Methods of information systems synthesis

UDC 621.395.721.5 **doi: 10.20998/2522-9052.2020.3.07**

Oleksandr Pliushch, Viktor Vyshnivskyi, Yuliia Berezovska

State University of Telecommunications, Kyiv, Ukraine

ROBUST TELECOMMUNICATION CHANNEL WITH PARAMETERS CHANGING ON A FRAME-BY-FRAME BASIS

Abstract. An approach is proposed to design of a robust data transfer channel for telecommunication networks that is based on the desired bits spectrum spreading and their additional scrambling by using two pseudo noise coding sequences derived from primitive polynomials of eighth and fifteenth degrees. Further information protection is offered to be achieved by deploying four 32768 chip-long pseudo noise coding sequences, instead of one, with 128 cyclic shifts each. It is proven that selection of a scrambling sequence and its cyclic shift according to a secret algorithm on a frame-by-frame basis helps substantially improve performance of the telecommunication channel in terms of protection against interception while preserving its useful properties. Research results permit to claim that the designed telecommunication channel could be used in noise immune and concealed telecommunication networks.

Keywords: telecommunication network; primitive polynomial; pseudo noise coding sequences; computer simulation; spectrum spreading; cyclic sequence shift.

Introduction

Problem statement. Telecommunication networks have always been a prime target for those rogue elements who want to prevent information transfer, intercept messages or even take control over the channel by sending spurious information instead of the legitimate one. The latter is especially widespread when it comes to control over unmanned aerial vehicles or drones. In general, it is widely accepted that susceptibility of the wireless networks is much higher than that of any other. That is why enhancing noise immunity, concealment properties as well as improving resistance to deciphering of the telecommunication channels sending data over air interface play a major role in their practical implementations.

Deployment of the wideband signals is one of the most effective ways of improving the features of telecommunication channel mentioned above. Formation of the wideband signals in telecommunications is often achieved with the help of different spreading techniques, which are usually performed by using spreading coding sequences.

According to this approach, every bit of information in telecommunication channel is processed by the spreading coding sequence, which consists of a certain number of chips. The bigger the number of chips, the better noise immunity, transmission concealment and resistance to deciphering the channel possess. Besides, it is a common practice to transmit data in telecommunication channels frame-by-frame, which creates a precondition to use a second coding sequence that not only marks the limits of the frame, but also performs additional scrambling of the data. This additional scrambling gives an extra layer of protection to the data being transmitted.

Auto- and inter- correlation parameters of the spreading coding sequences are a key to their practical utilization. It is well-known that very good correlation properties can be found in pseudo noise coding sequences that are derived from the primitive polynomials of the certain degree. These coding sequences have proved their effectiveness in the third generation mobile networks [1], [2]. But in those networks the pseudo noise coding sequences are used only to organize multiple access to the system for many subscribers both within one cell and between cells. At the same time, utilization of the pseudo noise coding sequences to enhance noise immunity, concealment properties and improving resistance to deciphering have received insufficient attention in research.

Additionally, deployment of the two, even with the best properties, pseudo noise coding sequences with account of the current level of cyber rogue element's equipment is not near enough. That is why, this paper proposes to change the parameters of the pseudo noise spreading sequences on a frame-by-frame basis, namely using four (or even more) spreading sequences instead of the one marking the frame size, with each of them undergoing many cyclic shifts.

Thus, study of the practical realization of the noise immune, concealed, resistant to deciphering telecommunication channels with utilization of the pseudo noise coding sequences derived from primitive polynomials with different cyclic shifts and frame-by frame-parameters hopping is important and some extra research is needed in this direction.

Recent literature review. Utilization of pseudo noise coding sequences in third generation mobile networks is reasonably well-treated in [1] and [2]. In [1], an area of application of these coding sequences is outlined, as well as certain their examples are provided, although it is done with particular stress on multiple access to the network. In addition, correlation properties are considered in respect to subscriber separation while noise immunity and transmission concealment are not entertained. In [2], it is paid a big attention to the practical component of pseudo noise coding sequences deployment and, besides, it presents a lot of explanations concerning theory and practice of how to generate these sequences, including those with different cyclic shifts

using primitive polynomials. That is being said, this work focuses totally on the pseudo noise coding sequences that are used in CDMA2000 technology, while others are treated superficially.

The authors in [3] try to present full and, yet, detailed account of the spectrum spreading coding sequences that, according to their parameters, can be used in telecommunication networks. Unfortunately, study of performance of certain spreading sequences in a practical implementation of the telecommunication channel is not done properly. Although this source outlines ways of forming pseudo noise coding sequences and the advantages that they bring, it serves as more of a theoretical effort and does not support the information with, for example, computer simulation.

An approach to practical use of pseudo noise coding sequences for design of control channels for unmanned aerial vehicles is studied in [4]. But it lacks an analysis of the channel's noise immunity while the cyclic shifts option is not addressed, which could enhance both this parameter and the transmission concealment in the telecommunication control channel.

There are good reviews of the technologies that are used in wireless telecommunication networks in [5] and [6]. Nevertheless, these sources claim that pseudo noise coding sequences are only one of the technologies amongst many and, as a result, practical verification of the coding sequences parameters is not done. With account of the deficiencies in the reviewed known literature, the purpose of this article is to study practical implementation of the noise immune telecommunication channels based on pseudo noise coding sequences as used on frame-by-frame basis with different cyclic shifts.

Main material

Design of the code and chip structure of the telecommunication channel. As mentioned above, information transmission in a telecommunication channel is performed by frames. Frame size is determined by the channel type, the area of its use and required data rates. In wideband applications, each transmitted bit is spectrally spread by the short pseudo noise coding sequence. In this case, spreading factor is determined on the one hand by required date rate, on the other – available frequency band.

