Космічна наука і технологія. 1997. Т. 3. № 1/2. С. 83—86.

УДК 621.391.372.019.3

Аутентификация в космических системах связи и управления с множественным доступом

Ю. В. Стасев[1], И. Д. Горбенко[2], Н. В. Пастухов[1]

[1]Харківський військовий університет

[2]Інститут інформаційних технологій НАН України, Харків

Надійшла до редакції 28.05.96

Приводиться аналіз аутентифікації космічних систем зв'язку і керування на фізичному рівні. Показано, що розв'язок проблеми аутентифікації можливий при реалізації динамічного режиму функціонування та використанні великих ансамблів слабокорельованих складних сигналів.

Одним из главных элементов, определяющих механизм защиты информации в космических системах связи и управления, является метод многостанционного доступа к каналу. Среди известных методов многостанционного доступа, обеспечивающих разрешение конфликтов и децентрализацию управления в космических системах связи, выделяют метод с кодовым разделением каналов. Однако реализация метода кодового разделения каналов в космических системах связи и управления выдвигает на первый план проблему аутентификации пользователей и информации. В ряде работ (например в работе Тузова, 1993) аутентификацию пользователей и контроль их полномочий предлагается осуществлять на этапе обработки сигналов.

Реализация такого подхода в системах NAVSTAR, MILSTAR, «Metricom», ARDIS, «RAM Mobile» обеспечивает на физическом уровне требуемую аутентичность и конфиденциальность передаваемой информации. По мнению специалистов First National Bank реализация метода кодового разделения каналов и решения вопроса аутентификации абонентов сети на физическом уровне открывает широкие перспективы в приложениях с повышенными требованиями к безопасности передаваемой информации. В то же время сегодня остаются нерешенными вопросы аутентификации пользователей при асинхронном доступе к каналу. В предлагаемой статье проводится анализ аутентификации в космических системах связи и управления с множественным доступом при использовании сигналов с псевдослучайной перестройкой рабочей частоты (ППРЧ), фазоманипулированных сигналов (ФМ) и сигналов с псевдослучайной перестройкой рабочей частоты и дополнительной фазовой манипуляцией (ППРЧ-ФМ).

Количественно аутентификация на физическом уровне оценивается вероятностью приема ложного сигнала $P_{л}$.

Пусть в космической системе связи и управления используются сложные ППРЧ-сигналы, ФМ-сигналы или ППРЧ-ФМ-сигналы. Тогда при использовании в космических системах связи и управления ППРЧ-сигналов вероятность приема ложного сигнала с учетом действия в радиоканале шума и мешающих сигналов запишется в виде

$$P_{л} = P_{i}(P_{m} + P_{c}) + (1 - P_{i})P_{m} \qquad (1)$$

Здесь P_{i} — априорная вероятность попадания мешающего сигнала в разрешенный в данный момент времени частотный диапазон; P_{m} — условная вероятность приема ложного сигнала при воздействии мешающего сигнала в канале, где сигнал отсутст-

вует; $P_с$ — условная вероятность переименования сигнала при воздействии на него мешающего сигнала и шума; $P_о$ — вероятность ошибки из-за действия шума. Для вычисления $P_м$ и $P_с$ (Пышкин, 1980) 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 входе 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, — простая рэлеевская. Безусловная плотность распределения вероятности напряжения на входе решающего устройства имеет вид

$$\omega^{с}_{B_x p_y}(y) = \int_0^1 \int_{E_i - E_m R}^{E_i + E_m R} \omega\left(\frac{\alpha}{R}\right) \int_a^\infty \omega\left(\frac{y}{\alpha}\right) dy d\alpha dR, \quad (2)$$

где $\omega(\alpha/R)$ — плотность распределения вероятности случайной величины α, являющейся функцией случайных величин $(\varphi_с - \varphi_i)$ и степени корреляции R; $\omega(y/\alpha)$ — условная плотность вероятности, характеризующая напряжение на входе решающего устройства, при действии мешающего сигнала; E_i и E_m — энергия полезного и мешающего сигналов;

$$a = \begin{cases} 0, & y > 0, \\ -y, & y < 0. \end{cases}$$

В работе Пышкина (1980) 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. Обозначим $\xi = \cos(\varphi_с - \varphi_i)$. Функция распределения случайной величины ξ определяется как

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

Отсюда

$$\omega_\alpha(y) = \omega_\xi[\Psi(y)]\, d\Psi(y)_{dy}, \quad (3)$$

где $x = \Psi(y)$ — функция, обратная к функции $\alpha = \varphi(\xi)$. С учетом (3)

