УДК 004.056

THE INCREASE OF TRANSMISSION PROTECTION BASED ON MULTIPLEXING OF TIMER SIGNAL CONSTRUCTIONS

Korchynskii V.V., Kildishev V.I., Osadchuk K.O.

O.S. Popov Odesa National Academy of Telecommunications,
1 Kuznechna St., Odesa, 65029, Ukraine.
vladkorchin@ukr.net

ПІДВИЩЕННЯ ЗАХИЩЕНОСТІ ПЕРЕДАВАННЯ НА ОСНОВІ МУЛЬТИПЛЕКСУВАННЯ ТАЙМЕРНИХ СИГНАЛЬНИХ КОНСТРУКЦІЙ

Корчинський В. В., Кільдішев В.Й., Осадчук К.О.

Одеська національна академія зв'язку ім. О.С. Попова,
65029, Україна, м. Одеса, вул. Кузнечна, 1.
vladkorchin@ukr.net

ПОВЫШЕНИЕ ЗАЩИЩЁННОСТИ ПЕРЕДАЧИ НА ОСНОВЕ МУЛЬТИПЛЕКСИРОВАНИЯ ТАЙМЕРНЫХ СИГНАЛЬНЫХ КОНСТРУКЦИЙ

Корчинский В. В., Кильдишев В.Й., Осадчук Е.А.

Одесская национальная академия связи им. А.С. Попова,
65029, Украина, г. Одесса, ул. Кузнечная, 1.
vladkorchin@ukr.net

Abstract. In the article the method for increasing the security of confidential information transmission based on multiplexing of timer signal structures is addressed. The feasibility of this study is justified by the need to ensure the security of information transfer in the conditions of electronic conflict. The use of OFDM technology for this task increases the noise immunity of communication systems in complex signal propagation conditions. The examples are the IEEE 802.11a and HiperLAN / 2 radio channels, as well as communication systems in which a wired channel is implemented based on ADSL. No less important task is to protect the transmitted information from unauthorized access. The majority of methods of protecting information from unauthorized access are concentrated on the upper layers of the OSI model, which is in accordance with the recommendations of X.800. Progress in improving methods and means of electronic reconnaissance and unauthorized access increases the risk of compromising certain information security mechanisms. Therefore, comprehensive approach to protecting information from unauthorized access is justified, in which not only the upper but the lower layers of the OSI model should be involved. It is proposed to use information signals of complex information that are formed by multiplexing the pulses of timer signal constructions in order to increase the transmission security at the lower levels of the OSI model. The advantage of timer signal constructions is the possibility of increasing the information transfer rate in binary channels. Also, based on timer coding, noise immunity coding and various algorithms for enhancing the structural secrecy of signal construction are implemented. The correcting ability and structural construction of the timer signals depends on the parameters of their constructions. The multiplexing method based on OFDM is designed for position signals, therefore it cannot be applied to non-position timer signal constructions. A new method for multiplexing and demultiplexing timer signal constructions is proposed. Obviously, increasing the security of OFDM technology is no less important, so the relevance of this research is beyond doubt. **The aim of the work** is to increase the security of the transmission channel on the basis of multiplexing of non-position timer signals.

Key words: security, multiplexing, timer signal constructions, secrecy, noise immunity, unauthorized access, channel.

Анотація. Доцільність даного дослідження обґрунтована необхідністю забезпечення безпеки передавання інформації в умовах радіоелектронного конфлікту. Використання для цього завдання технології OFDM підвищує стійкість систем зв'язку у складних умовах поширення сигналу. Не менш важливим завданням є захист передаваної інформації від несанкціонованого доступу. Більшість

методів захисту інформації від несанкціонованого доступу зосереджені на верхніх рівнях моделі OSI, що відповідає рекомендаціям X.800. Прогрес в області удосконалювання методів і засобів радіотехнічної розвідки та несанкціонованого доступу збільшує ризик компрометації окремих механізмів інформаційної безпеки. Тому обґрунтованим є комплексний підхід щодо захисту інформації від несанкціонованого доступу, за якого повинні бути задіяні не тільки верхні, але і нижні рівні моделі OSI. Пропонується для підвищення захищеності передавання на нижніх рівнях моделі OSI використовувати сигнали-переносники інформації зі складною структурою, які формуються шляхом мультиплексування імпульсів таймерних сигнальних конструкцій. У роботі запропоновано новий метод мультиплексування і демультиплексування непозиційних таймерних сигнальних конструкцій. Очевидно, що підвищення захищеності технології OFDM є не менш важливим завданням, тому актуальність даного дослідження не викликає сумнівів. **Метою статті** є підвищення захищеності каналу передавання на основі мультиплексування непозиційних таймерних сигналів.

