h_м+h_i)^2} - (h_м - h_i)^2 e^{-0{,}5(h_м-h_i)^2}] \Big\} +$$

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

$$\left. \left. \times [e^{-0{,}5(h_м+h_i)^2} - e^{-0{,}5(h_м-h_i)^2}] \right\} \right\} +$$

$$+ 0{,}5 \left[1 - \frac{1}{0{,}125L\,[(1+R)^{1+R}(1-R)^{1-R}]^{0{,}5L}} \right] e^{-0{,}5h_i^2} + 0{,}5\,(1 - P_{\text{ппрч}})\, e^{-0{,}5h_i^2}. \qquad (17)$$

По формулам (12), (15), (17) можно провести анализ аутентификации пакетной сети с множественным доступом при некогерентном приеме для различных значений h_i, $h_м$ и $P_п$.

Список литературы: 1. *Эфремидес Э., Уизелтир Дж. Э., Бейкер Д. Дж.* Вопросы проектирования надежных мобильных радиосетей, использующих методы передачи и приема сигналов с псевдослучайной перестройкой рабочей частоты // Тр. Ин-та инж. по электротехнике и радиоэлектронике. 1987. Т. 75, № 1, С. 68—90. 2. *Пышкин И. М.* Теория кодового разделения сигналов. М., 1980. 208 с. 3. *Левин Б. Р.* Теоретические основы статистической радиотехники. Кн. 3. М., 1976. 386 с. 4. *Бейтман Г., Эрдели А.* Таблицы интегральных преобразований. М., 1969, Т. 1. С. 569. 5. *Варакин Л. Е.* Теория систем сигналов. М., 1970. 240 с.

Поступила в редколлегию 11.04.90