Let us assume that required data rate in the telecommunication channel is 20 Kbit/sec, while available frequency band is 5 MHz. Thus, a possible spreading factor equals 256 units and, in this way, short pseudo noise coding sequence, which spreads bits, must comprise 256 chips.

According to the recent developments in the field, network developers are trying to use shorter frames because it simplifies retransmission techniques, deployed when there are too many errors. Let us assume that the frame is composed of 128 bits, and, then, it includes 32768 chips, as does the long pseudo noise coding sequence determining frame size.

For the reasons given above, chip and frame structure, as well as algorithm of the telecommunication channel design, look as follows:

- Each frame with duration of 32768 chips contains 128 bits of data, every one of them comprising 256 chips;
- First pseudo noise coding sequence is formed that includes 256 chips and matches the duration of one bit;
- Second pseudo noise coding sequence is formed that includes 32768 chips and determines frame duration;
- All bits except for the first one are spread by short coding sequence with 256 chips;
- First bit always assumes value unity and is not spread by the short pseudo noise coding sequence with 256 chips, but is, rather, used for frame synchronization;
- All frame's bits are processed by the long coding sequences with duration 32768 chips;
- Frame synchronization is performed using first 256 chips of the long coding sequence with 32768 chips.

Let us not forget that we need at least four long pseudo noise coding sequences and they are used with different cyclic shifts. Hence, it is important to study how to generate them and check their auto- and inter correlation properties.

Synthesis of the long pseudo noise coding sequences and assessment of their properties. Good performance of the telecommunication channel can be secured only using coding sequences with required correlation properties. To obtain good auto- and inter correlation properties, it is highly recommended to utilize primitive polynomials of a certain degree.

Primitive polynomials of the required degree can be found in [2], as well as in many other places. We are interested in the primitive polynomials of the fifteenth degree. According to [2], there are 1800 of them available, but for the purpose of this article we need just four. These polynomial $F(x) = 1 + x^2 + x^6 + x^7 + x^8 + x^{10} + x^{15}$ is can be also deduced by polynomial division. Four primitive polynomials of the fifteenth degree that can be used to generate pseudo noise coding sequences comprising 32768 chips and selected by the authors are as follows:

$$\begin{aligned} F(x) &= 1 + x^5 + x^7 + x^8 + x^9 + x^{13} + x^{15}; \\ F(x) &= 1 + x^2 + x^6 + x^7 + x^8 + x^{10} + x^{15}; \\ F(x) &= 1 + x^3 + x^4 + x^5 + x^9 + x^{10} + x^{11} + x^{12} + x^{15}; \\ F(x) &= 1 + x + x^2 + x^6 + x^7 + x^{11} + x^{15}. \end{aligned} \quad (1)$$

Pseudo noise coding sequence derived from (1) can be synthesized using 15 element shift register presented in Fig. 1.

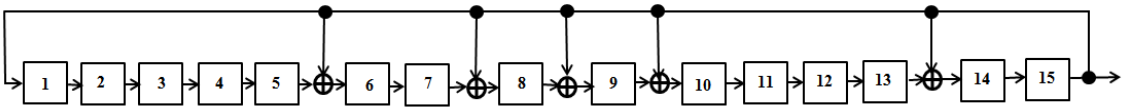

Fig. 1. Block diagram of pseudo noise coding sequence generator with 32768 chips from the primitive polynomial

In this picture, at the output of the fifth, seventh, eighth, ninth and thirteenth elements, the modulo 2 addition is performed. In principle, the diagram in Fig.1 is able to generate only 32767 chips because 15 zeros cannot exist in it. Therefore, one additional "0" is inserted to the run of 14 zeros without shifting the data along the register [2]. If initial loading vector is all zeros but last, then the fourteen zeros are the last ones in the sequence and the additional zero is added as number 32768. Similar diagrams can be drawn for other polynomials; they differ only in the way where the modulo 2 addition is performed. The similarity is important because we can easily switch from one sequence to another, out of three left, using just one device with almost no equipment cost.

As mentioned above, each sequence of 32768 chips undergoes cyclic shifts with the step equaling any number of chips in the expression n*256, where n assumes integer values from 1 to 127.

To quickly perform the shifts, one can use 15 bit masks and those 15 bit long words should equal 127, which corresponds to the number of cyclic shifts. To perform this task, block diagram in Fig. 1 can be modified as is shown in Fig. 2.

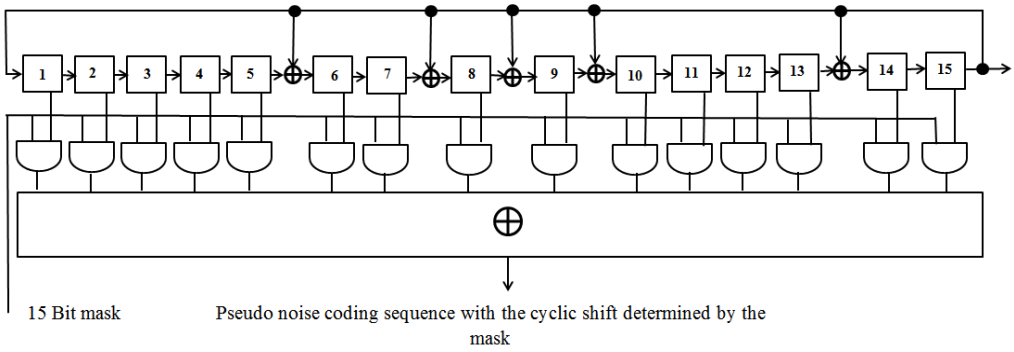

Fig. 2. Block diagram of pseudo noise coding sequence generator with 32768 chips and cyclic shifts determined by the mask

In Fig. 2, each of the fifteen bits of the certain cyclic shift mask is processed by logical "&" with the binary signal of the corresponding element of the shift register. After that, output sequence with the shift, corresponding to the mask, is formed by modulo 2 addition of all the signals from logical elements performing logical "&".