Ключові слова: захищеність, мультиплексування, таймерні сигнальні конструкції, прихованість, завадостійкість, несанкціонований доступ, канал.

Аннотация. Целесообразность данного исследования обоснована необходимостью обеспечения безопасности передачи информации в условиях радиоэлектронного конфликта. Использование для этой задачи технологии OFDM повышает помехоустойчивость систем связи в сложных условиях распространения сигнала. Не менее важной задачей является защита передаваемой информации от несанкционированного доступа. Большинство методов защиты информации от несанкционированного доступа сосредоточены на верхних уровнях модели OSI, что соответствует рекомендациям X.800. Прогресс в области совершенствования методов и средств радиотехнической разведки и несанкционированного доступа увеличивает риск компрометации отдельных механизмов информационной безопасности. Поэтому обоснованным является комплексный подход по защите информации от несанкционированного доступа, при котором должны быть задействованы не только верхние, но и нижние уровни модели OSI. Предлагается для повышения защищённости передачи на нижних уровнях модели OSI использовать сигналы-переносчики информации со сложной структурой, которые формируются путем мультиплексирования импульсов таймерных сигнальных конструкций. В работе предложен новый метод мультиплексирования и демультиплексирования непозиционных таймерных сигнальных конструкций. Очевидно, что повышение защищённости технологии OFDM является не менее важной задачей, поэтому актуальность данного исследования не вызывает сомнений. **Целью статьи** является повышение защищённости канала передачи на основе мультиплексирования непозиционных таймерных сигналов.

Ключевые слова: защищённость, мультиплексирование, таймерные сигнальные конструкции, скрытность, помехоустойчивость, несанкционированный доступ, канал.

In the condition of electronic conflict, a special role is played by the construction of noise-protected communication systems. It is known [1,2], by using OFDM (Orthogonal Frequency Division Multiplex) technology, that the problem of increasing the noise immunity of communication systems in difficult signal propagation conditions is solved, both in radio channels (IEEE 802.11a and HiperLAN / 2 standards) and wired channels, e.g. an asymmetric digital subscriber line (ADSL). No less important a task is the protection of transmitted information from unauthorized access (UAA).

In accordance with the recommendations of X.800, the majority of methods of protecting information from UAA are concentrated at the upper levels of the OSI model. Progress in improving the methods and means of radio technical intelligence and UAA increases the risk of compromising certain mechanisms of information security. Therefore, a complex approach to protecting information from UAA, which involves not only the upper but lower layers of the OSI mode, is relevant.

One of the methods for increasing the transmission security at the lower layers of the OSI model is the complication of the structure of signal-carriers information [3]. In this article, it is proposed to use timer signal construction (TSC) [4]. In the first articles on the synthesis of TSC, the task was to increase the information transfer rate in binary channels. Further research of the possibilities of timer coding showed [5] that, based on TSC, it is possible to create various algorithms to increase the structural secrecy of signal constructions.

In [6], with the aim to increase the structural and energy secrecy of transmission, algorithms for the formation of noise-like timer signals based on direct spreading of the spectrum by random

sequences and random tuning of the operating frequency are proposed. Obviously, increasing the security OFDM technology is no less important, so the relevance of this research is beyond doubt.

The aim of the article is to increase the security of the transmission channel on the basis of multiplexing of non-position timer signals.

The main advantages of OFDM technology include high spectral efficiency, resistance to radio frequency interference and low level of multipath distortions [1, 2]. It is achieved by multiplexing the broadband signals with orthogonal multiplexing and simultaneously transmitting at different subcarrier frequencies. It should be noted, this method of multiplexing is developed for position signals, which does not allow to fully apply it to the TSC. For this reason, a new approach to multiplexing non-position TSCs is required.

