AMERICAN JOURNALS
Open Access, Peer Reviewed Journals

American Journal of Pedagogical and Educational Research
ISSN (E): 2832-9791| Volume 7, | Dec., 2022

ANALYSIS OF AVAILABLE PROTOCOLS IN OPTICAL COMMUNICATION NETWORKS

Yusupova Zamira Zaripovna,
Senior Lecturer, Department of Information and
Educational Technologies, TUIT, Muhammad al-Khwarizmi

A B S T R A C T	K E Y W O R D S
Nowadays, it is difficult to imagine the whole world without optical fiber, because all the Internet is being organized through optical fibers. Their security is of great importance, cryptographic algorithms have a great place to implement it, so the protocols in optical fiber were analyzed in the article.	Protocol, network, base, byte, ethernet, HTTP, DNS, IP, UPD.

It is known that every network works through protocols. Any network protocol is a set of certain actions and rules that allow the correct connection and data exchange between any devices that enter the network. The communication medium is, of course, a fiber optic communication cable. Typically, protocols describe different aspects of any type of communication, and together they form a set of protocols. Its purpose depends on the type of protocol. For example, a protocol can determine the physical characteristics of lines, the rules for using network nodes, the order in which parts of messages pass, and so on.

Standard TOAL protocols are Ethernet-100 BASE-F, Ethernet-1000 BASE-SX, ATM, FDDI LSF, Fiber Channel, 10GBASE-E and 10GBASE-L. All of them are designed for the correct operation of optical fiber communication lines. Let's look at the characteristics of some of them. It is important to know them before you start connecting the optical cable to the receiver.

ATM protocol (asynchronous transfer mode) is a broadband version of ISDN, operating at a speed of 150.52 Mbit/s. The ATM protocol is based on ready-made port switching tables through switches with installed and configured virtual connections.

In addition to this main task, the ATM protocol performs a number of functions of monitoring the execution of the traffic contract by the network user, as well as flow control.

Ethernet-100 BASE-F is a standard that uses the long-wavelength part of the spectrum-1300 nm. It is transmitted through two transmitters used for receiving and transmitting. The length of such a line can be up to 400 meters.

We'll also look at protocols that allow data to be hidden on the network. These are the following:

1) Hypertext Transfer Protocol (HTTP) - HTTP is an application layer protocol designed to transfer data between networked devices and runs on top of other layers of the network protocol stack. A

typical flow over HTTP involves a client machine sending a request to the server, which then sends back a response message. Hidden messages can be embedded in HTTP protocol headers.

2) Domain Name System (DNS) protocol - A covert channel can be created indirectly through the DNS protocol. The channel uses negative caching of domain names. IP packets can be tunneled through the DNS protocol. Communication is between the client and the fake DNS server.
3) Various other application protocols can be used as covert channels. Voice over IP (VoIP), Real-time Transport Protocol (RTP), Real-time Control Protocol (RTCP), Secure Shell (SSH) protocol, Message Authentication Code (MAC) header, and File Transfer Protocol (FTP) are used to implement network steganography possible
4) Payload tunnels are hidden channels that carry the payload of one protocol to another protocol. The IP protocol is often used. IP over ICMP, SSH over HTTP proxies, and UDP or TCP over HTTP can be used to tunnel payloads.

Table 1 below shows important points from different protocols for network steganography. The protocol used by the corresponding layer and the Steganographic power thus obtained are also shown. The detection capabilities of a given protocol are also given.

Table 1 Using different protocols for network steganography

№	Title	Protocol	Opportunity	Determination
1.	Steganography based on network packet payload parity	UDP	1 bit/pack et	It's difficult
2.	Practical Internet Steganography: Hiding Data on IP	IP	Depends on the selected field	-
3.	Retransmission steganography and its detection	TCP	180 byte/s	Not easy
4.	Length-based network steganography using the UDP protocol	UDP	456 byte/s	Not easy
5.	StegTorrent: A Steganographic Method for P2P File Sharing Service	UDP	270 byte/s	It's difficult
6.	PadSteg: Introducing Interprotocol Steganography	TCP/ARP	32 byte/s	It's difficult
7.	Flow Control Transfer Protocol Steganography	TCP/UDP	Depends on the selected field	-

REFERENCES

1. Jorayev N.M., Technical service of fiber optic communication systems and networks, Tashkent University of Information Technologies, Tashkent, 2017.
2. Ganiev S. K, Karimov M. M., Tashev K. A., 2016. Information security. Tashkent University of Information Technologies Tashkent, Uzbekistan, pp. 17-24.
3. Bartosz Jankowski, Wojciech Mazurczyk and Krzysztof Szczypiorski. “PadSteg: introducing interprotocol steganography”, Institute of Telecommunications, Warsaw University of Technology, Warsaw, Poland, ISSN 1018-4864, Volume 52, Number 2, Springer 2013.