Thus, the block diagram in Fig. 2 can easily switch from generating one sequence to another of the four pseudo noise coding sequences with 127 possible cyclic shifts each, on a frame-by-frame basis. This hopping can be performed according to a secret algorithm, while there are 512 possible options available to choose from.

Before proceeding to studying performance of the designed channel, it is important to assess the correlation properties of the pseudo noise coding sequences presented above.

Fig.3 illustrates autocorrelation properties of the first out of the four pseudo noise coding sequences comprising 32767 chips, which is without adding an extra chip and is generated according to (1). Autocorrelation functions for the second, third and fourth sequences are the same, as the one in Fig. 3.

It is evident from the figures that the polynomials used to derive the sequences are truly primitive, because once a single shift occurs, the correlation function assumes -1 value and it stays this way for the whole duration of the sequence. When there is no shift, the correlation function value is that of the number of chips in the sequences – 32767 (the figure does not reflect this because it is focused on verifying the -1 value).

It is interesting to see what happens to the autocorrelation functions when an extra chip is added to obtain the sequences with 32768 chips. The autocorrelation function for the pseudo noise coding sequence with an extra chip is presented in Fig.4.

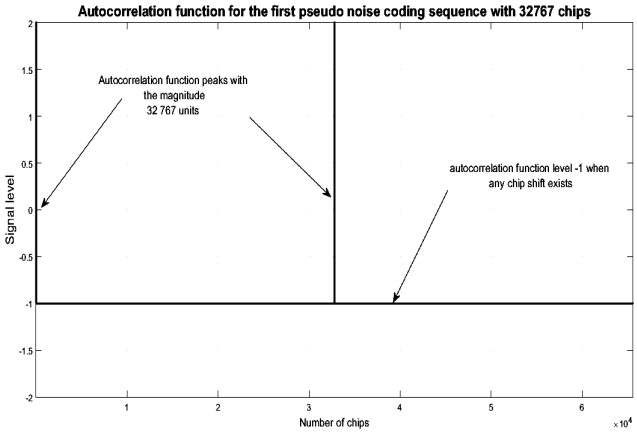

Fig. 3. Autocorrelation function for the first pseudo noise coding sequence with 32767 chips

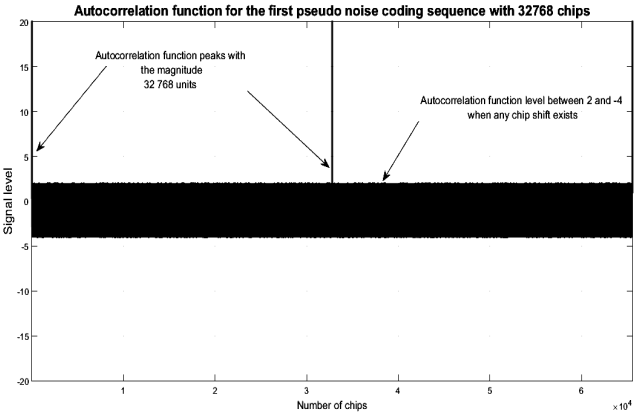

Fig. 4. Autocorrelation function for the first pseudo noise coding sequence with 32768 chips

As evidenced by the data in Fig. 4, an extra chip degrades the autocorrelation properties, but still they

remain very good. Autocorrelation functions for the second, third and fourth sequences with 32768 chips are the same, at least when it comes to signal levels, as that in Fig. 4. To assess the behavior of the correlation function in Fig. 4, 5 presents the same graph but on is bigger scale, just 1000 first chips. It is clear from this figure that, although the upper and low bounds stay the same, the function assumes three different values determined by the coding sequence structure.

Data in Fig. 3 and 4 illustrate correlation functions when the integration is carried out on the whole length of the sequence. In real installations, the integration is performed on a limited plot, and it obviously degrades the performance.

In the synthesized telecommunication channel, the sequence segment allocated for the integration is the first 256 chip section of any of the four 32768 chip long sequences with appropriate cyclic shift.

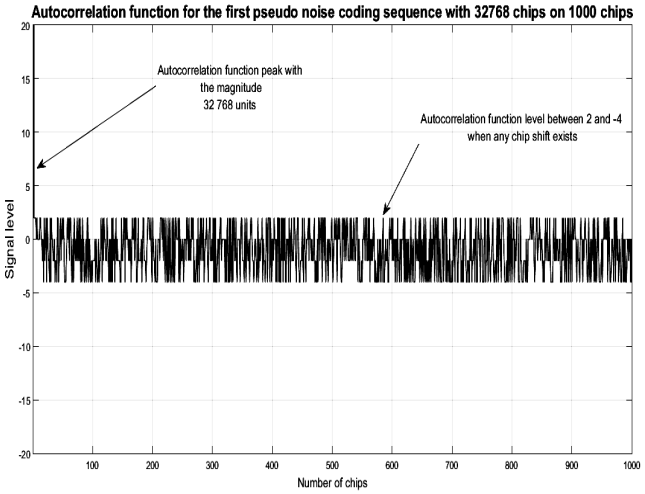

Fig. 5. Autocorrelation function for the first pseudo noise coding sequence with 32768 chips on the first 1000 chips

To study the correlational properties in this case of the limited integration segment, Fig. 6-10 show correlation function of the selected frame synchronization segment, or window function, and the four pseudo noise sequences of 32768 chip long.

