ISSN 2278-3091

Volume 9, No.3, May - June 2020

International Journal of Advanced Trends in Computer Science and Engineering

Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse177932020.pdf

https://doi.org/10.30534/ijatcse/2020/177932020

# Dynamic Information Protection Method on Computer Optical Networks

**Kharlai Liudmila**[1], **Kunakh Nataliya**[2], **Sotnichenko Yulia**[3], **Konovalov Oleksiy**[4], **Skubak Olexandr**[5], **Manko Oleksandr**[6]

[1]Philosophy Doctor, the Head of the Information and Communication Networks Department, Kyiv College of Communication, Kyiv, Ukraine, lharlay@i.ua

[2]Doctor of Technical Sciences, Professor, Department of Telecommunications of Odessa National Academy of Communications named after O.S. Popov, Kyiv, Ukraine, ignaku@ukr.net

[3]Lecturer high category, Kyiv College of Communication, Kyiv, Ukraine

[4]Philosophy Doctor, the Head of the Scientific Department, Kyiv College of Communication, Kyiv, Ukraine, alex_metapost@meta.ua

[5]Philosophy Doctor, docent, Department of Telecommunications of Odessa National Academy of Communications named after O.S. Popov, Kyiv, Ukraine, skubakan@ukr.net

[6]Doctor of Technical Sciences, Professor, Department of Telecommunications of Odessa National Academy of Communications named after O.S. Popov, Kyiv, Ukraine, manko_kiev@ukr.net

## ABSTRACT

This paper describes a new method of protecting the information flows transmitted by optical links. It is based on the formation of special linear codes with an increased number of units, which can be significantly increased compared to the number of units of the main code at the entrance to the line. At the same time, only passive optical elements are used to form linear codes and produce reverse operations, namely: it is fiber splitters and delay lines for a certain part of the clock interval.

Using a special linear code significantly increases the security of information in case of unauthorized access to linear structures. However, when using a constant type of code, there is a risk that it will be intercepted during unauthorized access and further analyzed to develop appropriate counter-measures. Taking into account this, regular change of linear codes by pseudorandom law is envisaged in the use of active devices such as optical switches, which differ in almost negligible switching time, and at the expense of which they can be applied at all possible transmission mode including the highest transmission rates. An appropriate construction of a linear optical tract is proposed for switching two types of codes with determining the connection points of passive and active equipment. The use of optical codes with a return to zero is proposed as the base codes for the further formation of linear codes. For the sake increasing of further level of security in the work dynamic switching of three types of generated linear codes are offered. The application of the proposed method with a high rate of switching of several types of code combinations significantly increases the security of such critical infrastructure as the computer optical network from unauthorized access to information at the level of linear structures. The use of passive and active elements allows you to create effective principles for the dynamic protection of information of linear structures of optical computer networks. These principles combine both the formation of a number of types of protected linear codes and the regular rapid switching of them at random times. This greatly increases the level of protection. An additional advantage is the ability to perform passive and active optical elements in integral-optical form.

**Key words:** Optical fiber, unauthorized access, information security, optical splitter, optical switch, optical delay line

## 1. INTRODUCTION

Currently, the amount of confidential information transmitted over optical communication networks is constantly growing. This necessitates the protection of such an important infrastructure as a computer optical communications network from unauthorized access, especially at the level of linear structures, most of which are located outdoors.

Fiber-optic communication lines, due to the characteristics of the distribution of electromagnetic energy in the optical fiber, have increased protection against access to information transmitted along the linear tract [1]. However, there are situations in which access to information becomes possible, and this leads to the need to develop measures to counter such attempts.

The protective sheath, the armor cover and other structural elements of the optical cable (OC) so strongly weaken the possible radiation outside the optical fiber (OF) that it practically does not penetrate the limits of the sheath. Consequently, information interception can only occur due to a violation of the integrity of the outer sheath and other cable sheaths in order to directly access the interception equipment to optical fibers. But even in this situation, without additional effects on the fiber, the interception of the optical signal is impossible, since there is practically no radiation outside the optical fiber.