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

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

$$\omega\left(\frac{y}{\alpha}\right) = \int_a^\infty \frac{x}{\sigma_0^2} \exp\left(-\frac{x^2 + \alpha^2}{2\sigma_0^2}\right) I_0\left(\frac{x_0\alpha}{\sigma_0^2}\right) \frac{x + y}{\sigma_0^2} \times \times \exp\left(-\frac{x^2 + y^2}{2\sigma_0^2}\right) dx, \quad (5)$$

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

$$P_с = \int_0^{-1} \int_a^\infty \frac{x}{\sigma_0^2} \exp\left(-\frac{x^2 + \alpha^2}{2\sigma_0^2}\right) \times I_0\left(\frac{x_0\alpha}{\sigma_0^2}\right) \frac{x + y}{\sigma_0^2} \exp\left(-\frac{x^2 + y^2}{2\sigma_0^2}\right) \times \int_{E_i - E_m R}^{E_i + E_m R} \frac{\alpha \cdot dx dR dy d\alpha}{\pi E_i E_m R\sqrt{1 - (\alpha^2 - E_i^2 - E_m^2 R^2)^2/(2E_i E_m R)^2}}. \quad (6)$$

После ряда преобразований двойной интеграл по x, y равен $0.5\exp(-\alpha^2/4\sigma_0^2)$. Следовательно, $P_с$ имеет вид

$$P_с = \int_0^1 \int_{E_i - E_m R}^{E_i + E_m R} 0.5\exp\left(-\frac{\alpha^2}{4\sigma_0^2}\right) \times \frac{\alpha}{\pi E_i E_m R\sqrt{1 - (\alpha^2 - E_i^2 - E_m^2 R^2)^2/(2E_i E_m R)^2}} d\alpha dR. \quad (7)$$

Используя таблицы интегральных преобразований (Бетман, 1969) преобразуем выражение (7) к виду

$$P_с = \frac{\sqrt{2\pi}}{4\pi h_i h_m} \exp(-0.5h_i^2) \times \left\{(h_m + h_i)\Phi(h_m + h_i) - (h_m - h_i)\Phi(h_m - h_i) + \left\{+\frac{2}{\sqrt{2\pi}}\left[\exp[-0.5(h_m + h_i)^2] - \exp[-0.5(h_m - h_i)^2]\right]\right\}\right., \quad (8)$$

где $\Phi(z)$ — функция Крампа; $h_j = \sqrt{E_j/N_0}$; N_0 — спектральная мощность шума.

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

Вероятность приема ложного сигнала $P_т$ опреде-

ляется интегралом, аналогичным (6):

$$P_{\text{т}} = \int_0^1 \int_0^\infty \frac{x}{\sigma_0^2}\exp\left(-\frac{x^2+E_{\text{i}}^2}{2\sigma_0^2}\right) I_0\left(\frac{xE_{\text{i}}}{\sigma_0^2}\right) \times$$
$$\times \int_0^\infty \frac{y+x}{\sigma_0^2}\exp\left(-\frac{(y+x)^2+E_{\text{т}}R}{2\sigma_0^2}\right) \times$$
$$\times I_0\left(\frac{(y+x)E_{\text{т}}R}{\sigma_0^2}\right) dydxdR. \qquad (9)$$

Интеграл (9) после громоздких преобразований может быть приведен к виду

$$P_{\text{м}} = 1 - \frac{\exp(-0.5h_{\text{i}}^2)}{3\sqrt{2\pi}h_{\text{i}}h_{\text{т}}} \times$$
$$\times \left\{(h_{\text{т}}+h_{\text{i}})^3\Phi(h_{\text{т}}+h_{\text{i}}) - (h_{\text{т}}-h_{\text{i}})^3\Phi(h_{\text{т}}-h_{\text{i}}) + \right.$$
$$+ \frac{2}{2\pi}\left[(h_{\text{т}}+h_{\text{i}})^2\exp[-0.5(h_{\text{т}}+h_{\text{i}})^2] - \right.$$
$$\left.\left\{\left[- (h_{\text{т}}-h_{\text{i}})^2\exp[-0.5(h_{\text{т}}-h_{\text{i}})^2]\right]\right\}. \qquad (10)$$