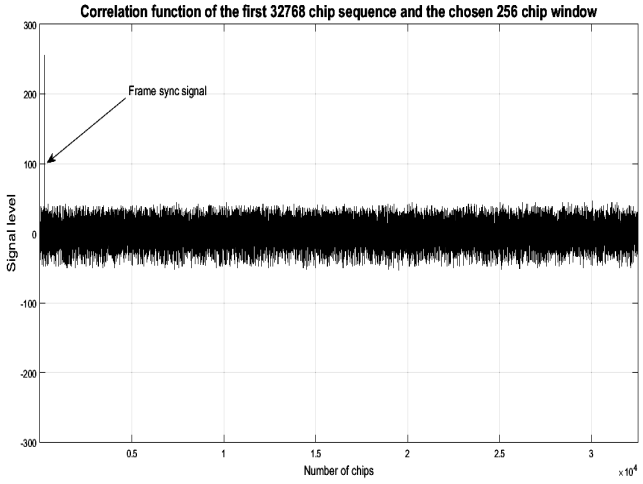

Fig. 6. Correlation function for the first pseudo noise coding sequence with 32768 chips and the chosen window function

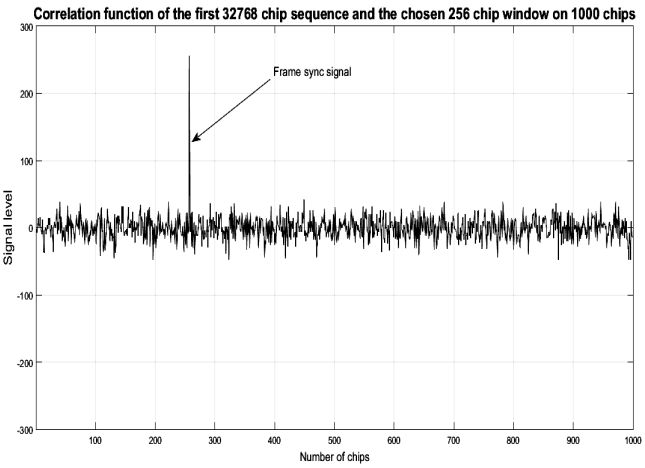

Fig. 7. Correlation function for the first pseudo noise coding sequence with 32768 chips and the chosen window function on the first 1000 chips

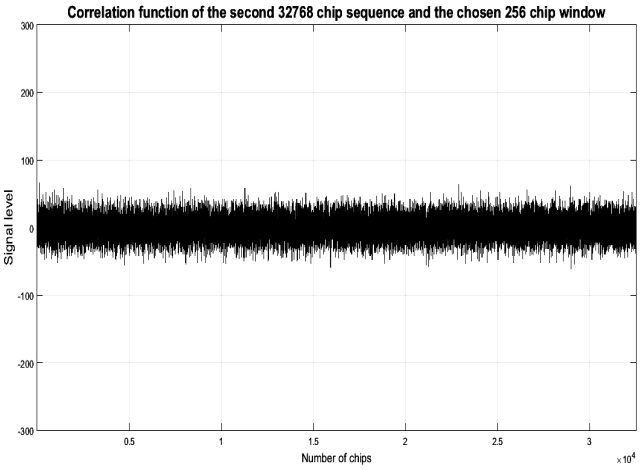

Fig. 8. Correlation function for the second pseudo noise coding sequence with 32768 chips and the chosen window function

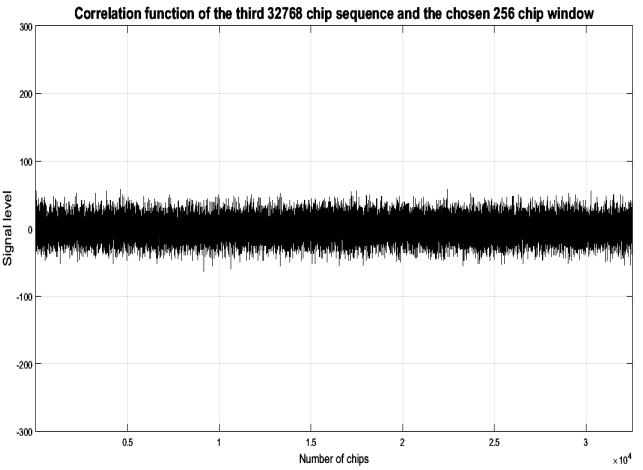

Fig. 9. Correlation function for the third pseudo noise coding sequence with 32768 chips and the chosen window function

Synthesis of the short pseudo noise coding sequence. As mentioned above, the telecommunication channel uses short pseudo noise coding sequence to spread bits of the useful information. Similarly to synthesis of the long pseudo noise coding sequences, a

primitive polynomial is required to obtain 256 chip long short pseudo noise coding sequence, but in this case that of the eighth degree. The one, chosen in this paper, can be presented as follows:

$$F(x) = 1 + x^2 + x^3 + x^4 + x^8. \quad (2)$$

As in the case with the primitive polynomial (1), (2) can be used to generate a pseudo noise coding sequence with the help of the shift register and addition of the 256th chip to 255 already formed.