In order to provide radiation outside the optical fiber in this situation, a bending of the OF is formed. In the place of such bending the law of full internal reflection is violated and radiation of energy of a light signal outside of OF is observed [2]. Because of this, at the point of interception of information, the fiber is characterized by an increased level of losses [3], which can be determined by optical reflectometry [4], or by increasing the error rate in the line [3]. In this case, from the moment of removal of information to the moment of detection of unauthorized connection, some time passes, which depends on the principles of monitoring the line and equipment used for control. If specialized high-sensitivity equipment is used to record information, the radiation at the bend of the OF required for its operation may be quite insignificant. In this case, it is not easy to establish the fact and determine the place of connection with the help of line control equipment. There is a method of determining the moment and place of violation of the armor of the cable in the process of unauthorized connection to the line [5], but it allows you to provide supervision at relatively short distances from the point of the control.

There is a method for determining the moment of unauthorized access to optical linear closures along the entire length of the regeneration section [6]. This allows you to accurately determine the location of the optical closure and the moment of access, but the linear structures between the optical closures go unnoticed. Thus, in order to prevent unauthorized access to information flows on optical lines, it is necessary, along with methods for determining the presence of access, to apply additional methods that make it impossible to adequately interpret the information during the fact of access. For this purpose, various cryptographic methods have been developed and are used, which are based on fairly sophisticated software [7], [8]. At the same time, in [9], [10], [11] it was proposed to use continuous additional coding (masking) of optical linear codes of the RZ type using passive optical devices.

## 2. FORMATION OF LINEAR CODES USING PASSIVE ELEMENTS

At this time on optical communication networks there is a use of a linear code type RZ (return to zero) [12], [13]. The main difference of this code is that the value of the signal corresponding to the transmission of a single symbol is returned to zero before the end of the clock interval. The code type with a return to zero on half of the clock interval T is denoted as RZ-0.50, and on the quarter of the clock interval is denoted as RZ-0.25. The type of code, the duration of a single character of which is the full clock interval T, is denoted as NRZ (without returning to zero).

Studies show that when using the optical transmission system of the linear code RZ-0.25, it is possible, using only passive optical elements such as optical delay lines and optical splitters (dividers), to perform additional coding (masking) of the signal at the input of the tract to protect the information that is transmitted along a linear tract [9]. Fig.1 shows the method of masking the optical signal in order to protect it from unauthorized access to the linear tract and its subsequent decoding at the receiving end. The figure shows the time diagrams of the code combination during the passage of certain points of the optical linear tract. Here as I the designation of the intensity of the optical signal is given. Figure 2 shows the construction of a linear tract using this principle. As can be seen from the figure, the output signal of the transmission system, which is also the input signal for the linear tract, based on the code RZ-0.25, and denoted as $I_{in\ RZ\text{-}0.25}$, is connected to the optical splitter ($OD_1$). The optical splitter (divider) works as an optical power divider in half. Then, to the inputs of the second divider ($OD_2$), operating in the adder mode, connects the part of the signal that has passed through the optical delay line ($ODL_1$) with a delay time T/2 ($I_{out\ ODL\ (T/2)}$) and the undelayed part of the signal. As a result, at the output of the second divider code combinations are formed that differ from the original by twice the number of units ($I_{\Sigma}$), which are transmitted on a linear tract. At the output of the linear tract, the optical power divider ($OD_3$) is turned on as an optical power divider in half. In this case, to the second divider ($OD_4$), operating in the adder mode, is fed an undelayed part of the signal $I_{\Sigma}$, and part of the signal that has passed through the delay line ($ODL_2$) with a delay time T/4 ($I_{out\ ODL\ (T/4)}$). After assembling these parts, an optical signal corresponding to the original is formed in the NRZ code ($I_{\Sigma out\ NRZ}$). The double number of units in the optical linear tract during transmission makes it impossible to adequately recover the signal when trying to gain unauthorized access to information. This ensures the protection of the transmitted information.