The basic concept of constructing TSC is to increase the number of combinations in the time interval $T_{TSC} = nt_0$, where n – is the number of Nyquist elements with duration t_0. The moments of pulse modulation in TSC, in contrast to positional codes, are not multiples of t_0, but are multiples of some basic time interval Δ (where $\Delta = t_0 / s$; $s = 1, 2, 3, ..., l$ are integers). According to the rule of forming TSC, the duration of their design impulses cannot be less than the Nyquist interval, i.e. $t_s = t_0 + k\Delta$ (where $k = 0, 1, 2, ..., s \cdot (n-2)$). A larger number of realizations N_R in the interval T_{TSC} compared to the digit digital code (RRC) is achieved by reducing the energy distance between the signal constructions, which is determined by the quantity $\Delta < t_0$. The value of the interval Δ affects the noise immunity and the relative transmission rate, which have to be taken into account when selecting the parameters for building the TSC. The total number of realizations` signal constructions for timer coding is determined:

$$N_R = \sum_{i=1}^{n} \frac{[(n \cdot s) - [(s-1) \cdot i]]!}{i! \cdot [[(n \cdot s) - [(s-1) \cdot i]] - i]!}, \quad (1)$$

where i is the number of information modulation moments. The example of the constructing of three TSC on interval $T_{TSC} = 4t_0$, $t_s = 4\Delta$ is shown in Fig. 1,*a*.

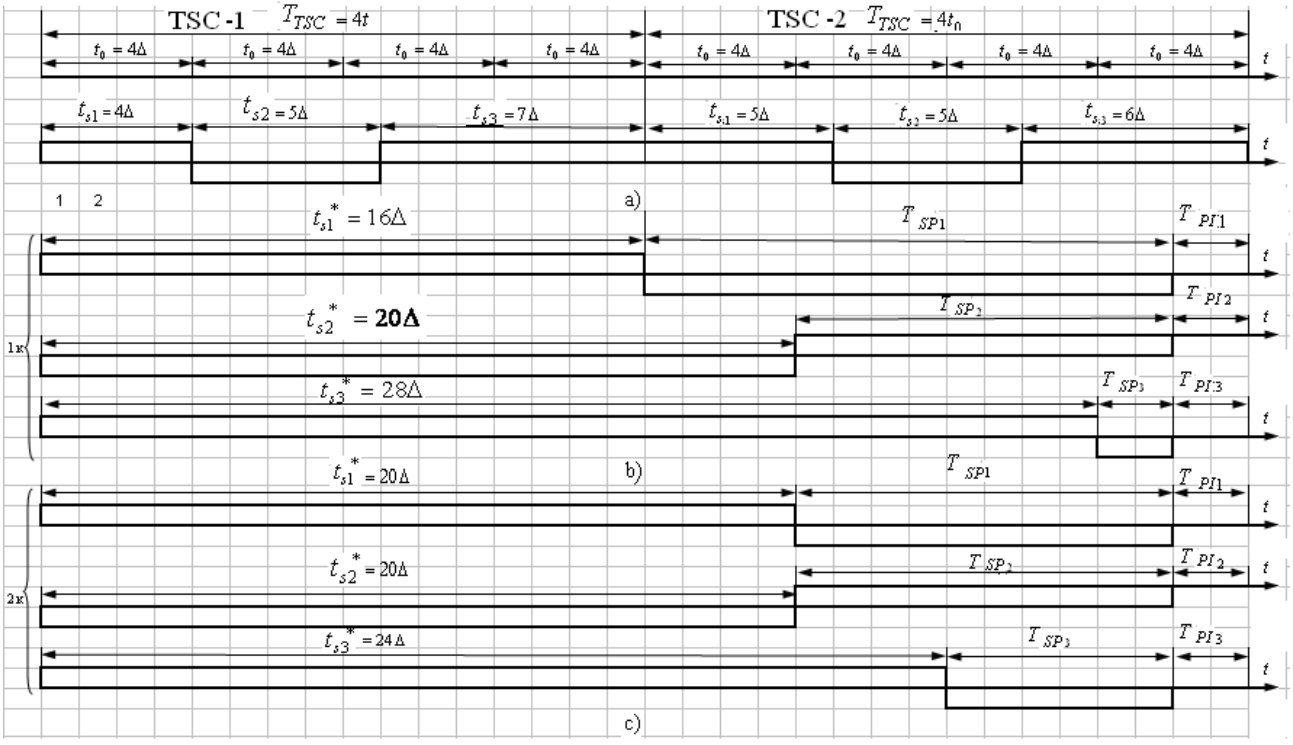

Figure 1 – The example of the constructing and multiplexing of TSC x_{TSC}

Features of the constructing a TSC do not allow multiplexing of non-position pulses in the same way as it is realized in OFDM technology. In a communication system with positional coding, the sequence of elements is converted into parallel bitstreams over a time interval , i.e. the transmission rate in each channel will decrease by times.