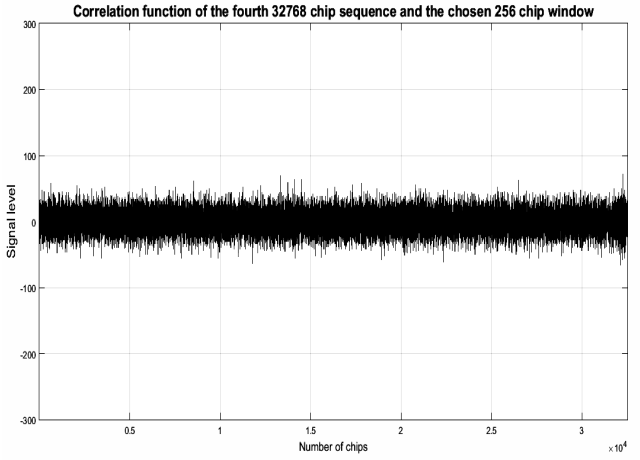

Fig. 10. Correlation function for the fourth pseudo noise coding sequence with 32768 chips and the chosen window function

Fig. 11 illustrates pseudo noise coding sequence with 256 chips synthesized according to (2).

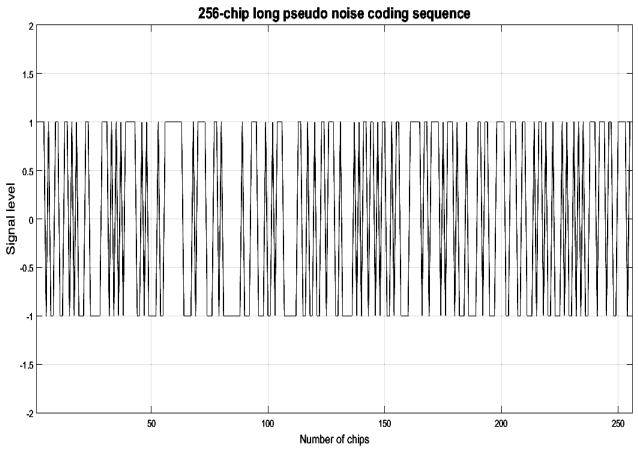

Fig. 11. 256-chip long pseudo noise coding sequence

Performance study of the designed telecommunication channel on the background of the internal noise and interfering signal. Having synthesized the pseudo noise coding sequences and studied their properties, let us proceed to assessing performance of the proposed telecommunication channel.

As was shown above, useful signal is presented as a binary modulation of a 128 bit sequence (bit frame), each of which is spectrally spread 256 times by the short pseudo noise coding sequence just described. In addition, each frame is scrambled by the 32768 chip long pseudo noise coding sequence, which marks the frame limits. Internal noise is presented as normally distributed samples with one unite power level. Interfering signal has the same probability distribution and power as does the internal noise. Additive mixture of useful signal, internal noise and interfering signal over one frame is shown in Fig. 12. Here, the first 32768 chip long pseudo noise coding sequence is used with the cyclic shift of 256 chips.

Further research is directed at establishing whether it is possible to extract from the mixture in Fig. 12 frame structure of the information and the values of all bits of information.

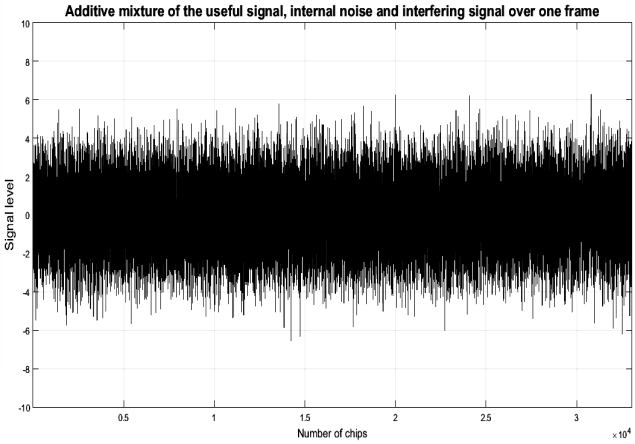

Fig. 12. Additive mixture of the useful signal, internal noise and interfering signal over one frame

Fig. 13 illustrates signal at the output of the matched filter for the selected frame signal when it processed the frame depicted in Fig. 12. Extracted frame sync pulse is clearly visible in Fig. 13 at the beginning of the frame.

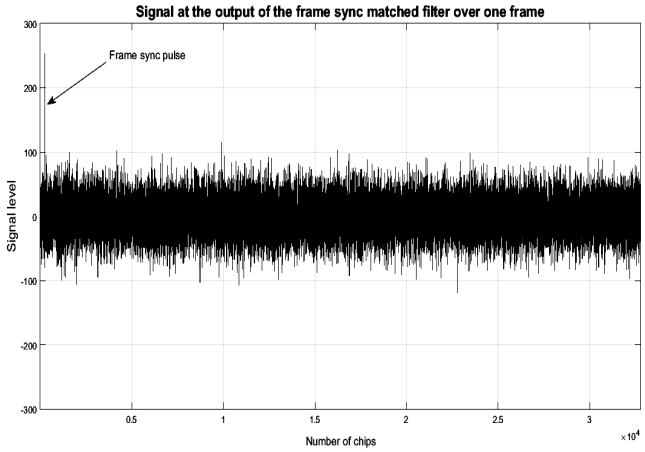

Fig. 13. Signal at the output of the frame sync matched filter over one frame

Fig. 14 shows the signal at the output of the spread bits matched filter over one frame after it processed signal mixture depicted in Fig. 12, preliminary descrambled by the long pseudo noise sequence.

Analysis of the data in Fig.14 indicates that the bits are confidently extracted from the mixture on the background of the internal noise and interfering signal.