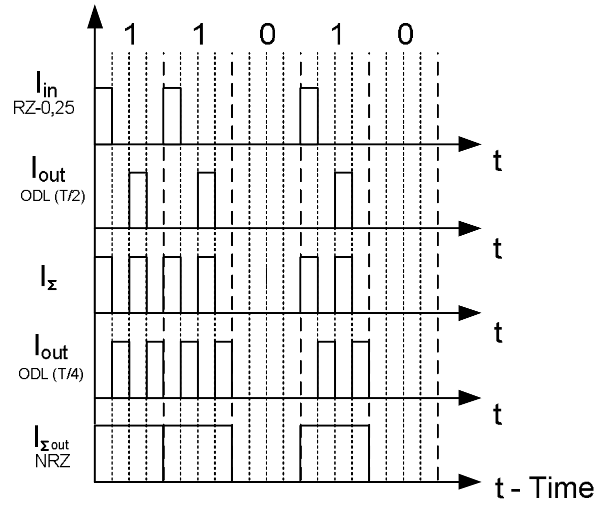


**Figure1:** Method of forming a linear code for the optical signal in the code RZ-0.25 when transmitting it on a linear tract and restoring the output signal in the NRZ code. I – is the designation of the intensity of the optical signal

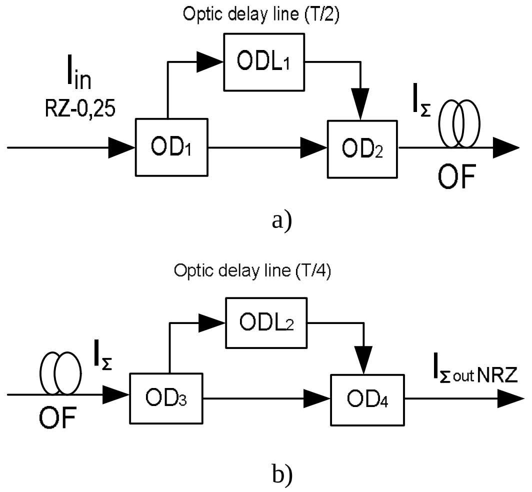


**Figure 2:** Construction of a linear tract using linear encoding and decoding of the optical signal in the code RZ-0.25 using passive elements. Here a - is the transmitting part; b - is the receiving part

The proposed method can be developed and improved, and extended to other types of RZ code. For example, Figure 3 shows a method of masking linear code combinations of an optical signal in order to protect it from unauthorized access to the linear tract and its subsequent decoding at the receiving end using the optical code RZ-0.125 [9], [10], [11]. Figure 4 shows the construction of a linear tract using this principle.

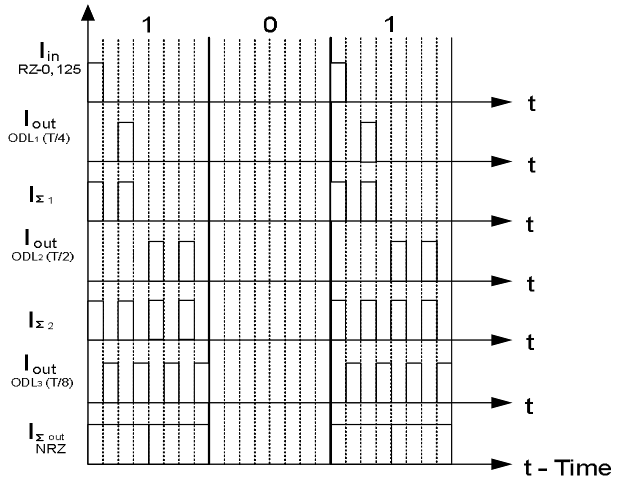


**Figure 3:** Method of forming a linear code for the optical signal in the code RZ-0.125 when transmitting it on a linear tract and restoring the output signal in the NRZ code. I – is the designation of the intensity of the optical signal

The construction of the linear tract in this case contains one degree of optical delay more than in the previous case. An optical signal (code combination) using the code RZ-0.125 and denoted as $I_{in\ RZ\text{-}0.125}$, is fed to the divider ($OD_1$). The optical divider works as an optical power divider in half. After that one part of signal is fed to the delay line $ODL_1$ with a delay time of a quarter of the clock interval T/4 ($I_{out\ ODL1\ (T/4)}$). The second part of the signal propagates without delay. Then the both components of the signal are added, and at the output of the optical splitter in the adder mode ($OD_2$) a code signal with twice the number of units ($I_{\Sigma 1}$) is formed. This signal is fed to the splitter $OD_3$. One of the components after leaving the divider passes through the optical delay line $ODL_2$ (delay time T/2, and on the output of the line $ODL_2$ signal is denoted as $I_{out\ ODL2\ (T/2)}$ ) and adds with the undelayed part in the adder $OD_4$. The number of units after such a forming process in the linear code combination will be four times greater than in the original. The generated and protected signal $I_{\Sigma 2}$ from the output $OD_4$ is fed to the linear tract. At the output of the linear tract, the signal is fed to the optical splitter $OD_5$ which divides it into two components.

