Fiber-Optic Channel of Voice Information Leakage

Vladimir Grishachev, Yuliya Kalinina, Oleg Kazarin
Institute for Information Sciences and Security Technologies
Russian State University for the Humanities
Moscow, Russia
grishachev@mail.ru, abarakedavra@gmail.com, okaz2005@yandex.ru

***Abstract* – The article describes a technical channel of voice information leakage in fiber-optic communications, which is created with parasitic modulation in the light stream that goes through regular connection system. A threat model for voice information is presented with a description of channel operation distinctions. Places and areas of intelligence accessibility are researched and a possible scenario of threat attack is considered. In addition, the article gives recommendations for building an effective system of voice data protection in facilities containing fiber-optic communications.**

Keywords – voice information leakage; fiber-optic communications; technical channel of information leakage; threat model, information security

INTRODUCTION

Fiber-optic technology has several advantages such as: multifunctionality, high bandwidth, noise immunity and the absence of spurious electromagnetic radiation and interference. The wide spread of fiber-optic technologies in communication and measurement systems implies that we should concider the safety of their use. Fiber has a really wide use of external physical fields as a measuring transducer [1]. In this regard, the question arises about the possibility of convergence of transmitting and receiving information functions. For instance, the use of standard optical communication networks as a non-standard distributed acoustic measuring system for collecting voice information [2]. This article describes threats and methods of ensuring the security of confidential negotiations at an information object containing fiber-optic networks.

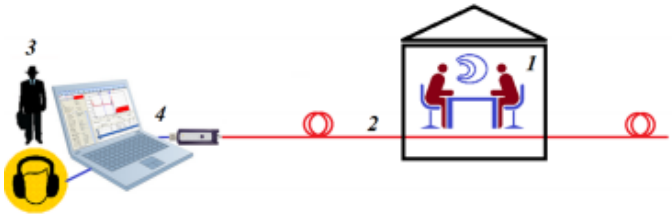

Fig. 1 The generalized structure of the fiber-optic channel of voice information leakage. 1 - source of speech information at the information object, 2 - standard optical system, 3 - violator, 4 - means of technical intelligence

LEAK CHANNEL MODEL

To estimate the parameters of the leak channel, we take some averaged parameters of the protected premises and a signal. The building is no more than 100 m high, the perimeter length is about 400 m, in which the protected room of 3 x 10 x 20 m3 is located, the wall material is concrete, 0.25 m thick, the sound absorption of walls is 0.3. Speech is a homogeneous acoustic signal in the air with a sound pressure level (SPL) of 40–75 dB, frequency range 100–4000 Hz, the ratio of the mean-square power of the information signal-to-noise ratio (SNR) of at least 10 dB.

Fiber-optic channel of voice information leakage: generalized structure

Fiber-optic communications for various purposes in cable channels are distributed throughout the information object. Communications can be in acoustic contact with the source of speech through the air and building structures [3]. The intruder gains access to the optical cable and conducts optical sensing, recording the optical informative signal.

Fiber-optic channel of voice information leakage: the formula

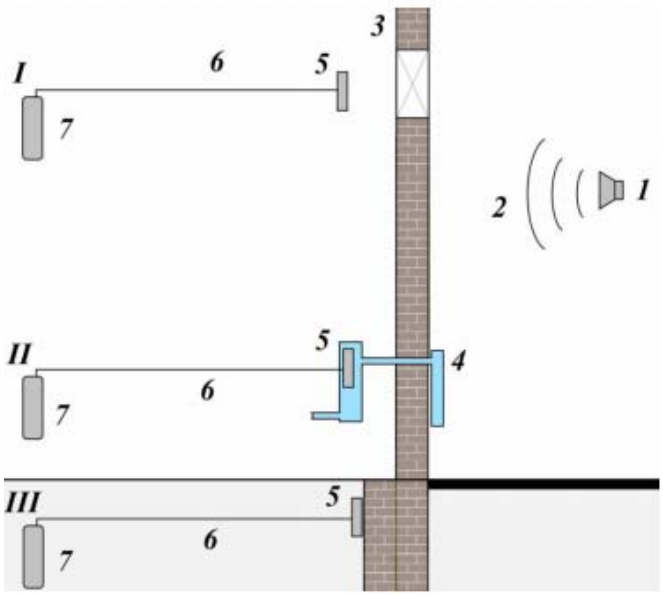

Fig. 2 The generalized structure of the formation of informative signals.