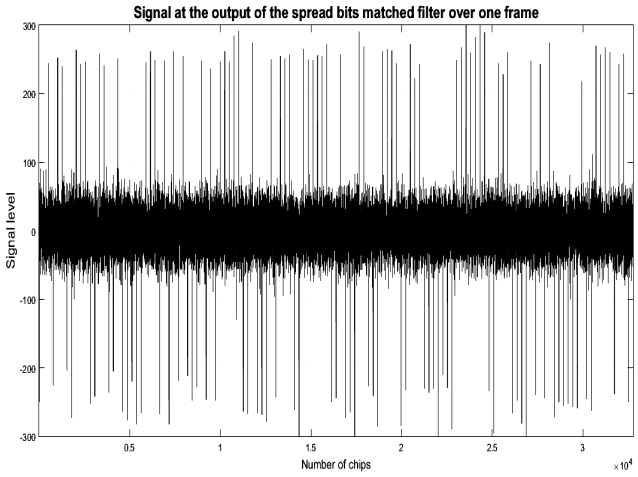

Fig. 14. Signal at the output of the spread bits matched filter over one frame

Performance study of the designed telecommunication channel with use of different long pseudo noise coding sequences and cyclic shifts. In some cases, deployment of the two pseudo noise coding sequences cannot secure complete protection of the information from the interception. This paper proposes to further enhance concealed information transfer by using not one but four 32768 chip long pseudo noise coding sequences, as well as their cyclic shifts. There are 128 cyclic shifts for each sequence and with account of 4 sequences one can number 512 possible options to choose from. In this case, any one of 512 options can be chosen according to preselected secrete algorithm, which frequently changes.

To test feasibility and effectiveness of the proposed method, the signal similar to that in Fig. 12 was formed, with only exception that the third 32 768 chip long pseudo noise coding sequence was deployed with the cyclic shift 1280 chips.

This signal is shown in Fig. 15.

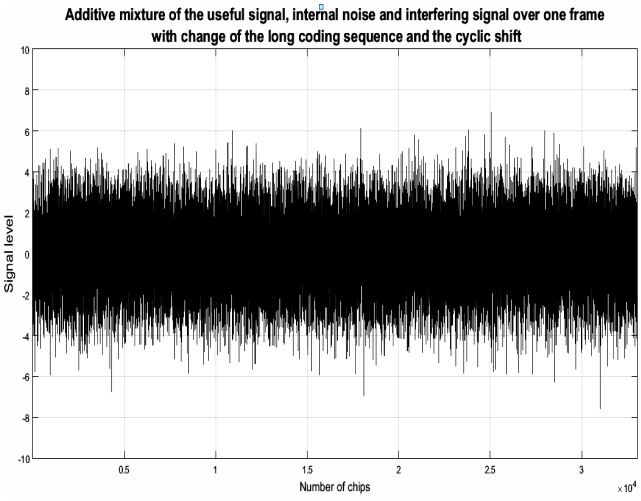

Fig. 15. Additive mixture of the useful signal, internal noise and interfering signal over one frame with change of the long coding sequence and the cyclic shift

Let us assume that the rogue elements somehow learnt about the structure of the short 256 chip long pseudo noise coding sequence and the long 37268 chip long pseudo noise coding sequence. But they are ignorant of the possible change of the long sequence and its cyclic shift. In this case, while trying to intercept the message they will use known to them data about the sequences. As a result, the rogue elements will obtain the frame sync pulse and the bit sequence portrayed in Fig. 16 and 17 respectively.

As it seems from these figures, they will not be able to decode the fame structure and extract the bits of useful information.

Fig. 18 and 19 present the signals at the output of matched frame sync filter and bits matched filter, respectively, with the full knowledge about the selection of the long pseudo noise coding sequence and the cyclic shift.

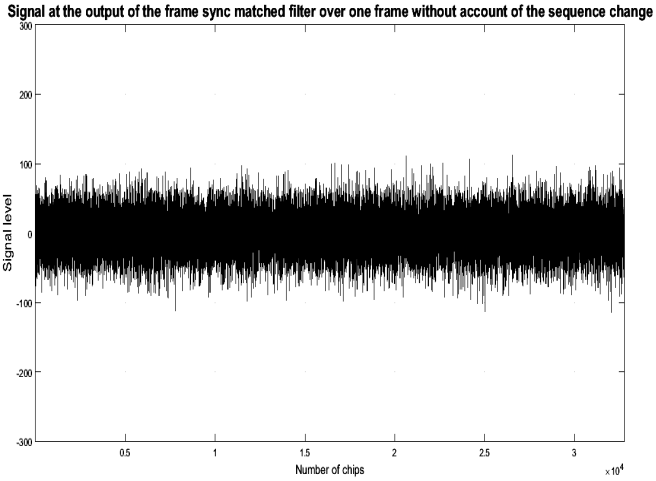

Fig. 16. Signal at the output of the frame sync matched filter over one frame without account of the sequence change and the cyclic shift

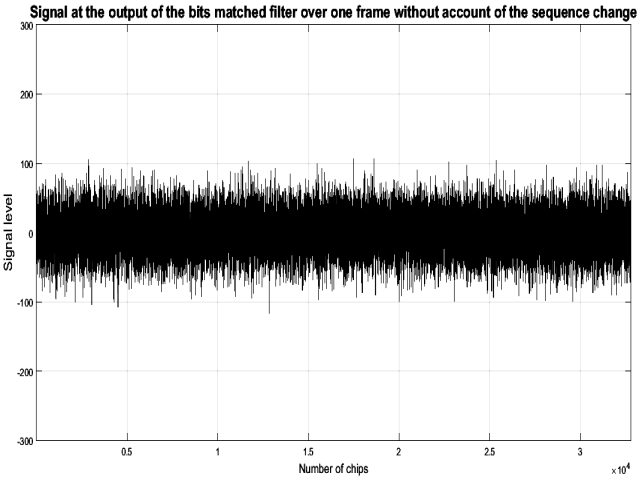

Fig. 17. Signal at the output of the bits matched filter over one frame without account of the sequence change and the cyclic shift

As data in Fig. 18 and 19 indicate, when the change of the long pseudo noise coding sequence, as well as the cyclic shift, are taken into account, respective processing in matched filters permits to effectively extract frame sync signal and bits of information.