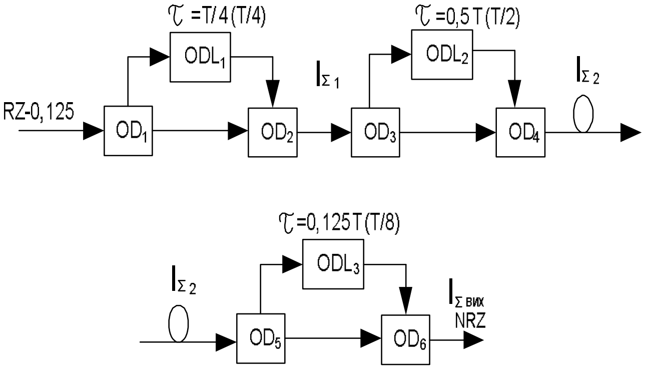
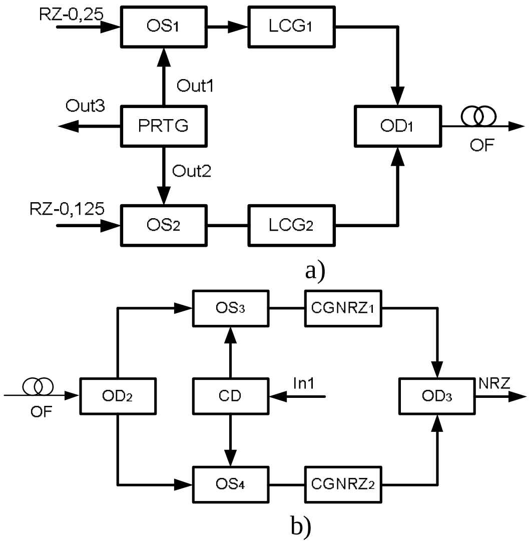


**Figure 4:** Construction of a linear tract using linear encoding and decoding of the optical signal in the code RZ-0.125 using passive elements

One of these parts passes through the optical delay line $ODL_3$ (delay time T/8, and on the output of the line $ODL_3$ signal is denoted as $I_{out\ ODL3\ (T/8)}$) and is added to the undelayed part of the code combination in the optical adder $OD_6$. In this case, an optical signal is generated at the output of $OD_6$, with code combinations that are adequate to the initial code combinations, only in the NRZ code ($I_{\Sigma out\ NRZ}$). This method can be generalized for the code RZ-($1/2^{n+1}$), where n is a positive integer. Cases when n = 1 and n = 2 were discussed above. Construction of a linear tract with increasing number n will be performed at the transmitting end as the connection of a number of elements that perform the division of the signal in half, the delay of one of the components to the corresponding part of the clock interval and their subsequent assembly. At the receiving end, the function of translating the linear code into the NRZ code will be performed by the same elements using the optical delay line for time $T/2^{n+1}$. The number of units in the code combinations of the optical linear tract will be $2^n$ times greater than in the original combinations. The use of fairly inexpensive passive optical elements to mask optical linear codes significantly increases the reliability of the information protection process, compared with the use of active equipment.

## 3. DYNAMIC PROTECTION OF INFORMATION ON COMPUTERS OPTICAL NETWORKS

Given the fact that unauthorized access systems can be adapted to a certain fixed variant of linear codes, the paper proposes a dynamic system for switching variants of linear codes under a pseudo-random law. The block diagram of such a device is shown in Figure 5. In this case, two systems of forming linear code combinations are used, which are switched according under pseudo-random law. To this end, the paper proposes to use two systems for generating linear codes based on input codes (e.g. RZ-0.25, RZ-0.125), as shown in Fig. 5. In this case, two types of linear code generator (LCG) operate on the transmitting end, forming code combinations based on signals from the transmission system in the codes RZ-0.25 and RZ-0.125, respectively. The linear tract receives signals in the selected code in accordance with the control signals from the generator of pseudo-random time intervals (PRTG). The signal from the outputs 1, 2 of the PRTG generator is fed to the control input of the optical switches $OS_1$ and $OS_2$, operating in key mode. In this case, a linear code generator is selected for forming linear code combinations. The output signal PRTG from output 3 is supplied to the transmission system to generate a pilot signal when the linear code changes. Considering the fact that the signals at the outputs of the LCG generators must be mutually inverted - the corresponding information signal is received at the input of only one of the linear code generators ($LCG_1$ or $LCG_2$). After the formation of the linear code combination, it enters the optical divider $OD_1$, which operates in the mode of combining signals, and then enters the optical linear tract. At the receiving end, a linear code combination is supplied to the optical divider $OD_2$ and to the inputs of the optical switches $OS_3$ and $OS_4$ operating in key mode.