Aerial or structural acoustic signal from a source of voice information has a mechanical effect on passive elements of a standard fiber-optic network (fiber, fiber connections, splitters, etc.). Changing the geometric and optical parameters of network elements in the field of an acoustic wave leads to

978-1-7281-0339-6/19/$31.00 ©2019 IEEE

parasitic modulation of the light flux. An internal or external intruder is connected to the optical network of an information object using standard radiation or other probing radiation in the circuit for transmission or reflection (reflectometry) from selected sections of the network with optical inhomogeneities. Luminous flux with spurious acoustic modulation is output and decoded, which provides covert access to confidential voice information circulating at the information object in designated rooms such as meeting rooms, executive offices, and office premises.

Parasitic acoustic modulations do not exceed 0.3% for the transmitted light fluxes and do not have a significant effect on the transmission of the main signal in optical networks, so they are not given a value [4]. The modulation depth of the optical signal determines the effectiveness of the leak channel information signal. The greatest modulation depth is possible on the internal optical inhomogeneities of the network, which are created by connecting fibers, cable bends or mounting fixtures.

Informative leak channel signals

In the channel of voice information leakage, there are two types of informative signals, primary and secondary. Acoustic informative signal (primary) is an acoustic field outside protected premises. According to the distribution environment, it is divided into three types, one being an aerial leakage channel (sound in the air), the other being a structural leakage channel (sound in built formations) and, finally, a leakage hydroacoustic channel (sound in water communications). The impact of the acoustic informative signal on elements of the fiber-optic channel forms an optical informative signal (secondary) in the optical fiber, which is a modulated light flux passing near the protected premises. The signal propagation environment is optical networks. The convergence of fiber optic functions on the basis of a regular information network of an information object makes it possible to create a non-standard distributed measuring speaker system that exceeds the size of the information object itself.

Under critical conditions, the radius of the general zone of intelligence accessibility for a channel of voice information leakage through fiber-optic communications reaches 250 km, which includes the maximum distance for acoustic and optical informative signals.

THREAT SCENARIO

Stage 1. Research / Preparation

The main technical intelligence tool for the fiber-optic channel is an optical reflectometer. Its basic function is to take the reflectogram with a frequency of sound from 10 Hz and higher, with different duration and power of the probing light pulse, depending on the distance. For probing the intruder requires registration of backscattered radiation only from specific fiber sections with a frequency of about 1000 Hz. This requires rebuilding the driver's software code. The resulting functionality is called the sensor mode. The reflectometer is tuned to probe standard and artificially created optical inhomogeneities. The main effect is achieved by distributed measurements over a large number of inhomogeneities with the selection of informative signals in a phase. To implement a fiber-optic channel of voice information leakage, the presence of optical networks near the information object with connected reflectometers is necessary. Reflectometers are combined into a single virtual information intelligence network through the same standard or other artificially created networks.

Stage 2 Setup / Test

It is essential to form an intelegence network. For each measurement site it is required to determine the sensitivity (weighting factor) and also relative and absolute response time needed to select the signal from the noise phase. Specially prepared reflectometers have to be connected to the selected optical networks. Reflectometers are to be combined into an information intelligence network with a single control center remote from the object being explored. Analyze the networks for the presence of optical inhomogeneities and record the relative response time. Set up an intelligence network, for example, using an ultrasound monochromatic signal inside or near the protected premises to determine the sensitivity, relative and absolute response time.

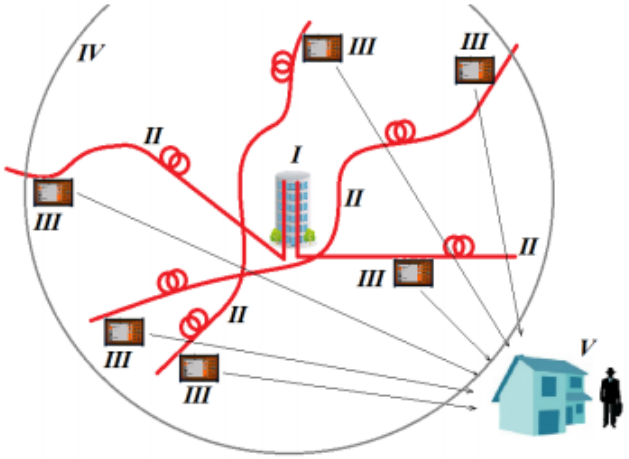

Fig. 3 Schematic diagram of an illegal distributed optical measuring network based on standard optical networks. I - the informatization object, II - the standard optical networks in and near the object, III - optical reflectometers, IV - the intelligence accessibility area, V - the intruder

Stage 3 Practical work

The work of the intelligence network is carried out according to the scheme of continuous data collection from all reflectometers for all probed inhomogeneities in real time. The selection of the informative signal is carried out in the processing center according to an algorithm corresponding to the chosen listening position at the object and phase of the signal.