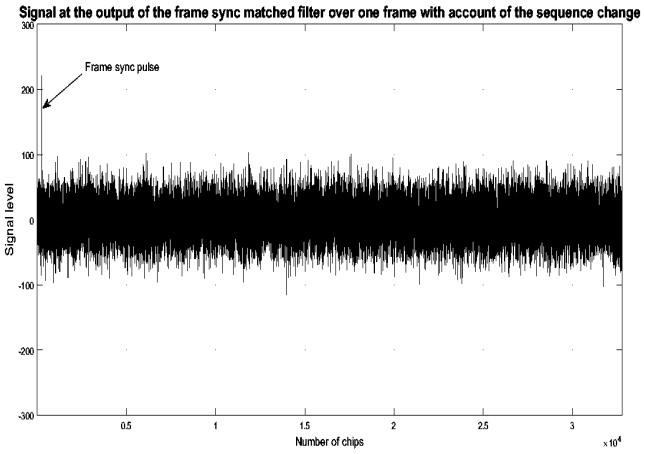

Fig. 18. Signal at the output of the frame sync matched filter over one frame with account of the sequence change and the cyclic shift

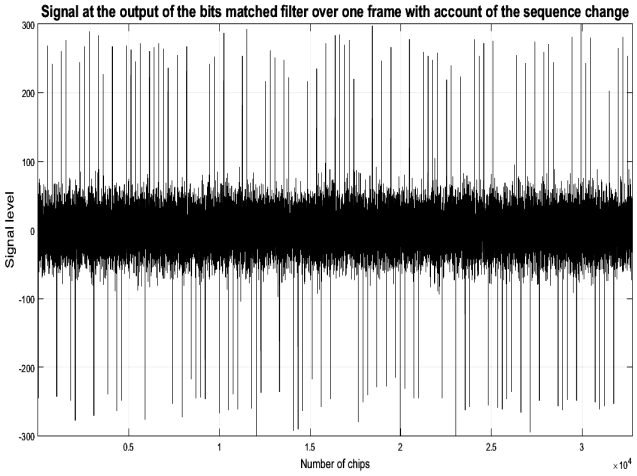

Fig. 19. Signal at the output of the bits matched filter over one frame with account of the sequence change and the cyclic shift

When shifts and sequences change almost randomly on a frame-by-frame basis, the adversary must follow all possible options, and there can be too many for him.

According to [2] there are 18000 primitive polynomials of the fifteenth degree and with account of the 128 possible shifts, it can become an insurmountable problem for the interceptors.

Conclusions

Data transfer telecommunication channels are among the important targets of the rogue cyber actors. There is a constant battle between those who protect information and those who try to intercept it. Thus, enhancing noise immunity of the information, its concealment and resistance to interception is a very important topic to research.

To improve these parameters, it is proposed to design a telecommunication channel with deployment of the two pseudo noise coding sequences: one is 265 chip long sequence for spectral spreading of the useful bits, while the other is 32768 chip long to mark the frame limits and provide additional scrambling of the information.

To further increase resistance to interception, use of four 32768 chip long sequences, instead of one, is considered with different cyclic shifts. It is proven that these pseudo noise coding sequences, derived from the primitive polynomials, possess good auto and inter correlational properties.

Performance study of the telecommunication channel was carried out with the help of computer simulation in Mathlab software package.

Computer simulation helped to establish that proposed telecommunication channel permits to extract useful bits of information from the additive mixture of the internal noise and an interfering signal. Additionally, it was revealed that using four different 32768 chip long pseudo noise sequences with cyclic shifts changing on a frame-by-frame basis, according to a secret algorithm, can substantially improve resistance to interception while preserving all other useful characteristics of the channel.

In this case, cyber criminals have a very difficult task to intercept the useful information bits.

References

1. Andreas, Springer and Robert, Weigel (2013), *UMTS: The Physical Layer of the Universal Mobile Telecommunications System*, Springer Science & Business Media, USA, 298 p.
2. Lee, Jhong S.and Miller, Leonard E. (1998), *CDMA systems engineering handbook*, Artech House, Boston, London, 1228 p.
3. Byeong, G. Lee and Seok, C. Kim (2012), *Scrambling Techniques for Digital Transmission*, Springer Science & Business Media, USA, 448 p.
4. Kamesh, Namuduri, Serge, Chaumette, Jae, H. Kim, James P.G., Sterbenz (2017), *UAV Networks and Communications*, Cambridge University Press, UK, 242 p.
5. Evgenii, Krouk and Sergei, Semenov (2011), *Modulation and Coding Techniques in Wireless Communications*, John Wiley & Sons, USA, 680 p.
6. Clint, Smith and Daniel, Collins (2013), Wireless Networks, McGraw Hill Professional, USA, 752 p.