a)

b)

**Figure 5:** Construction of a linear tract that uses dynamic information protection. Here a - is the transmitting part; b - is the receiving part

The control inputs of the switches receive a signal from the control device (CD), which is formed at the receiving end according to the pilot signal from the transmitting end. The signal from the CD provides the passage of a linear signal to the corresponding code generator NRZ ($CGNRZ_{1,2}$) and the subsequent passage of the code in NRZ format through the optical splitter $OD_3$, operating in the mode of combining signals, to the input of the optical receiver.

Thus, the proposed solution further protects information flows from unauthorized access at the level of linear optical computer communication structures. If it is necessary to increase the level of protection, you can use the code RZ-0.0625 and the corresponding line code generator in addition to the input codes RZ-0.25 and RZ-0.125.

The construction of protection is complicated by the appearance of additional elements. The switching speed of linear code variants is determined by the switching time of optical switches, among which should be noted switches based on the Mach-Zender interferometer (MZI) and electro-optical switches (EOS) [14], [15]. The switch based on the MZI is built on the basis of two series-connected optical splitters (branch factor 3 dB), which are interconnected by two optical waveguides of different optical lengths to create a phase difference at the output of II by changing the voltage U applied to one of shoulders of the interferometer Figure .6.

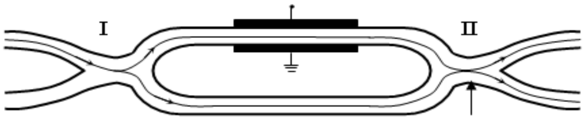


**Figure 6:** Switch based on the Mach - Zender interferometer

Due to the fact that the optical waveguide to which the electric field is applied is made of an electro-optical material, such as lithium niobate ($LiNbO_3$), its refractive index changes with voltage. This changes the phase difference between the signals coming to the output II and there is a redistribution of signal power between the outputs of the interferometer so that it can be directed completely to one of the two outputs of the interferometer. When using only one output, the switch can operate in key mode.

Electro-optical switches also use directional couplers to generate light flux at one of the output ports Figure 7. But this is done by changing the coupling factor between the optical waveguides. The coupling factor is changed by changing the refractive index of the splitter material in the optical coupling zone. Optical waveguides a) and b) in sections MN and DF are made of electro-optical material. Transparent electrodes are available on the outside between the optical waveguides. Due to the applied voltage, the refractive indices of optical waveguides can be changed. The division factor of the splitter also changes as a result. Electro-optical switches have a great advantage, which is manifested in the switching time, which reaches a value of the order of 10 - 100 ps [12], and it is manifested in small values of control voltages - 2.5 - 3 V. The advantage of electro-optical switches is also the ability to be made in integral-optical form.

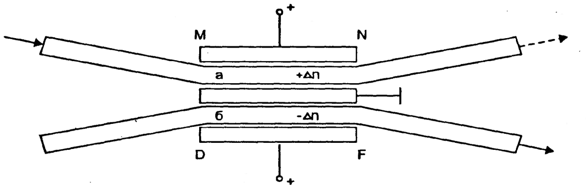


**Figure 7:** Switch based on a directional splitter X - type.

Thus, the use of passive (splitters and delay lines) and active elements (switches) allows creating effective principles of dynamic protection of information on the linear structures of computer optical networks. These principles combine both the formation of a number of types of protected linear codes and their regular rapid switching at random times. This significantly increases the level of protection, as it makes it virtually impossible to adequately and timely track and identify a specific type of code in real time. In addition to this, the proposed protection method practically excludes the operation of a hidden transmitter in a line [16].