Вероятность ошибки из-за действия шума $P_{\text{ш}}$ равна (Пышкин, 1980)

$$P_{\text{ш}} = 0.5\exp(-0.5h_{\text{i}}^2). \qquad (11)$$

После подстановки (8), (10), (11) в (1) получим:

$$P_{\text{л}} = P_{\text{i}}\left\{\frac{\sqrt{2\pi}}{4\pi h_{\text{i}}h_{\text{т}}}0.5\exp(-0.5h_{\text{i}}^2) \times \right.$$
$$\times \left\{(h_{\text{т}}+h_{\text{i}})\Phi(h_{\text{т}}+h_{\text{i}}) - (h_{\text{т}}-h_{\text{i}})\Phi(h_{\text{т}}-h_{\text{i}}) + \right.$$
$$+ \frac{2}{\sqrt{2\pi}}\left[\exp[-0.5(h_{\text{т}}+h_{\text{i}})^2] - \right.$$
$$\left.\left\{\left[- \exp[-0.5(h_{\text{т}}-h_{\text{i}})^2]\right]\right\} + 1 - \frac{\exp(-0.5h_{\text{i}}^2)}{3\sqrt{2\pi}h_{\text{i}}h_{\text{т}}} \times \right.$$
$$\times \left\{(h_{\text{т}}+h_{\text{i}})^3\Phi(h_{\text{т}}+h_{\text{i}}) - (h_{\text{т}}-h_{\text{i}})^3\Phi(h_{\text{т}}-h_{\text{i}}) + \right.$$
$$+ \frac{2}{\sqrt{2\pi}}\left[(h_{\text{т}}+h_{\text{i}})^2\exp[-0.5(h_{\text{т}}+h_{\text{i}})^2] - \right.$$
$$\left.\left\{\left\{\left[- (h_{\text{т}}-h_{\text{i}})^2\exp[-0.5(h_{\text{т}}-h_{\text{i}})^2]\right]\right\}\right\} +$$
$$+ 0.5(1-P_{\text{i}})\exp[-0.5h_{\text{i}}^2]. \qquad (12)$$

При использовании в космических системах связи и управления с множественным доступом ФМ-сигналов вероятность приема ложного сигнала определяется выражением

$$P_{\text{л}} = P_{\text{п}}P_{\text{с}} + (1-P_{\text{п}})P_{\text{ш}}, \qquad (13)$$

где $P_{\text{п}}$ — вероятность постановки мешающего сигнала; $P_{\text{с}}$ — вероятность ошибки при действии мешающего сигнала; $P_{\text{ш}}$ — вероятность ошибки при отсутствии мешающего сигнала. Выражение для вычисления $P_{\text{с}}$ для случая использования в космических системах связи и управления с множественным доступом ФМ сигналов совпадает с (8). Однако надо помнить, что $h_{\text{т}}$ в $\sqrt{L}$ раз меньше, чем при использовании ППРЧ-сигналов (L — число элементов ФМ-сигнала). Вероятность постановки ложного ФМ-сигнала с заданной степенью корреляции определяется выражением (Варакин, 1985)

$$P_{\text{п}} = \frac{1}{0.125L[(1+R)^{1+\text{R}}(1-R)^{1-\text{R}}]^{0.5\text{L}}}. \qquad (14)$$

С учетом высказанных замечаний выражение для $P_{\text{л}}$ запишется в виде

$$P_{\text{л}} = \frac{1}{0.125L[(1+R)^{1+\text{R}}(1-R)^{1-\text{R}}]^{0.5\text{L}}} \times$$
$$\times \frac{\sqrt{2\pi}}{4\pi h_{\text{i}}h_{\text{т}}}\exp(-0.5h_{\text{i}}^2) \times$$
$$\times \left\{(h_{\text{т}}+h_{\text{i}})\Phi(h_{\text{т}}+h_{\text{i}}) - (h_{\text{т}}-h_{\text{i}})\Phi(h_{\text{т}}-h_{\text{i}}) + \right.$$
$$+ \frac{2}{\sqrt{2\pi}}\left[\exp[-0.5(h_{\text{т}}+h_{\text{i}})^2] - \right.$$
$$\left.\left\{\left[- \exp[-0.5(h_{\text{т}}-h_{\text{i}})^2]\right]\right\} +$$
$$+ 0.5\frac{\exp(-0.5h_{\text{i}}^2)}{0.125L[(1+R)^{1+\text{R}}(1-R)^{1-\text{R}}]^{0.5\text{L}}}. \qquad (15)$$