The formed bit sequence is modulated by phase or amplitude-phase modulation (APM), and each stream is transmitted by its individual subcarrier to the orthogonal frequency. The total bit rate will remain unchanged. In order to prevent the violation of orthogonality due to the possible appearance at the receiver input of the multipath effect, it is envisaged to introduce protective time interval , the magnitude of which has to be no less than the signal delay in any beam. It follows that the value of the elementary premise will decrease to a value , and the interval .

Taking into account that the basic element of the TSC constructing is Δ, and not the Nyquist interval t_0 , choosing the number of parallel streams is expedient taking into account the number of pulses t_s on the chosen multiplex time interval.

In Fig. 1,*a* shows the process of multiplexing pulses t_{ci} on the interval $T_M = zT_{TSC}$ (where $z = 2$ is the number of multiplexed TSC with parameters: $n = 4$; $s = 4$; $i = 2$) with the increase in their duration by $L = 2z$ times. With the given parameters TSC on the interval $T_M = 2t_0 n$, there will be only six multiplexing streams formed, which is less than for RRC. Each elongated pulse of TSC t_s contains the stop pulse of variable length T_{SPi}, the help of which provides the same multiplexing interval for all streams. Depending on the polarity pulse of the TSC, the voltage of the stop element can be either positive or negative.

In Fig. 1, *b*, *c* shows the process of elongation of the pulses of the timer signals t_{s1}, t_{s2}, t_{s3} at $L = 4$ times when they are multiplexed on time interval $T_M = 2T_{TSC}$. Because of the non-equidistant pulses $t_{s1}^* = 16\Delta$, $t_{s2}^* = 20\Delta$, $t_{s3}^* = 28\Delta$, the receiving stop intervals will have different durations. For the pulses TSC-1 in Fig. 1,*b*: $T_{SP1} = 14\Delta$; $T_{SP2} = 10\Delta$; $T_{SP3} = 2\Delta$. For pulses of TSC-2 (Fig. 1,*c*: $T_{SP1} = 10\Delta$; $T_{SP2} = 10\Delta$; $T_{SP3} = 6\Delta$. As can be seen from Fig. 1, *b*, *c* the guard interval $T_{pi} = 2\Delta$ for all multiplexing channels will be the same.

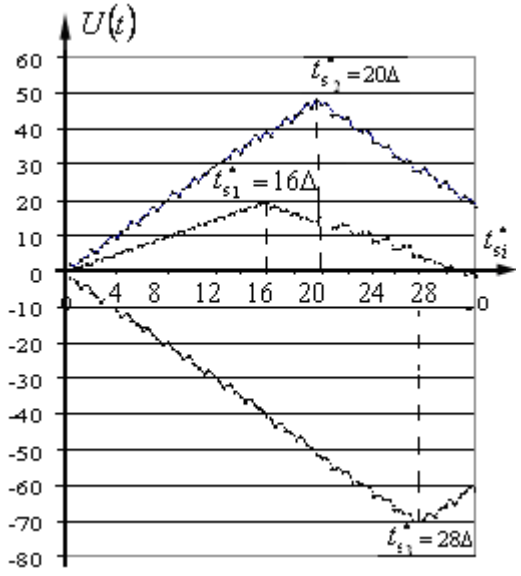

Figure 2 – Allocation pulses of TSC-1 t_{si} by means of correlation receivers

Obviously, increasing the number of multiplexed channels rises the noise immunity of the transmission. For $z = 2$ and $s = 4$ the multiplexing pulses of TSC, it allows the reduction of the number of orthogonal frequency subcarriers in comparison with the OFDM technology in which RRC is used. Clearly, the more complex structure of the timer signals compared to the TSC, and the completely different algorithm of their multiplexing, which depends on the parameters n, s and i increases the structural secrecy of signal construction, which complicates unauthorized access to confidential information. The fragment of the demultiplexing of the channels is shown in Fig. 2.