THE PROTECTION OF VOICE INFORMATION IN THE LEAK CHANNEL

Since leakage is possible both through aerial and structural channels, a set of protective measures is required to ensure that two channels are blocked:

- minimize spurious interference (modulation) in the optical cable system;
- limit the output of the acoustic and optical informative signal outside the protected area;
- prevent or detect illegal connections to the optical network.

Protection methods should be applied depending on the structure and purpose of the information network, including fiber-optic communications.

Acoustic cable shielding. The main recommendations for shielding are as follows: near the sources of confidential voice information, the quality of the cable should be the highest; network topology include the minimum number of bends and twists with the largest possible radius, connectors and other discontinuities; all switching elements are remote from the source of information, otherwise, they should be sound-isolated.

Filtering and noise masking of the optical signal. This method is implemented by directly connecting the intermediate active equipment into the optical network, or by applying an external noise physical field to the cable itself. For example, by installing a large number of vibro-acoustic noise emitters distributed throughout the building. In this case, the impact is on only at the required points in time and with the required power.

Detection of spurious interference (modulation) and probe radiation. There are several methods for monitoring spurious acoustic modulations and pickups in an optical network and abnormal network connections. Mode power monitoring method is a registration of the change in signal power of direct and return losses in case of unauthorized connection. The method of measuring optically significant power requires a constant level of a coded signal, not dependant on the availability of information [5]. These methods are implemented on the receiving side. The implementation of one more method is possible by adding light flux analysis functions to the transceiver, which will allow combining the signal source with the protection device [6]. Based on the presence of spurious modulation and probing radiation, it is possible to conclude that there are threats of eavesdropping [7].

Neutralization of informative return radiation [8] Counteraction to leakage channels based on reflectometric methods is the noise masking of returnable radiation, when the probe signal of the reflectometer follows the not noisy area, and the returnable radiation follows over the area with 100% noise. The creation of such a device is realized, for example, by a counter-asymmetric connection of 2 outputs of a 1x2 coupler with a branch of less than 10% with 2 outputs of the same coupler, so that the main channel is connected to a branch. In this case, direct and reverse directed luminous flux will follow in different parts of the device. When establishing a noise generator in one area, we obtain a slightly noisy stream (in direct) for probing radiation and a strongly noisy stream (in reverse) for an informative optical signal.

CONCLUSION

Fiber optic channel leakage of voice information is a high degree danger. Leak channel detection is possible only in networks with optical network monitoring. But the identification of changes in the signal level and even the elimination of several reflectometers will not precisely identify, localize and eliminate information leakage. To build an effective information protection model, it is necessary to combine all protection methods with regard to the design of a specific fiber-optic network.

REFERENCES

[1] N.K. Dushutin, A.Y. Mohovicov "Из истории физики конденсированного состояния". Irkutsk: ИГУ, 2014.

[2] V.V. Grishachev "Detecting threats of acoustic information leakage through fiber optic communication". Journal of Information Security, Vol. 3, Num. 2, 2012, pp. 149-155.

[3] V.V. Grishachev, D.B. Halyapin, N.A. Shevchenko "Анализ угроз утечки речевой информации через волоконно-оптические коммуникации." Information security questions, №4, 2008, pp. 12-17.

[4] V.V. Grishachev, O.A. Kosenko "Практическая оценка эффективности канала утечки акустической (речевой) информации через волоконно-оптические коммуникации". Information security questions, №2, 2010, pp.18-25.

[5] All Optical Networks (A ON), National Communication System, NCS TIB 00-7, August 2000.

[6] V.V. Grishachev, O.V. Kazarin, Y.D. Kalinina "Физические методы оценки эффективности угроз утечки речевой информации через технические каналы на объекте информатизации". Information security questions, №4, 2017, pp. 44-54.

[7] M.Z Iqbal, H Fathallah, N Belhad J. 2011. Optical Fiber Tapping: Methods and Precautions. High Capacity Optical Networks and Enabling Technologies (HONET).

[8] V.V. Grishachev "Устройство защиты оптической сети от несанкционированного зондирования методами оптической рефлектометрии" Patent of the Russian Federation for invention № 2 551 802 with priority 18.12.2012.