Надійшла (received) 27.05.2020
Прийнята до друку (accepted for publication) 26.08.2020

Відомості про авторів / About the authors

Плющ Олександр Григорович – кандидат технічних наук, професор кафедри мобільних та відеоінформаційних технологій, Державний університет телекомунікацій, Київ, Україна;
Oleksandr Pliushch – PhD, Professor Department of Mobile and Videoinformation Technologies, State University of Telecommunications, Kyiv, Ukraine;
e-mail: opliusch@yahoo.com; ORCID ID: https://orcid.org/0000-0001-5310-0660

Вишнівський Віктор Вікторович – доктор технічних наук, завідувач кафедри комп'ютерних наук, Державний університет телекомунікацій, Київ, Україна;
Viktor Vyshnivskyi – Doctor of Technical Sciences, Head of Department of Computer science, State University of Telecommunications, Kyiv, Ukraine;
e-mail: vish_vv@ukr.net; ORCID ID: https://orcid.org/0000-0003-1923-4344

Березовська Юлія Володимирівна – аспірант, Державний університет телекомунікацій, Київ, Україна;
Yuliia Volodymyrivna – Postgraduate Student, State University of Telecommunications, Kyiv, Ukraine;
e-mail: krasabereza@gmail.com; ORCID ID: https://orcid.org/0000-0002-9973-0497

Стійкий телекомунікаційний канал зі зміною параметрів від кадру до кадру

О. Г. Плющ, В. В. Вишнівський, Ю. В. Березовська

Анотація. Зроблено висновок, що сучасні телекомунікаційні канали не є в достатній мірі захищеними від завад та перехоплення зловмисниками. Запропоновано підвищити ці показники в розробленому телекомунікаційному каналі за рахунок використання двох типів псевдовипадкових кодових послідовностей: короткої тривалістю 256 чипів, що використовується для розширення спектру бітів корисної інформації, та протяжної тривалістю 32768 чипів, що позначає розміри кадру та здійснює додаткове скремблювання інформації. Наголошується, що для задоволення вимог щодо протидії перехопленню інформації зловмисниками необхідно використовувати не одну, а чотири псевдовипадкових кодових послідовностей тривалістю 32768 чипів з різними циклічними зсувами кратними 256 чипів. З урахуванням того, що таких зсувів налічується 128 на кожну з чотирьох послідовностей і пара послідовність-зсув змінюється від кадру до кадру, зроблено висновок, що це значним чином збільшує захист інформації в каналі від перехоплення. Досліджено взаємно та авто кореляційні властивості псевдовипадкових кодових послідовностей, які виявилися дуже гарними для тих послідовностей, що отримуються з примітивних поліномів певного порядку. За допомогою програмного середовища MathLab проведене імітаційне комп'ютерне моделювання запропонованого телекомунікаційного каналу на основі запропонованих кодових послідовностей, в процесі якого доведено, що незнання певної послідовності тривалістю 32768 чипів та відповідного циклічного зсуву призводить до унеможливлення перехоплення інформації зловмисниками. Наголошується, що запропоновані псевдовипадкові кодові послідовності можуть бути легко практично реалізовані в зсувних регістрах восьмого та п'ятнадцятого порядку, при цьому перехід від одного циклічного зсуву до іншого може легко робитися за рахунок відповідних масок, в той час як перехід від послідовності до послідовності реалізується за рахунок активації або деактивації елементів додавання по модулю 2 на виходах відповідних елементів зсувних регістрів. Отримані в роботі результати досліджень дозволяють припустити, що запропонований телекомунікаційний канал з використанням чотирьох різних псевдовипадкових послідовностей з різними циклічними зсувами за певним прихованим законом від кадру до кадру може успішно застосовуватися при реалізації завадозахищених, скритних телекомунікаційних мереж.

Ключові слова: телекомунікаційна мережа; примітивний поліном; псевдовипадкові кодові послідовності; комп'ютерне моделювання; розширення спектру; циклічний зсув послідовності.

Робастный телекоммуникационный канал со сменой параметров от кадра к кадру

А. Г. Плющ, В. В. Вишневский, Ю. В. Березовская

Аннотация. Сделан вывод, что современные телекоммуникационные каналы не в должной мере защищены от помех и перехвата злоумышленниками. Предложено повысить эти показатели в разработанном телекоммуникационном канале за счет использования двух типов псевдослучайных кодовых последовательностей: короткой длительностью 256 чипов, которая используется для расширения спектра бит полезной информации, и протяженной длительностью 32768 чипов, которая помечает размеры кадра и осуществляет дополнительное скремблирование информации. Подчеркивается, что для удовлетворения требований по противодействию перехвату информации злоумышленниками необходимо использовать не одну, а четыре псевдослучайные кодовые последовательности длительностью 32768 чипов с разными цикличными сдвигами кратными 256 чипам. С учетом того, что таких сдвигов насчитывается 128 на каждую из четырех последовательностей и пара последовательность-сдвиг изменяется от кадра до кадра, сделан вывод, что это существенным образом повышает защиту информации от перехвата. Исследованы взаимно и авто корреляционные свойства псевдослучайных кодовых последовательностей, которые оказались очень хорошими для тех последовательностей, которые получаются из примитивных полиномов соответствующего порядка. С помощью программной среды MathLab проведено имитационное компьютерное моделирование предложенного телекоммуникационного канала на основе предложенных кодовых последовательностей, в процессе которого доказано, что незнание определенной последовательности длительностью 32768 чипов и соответствующего циклического сдвига приводит к невозможности перехвата информации злоумышленниками. Подчеркивается, что предложенные псевдослучайные кодовые последовательности могут быть практически реализованы в сдвиговых регистрах восьмого и пятнадцатого порядка, при этом переход от одного циклического сдвига к другому может быть легко осуществлен за счет соответствующих масок, в то время как переход от последовательности к последовательности реализуется за счет активации или деактивации элементов суммирования по модулю 2 на выходах соответствующих элементов сдвиговых регистров. Полученные в работе результаты исследований позволяют предположить, что предложенный телекоммуникационный канал з использованием четырех разных псевдослучайных последовательностей с разными циклическими сдвигами по определенному скрытому закону от кадра к кадру может успешно использоваться при реализации помехоустойчивых, скрытных телекоммуникационных сетей.

Ключевые слова: телекоммуникационная сеть; примитивный полином; псевдослучайные кодовые последовательности; компьютерное моделирование; расширение спектра; циклический сдвиг последовательности.