## 4. CONCLUSION

The proposed new method of dynamic protection of information on the linear structures of computer optical networks, allows increasing the security of these networks from unauthorized access. The main advantage of the method is the fast switching according to the pseudo-random law of a number of linear codes generated by a special algorithm using exclusively passive optical elements. The number of units in linear code combinations can significantly exceed the number of units of the main code. Due to this, adequate perception of the main code becomes impossible. However, in the case of constant use of a certain type of linear code, it is possible, as a result of analysis, to take measures to its adequate perception. In order to prevent such a situation, the paper proposes a dynamic principle of protection, which consists in the rapid switching of types of linear codes according to the pseudo-random law. Given the high switching speed, and the pseudo-random law of switching in time, adequate perception of information becomes almost impossible. An additional advantage of the method is the ability to perform all the elements it includes in an integral-optical form.

## REFERENCES

1. R. Freeman. ***Fiber Optic Communication Systems,*** Moscow: Technosphere, 2003, pp. 38-39. https://doi.org/10.1016/S0270-9139(03)80022-8
2. A. V. Listvin, V. N. Listvin, D. V. Shvyrkov. ***Optical fibers for communication lines,*** Moscow: LESARart, 2003, pp. 18-19.
3. A. V. Yakovlev. **Fiber optic system for transmitting confidential information**, *Telecommunication*, № 10, pp. 11-13, October 1994.
4. A. V. Listvin, V. N. Listvin. ***Reflectometry of optical fibers,*** Moscow: LESARart, 2005, pp. 17-18.
5. S. S.Gordienko, O. O. Manko, S. B.Gordienko. **Monitoring of fiber-optic line structures in order to protect information from unauthorized access,** *Communication*, № 1 (97), pp. 32-34, January 2012.
6. O. O. Manko. **Protection of fiber-optic line structures from unauthorized access using metal elements of optical cable,** *Modern information protection*, № 3, pp. 84-86, March 2012.
7. Rashad J. Rasras, Ziad Alqadi, Mutaz Rasmi Abu Sara, Belal Zahran. **Developing new Multilevel security algorithm for data encryption-decryption (MLS_ED),** *International Journal of Advanced Trends in Computer Science and Engineering***.** 2019. Vol. 8, № 6, November-December. pp. 3228-3235. https://doi.org/10.30534/ijatcse/2019/90862019
8. Mahendra Vucha, A. L. Siridhara. **High Speed Cryptography Architecture for Health Information Exchange,** *International Journal of Advanced Trends in Computer Science and Engineering*. 2019. Vol. 8, № 4, July-August. pp. 1443-1448.
9. O. O. Manko. **Using masking of optical line codes to protect information on fiber optics,** *Modern information protection*, special issue, pp. 90-92, 2012.
10. O. O. Manko. **Using Passive Optical Devices for the Protection of Information in the Optical Communication Lines,** *in Proc. Third International Scientific-Practical Conf. "Problems of Infocommunications. Science and Technology (PIC S&T`2016)"* October 4-6, 2016, Kharkiv, Ukraine, pp. 73-74.
11. O. O. Manko, O. S. Shmatok, A. A. Petrenko. **Use of passive optical devices for information protection in fiber-optic communication lines and networks,** *Information protection*, Vol. 19, № 2, pp. 143-147, April-June 2017
12. N. N. Slepov. ***Modern technologies of digital fiber-optic communication networks,*** 2nd ed. Moscow: Radio and communications, 2003, pp. 22-23.
13. S. A. Dmitriev, N. N. Slepov. ***Fiber optic technology: Current status and prospects***, 2nd ed. Moscow: Fiber Optic Technology LLC, 2005, pp. 81-82.
14. R. R. Ubaidullaev. ***Fiber optic networks***, Moscow: ECO-TRENDZ, 2001, pp. 277-278.
15. O. K. Sklyarov. ***Fiber optic networks and communication systems: a Training manual,*** 2nd ed. St. Petersburg: Publishing House "Lan", 2010, pp. 169-170.
16. Laptiev Oleksandr, Shuklin German , Savchenko Vitalii, Barabash Oleg, Musienko Andrii, Haidur Halyna. **The Method of Hidden Transmitters Detection based on the Differential Transformation Model,** *International Journal of Advanced Trends in Computer Science and Engineering*. 2019. Vol. 8, № 6, November-December. pp. 2840-2846. https://doi.org/10.30534/ijatcse/2019/26862019