For TSC-1, the example is given of allocation fronts of pulses using correlation receivers, the number of which depends on the number of multiplexed channels. In this case, the reference frequency is applied to each correlation receiver, which corresponds to the multiplexing channel on the transmitting side.

Conclusion. The method of increasing the security of transmission channel based on multiplexing and demultiplexing of TSC was proposed. In contradistinction to OFDM technology, the developed multiplexing and demultiplexing algorithm is applicable for non-position signals. The extension of the pulses of the TSC due to their multiplexing is allowed to increase the noise immunity of the transmission. Each multiplexed channel contains a stop pulse for equalizing the time intervals of the multiplexing of each channel. The fronts are separated by means of correlation receivers. To prevent violation of orthogonality due to the possible appearance of the multipath effect at the receiver input, the protective time interval is provided. The method of multiplexing timer signals with their subsequent orthogonalization and modulation allows the increase in the structural secrecy of signal constructions, the increase the amount of transmitted data in comparison with the RRC, and the reduction in the number of used subcarriers of frequencies.

REFERENCES:

1. Tihvinskij V.O. Seti mobil'noj svjazi LTE. Tehnologii i arhitektura / V.O. Tihvinskij. – M.: Jeko-Trendz, 2010. – 128 s.
2. Shahnovich I.V. Sovremennye tehnologii besprovodnoj svjazi / I.V. Shahnovich. – M.: Tehnosfera, 2004. – 187 s.
3. Zaharchenko M. V. Sistemi peredavannja danih. Tom 1. Zavadostijke koduvannja / Zaharchenko M. V. – Odesa: Feniks, 2009. – 447 s.
4. Zaharchenko N. V. Ocenka informacionnoj skrytnosti tajmernyh signal'nyh konstrukcij v sistemah peredachi konfidencial'noj informacii/ N. V. Zaharchenko, V. V. Korchinskij, B. K. Radzimovskij // Zbirnik naukovih prac' ONAZ im.O.S.Popova. – 2011. – № 1. – S. 3–8.
5. Zakharchenko N. Information security of Time-Controlled Signals in Confidential Communication Systems / N. Zakharchenko, V. Korchinsky, B. Radzimovsky // Modern problems of radio engineering, telecommunications and computer science: XI International Conference TCSET 2012, (Lviv-Slavske, 21-24 february 2012). – Lviv: Publishing House of Lviv Polyteshnic, 2012. – S. 317.
6. Korchinskij V.V. Povyshenie skrytnosti peredachi na osnove psevdosluchajnoj perestrojki rabochej chastoty i tajmernyh signalov / V.V. Korchinskij // Vestnik NTU «HPI». – Har'kov: HPI, 2012. – № 66 (972). – S.63-67.

ЛИТЕРАТУРА:

1. Тихвинский В.О. Сети мобильной связи LTE. Технологии и архитектура / Тихвинский В.О. – М.: Эко-Трендз, 2010. – 128 с.
2. Шахнович И.В. Современные технологии беспроводной связи / Шахнович И.В. – М.: Техносфера, 2004. – 187 с.
3. Захарченко М. В. Системи передавання даних. Том 1. Завадостійке кодування / Захарченко М. В. – Одеса: Фенікс, 2009. – 447 с.
4. Захарченко Н. В. Оценка информационной скрытности таймерных сигнальных конструкций в системах передачи конфиденциальной информации/ Н. В. Захарченко, В. В. Корчинский, Б. К. Радзимовский // Збірник наукових праць ОНАЗ ім.О.С.Попова. – 2011. – № 1. – С. 3–8.
5. Zakharchenko N. Information security of Time-Controlled Signals in Confidential Communication Systems / N. Zakharchenko, V. Korchinsky, B. Radzimovsky // Modern problems of radio engineering, telecommunications and computer science: XI International Conference TCSET 2012. (Lviv: Slavske, 21-24 february 2012). – Lviv: Publishing House of Lviv Polyteshnic, 2012. – C. 317.
6. Корчинский В.В. Повышение скрытности передачи на основе псевдослучайной перестройки рабочей частоты и таймерных сигналов / В.В. Корчинский // Вестник НТУ «ХПИ». – Харьков: ХПИ, 2012.– № 66 (972). – С. 63-67.