При использовании ППРЧ-ФМ-сигнала вероятность приема ложного сигнала запишется в виде:

$$P_{\text{л}} = P_{\text{i}}[P_{\text{п}}(P_{\text{т}}+P_{\text{с}}) + (1-P_{\text{п}})P_{\text{ш}}] +$$
$$+ (1-P_{\text{i}})P_{\text{ш}}. \qquad (16)$$

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

$$P_{\text{i}} = P_{\text{р}}\left\{\frac{1}{0.125L[(1+R)^{1+\text{R}}(1-R)^{1-\text{R}}]^{0.5\text{L}}} \times \right.$$
$$\times \left\{1 - \frac{\exp(-0.5h_{\text{i}}^2)}{3\sqrt{2\pi}h_{\text{i}}h_{\text{т}}} \times \right.$$
$$\times \left\{(h_{\text{т}}+h_{\text{i}})^3\Phi(h_{\text{т}}+h_{\text{i}}) - (h_{\text{т}}-h_{\text{i}})^3\Phi(h_{\text{т}}-h_{\text{i}}) + \right.$$
$$+ \frac{2}{\sqrt{2\pi}}\left[(h_{\text{т}}+h_{\text{i}})^2\exp[-0.5(h_{\text{т}}+h_{\text{i}})^2] - \right.$$
$$\left.\left\{\left[- (h_{\text{т}}-h_{\text{i}})^2\exp[-0.5(h_{\text{т}}-h_{\text{i}})^2]\right]\right\} +$$
$$+ \frac{\sqrt{2\pi}}{4\pi h_{\text{i}}h_{\text{т}}}\exp(-0.5h_{\text{i}}^2) \times$$
$$\times \left\{(h_{\text{т}}+h_{\text{i}})\Phi(h_{\text{т}}+h_{\text{i}}) - (h_{\text{т}}-h_{\text{i}})\Phi(h_{\text{т}}-h_{\text{i}}) + \right.$$

$$+\frac{2}{\sqrt{2\pi}}\left[\exp[-0.5(h_m+h_i)^2]-\right.$$
$$\left.\left\{\left\{\left\{\left[-\exp[-0.5(h_m-h_i)^2]\right]\right\}\right\}\right\}+\right.$$
$$+0.5\left\{1-\frac{1}{0.125L[(1+R)^{1+R}(1-R)^{1-R}]^{0.5L}}\right\}\times$$
$$\times\exp(-0.5h_i^2)+0.5(1-P_i)\exp(-0.5h_i^2). \quad (17)$$

С использованием выражений (12), (15) и (17) проведен анализ вероятности навязывания ложного сигнала при передаче информации ППРЧ-, ППРЧ-ФМ- и ФМ-сигналами. Установлено, что для ППРЧ- и ППРЧ-ФМ-сигналов вероятность навязывания зависит от метода обработки и соотношения мощности сигнала и помехи на элементе ППРЧ-сигнала и количества выставляемых помех. При этом наиболее опасными являются случаи, когда отношение мощностей сигнала и помехи равно единице. Если это отношение меньше 1, то вероятность навязывания ППРЧ- и ППРЧ-ФМ-сигнала определяется вероятностью попадания помехи на разрешенную рабочую частоту.

Для ФМ-сигналов вероятность навязывания ложного сигнала зависит от энергетических соотношений сигнала и помехи и степени их корреляции. Следовательно, аутентичность космических систем связи и управления может быть повышена за счет динамической смены форм используемых сигналов, а также расширения их ансамбля и уменьшения степени корреляции между сигналами.

Таким образом, решение проблемы повышения аутентичности космических систем связи и управления на физическом уровне достигается при реализации динамической смены форм сигналов и использовании сигналов с улучшенными ансамблевыми и корреляционными характеристиками.

Бетман Г., Эрдели А. Таблицы интегральных преобразований. — М.: Наука, 1969.—Т. 1.

Варакин Л. Е. Системы связяи с шумоподобными сигналами. — М.: Радио и связь, 1985.—384 с.

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

Тузов Г. И., Урядников Ю. Ф., Прытков В. И. и др. Адресные системы управления и связи. Вопросы оптимизации / Под ред. Г. И. Тузова. — М.: Радио и связь, 1993.—384 с.

AUTHENTICATION IN SPACE SYSTEM COMMUNICATION AND CONTROL WITH NUMEROUSE ACCESS

Yu. V. Stasev, I. D. Gorbenko, and N. V. Pastukhov

Authentication in space communication and control systems is analyzed on the physical level. We show that the authentication problem can be solved in the dynamical operation mode and when vast sets of weakly correlated complex signal are used.