The Central Research Institute
of the Armed Forces of Ukraine

Military Science. Vol. 1 No. 1 (2023)

DOI: 10.62524/msj.2023.1.1.14

The data transfer protocols analysis in the perspective scientific (scientific and technical) information exchange automated system in the Armed Forces of Ukraine

Oleksii Nozdrachov
deputy head of the institute for moral and psychological support
Central Research Institute of the Armed Forces of Ukraine
03049, 28B, ave. Povitroflotskyi, Kyiv, Ukraine
e-mail: o.o.nozdrachov@post.mil.gov.ua

Mykola Vasianovych
candidate of military sciences, senior researcher
head of the center
Central Research Institute of the Armed Forces of Ukraine
03049, 28B, ave. Povitroflotskyi, Kyiv, Ukraine
e-mail: m.o.vasianovych@post.mil.gov.ua
ORCID: 0000-0002-8409-4774

Andrii Shnukalo
Senior Research Fellow
Central Research Institute of the Armed Forces of Ukraine
03049, 28B, ave. Povitroflotskyi, Kyiv, Ukraine
e-mail: a.d.shnukalo@post.mil.gov.ua
ORCID: 0000-0002-1205-9953

Abstract. The relevance of the study is due to the need to define effective data transfer protocols that ensure high quality of service and security of automated information exchange systems in the Armed Forces of Ukraine and their components.

In this regard, the article is aimed at revealing the protocols of the transport level of the TCP/IP and OSI network models - User Datagram Protocol, User Datagram Protocol Lite, Transmission Control Protocol, Multipath Transmission Control Protocol, Stream Control Transmission Protocol, Datagram Congestion Control Protocol, Reliable User Datagram Protocol from the perspective of their application point of view in the automated systems of scientific (scientific and technical) information exchange in the Armed Forces of Ukraine.

The leading approaches to the study of this problem are the use of informational and logical analysis methods, which allow a comprehensive consideration of network models by means of comparison.

About 15 characteristics has been considered, in particular: transmission reliability, overload control, multithreading. Taking into account the requirements and features of the promising automated system of scientific (scientific and technical) information exchange in the Armed Forces of Ukraine, it was proposed to use certain technological combinations with higher-level protocols to achieve optimal data protection. As a result of the analysis, it was established that, in accordance with the functions of the automated exchange of scientific (scientific and technical) information system, it is more expedient to use the Stream Control Transmission Protocol.

The materials of the article are of a theoretical value for conducting further scientific research on the problem raised, as well as practical value for the improvement of military information systems, in accordance with the standards of the North Atlantic Alliance and today's challenges in cyberspace.

Keywords: data exchange, information technologies, network technologies, military-scientific automated systems.

Introduction

Automated systems of a scientific and technical information exchange in the Armed Forces of Ukraine (AF of Ukraine) are important for ensuring national security and defense. However, their development and functioning require the use of appropriate data transmission protocols that ensure the security of information exchange and the reliability of data transmission without loss of speed.

One of the problems that needs attention in this area is the lack of standards and a unified system of data transmission protocols in the scientific and technical information exchange systems in the Armed Forces of Ukraine. This leads to interaction of different systems difficulties, that can reduce the speed of data transmission, increase the risks of information leakage and compromise the confidentiality of data.

In addition, there is a problem of compliance of existing data transfer protocols with modern requirements for information protection, in particular for counter-cyber-attacks and cyber espionage protection. Due to insufficient security and efficiency of such protocols, significant threats to national security and defense may arise, therefore their analysis with the possibility of further improvement and optimization is an urgent scientific and practical task.

Methodological Framework

The exchange of scientific (scientific and technical) information automated systems (ESIAS) are specialized information systems used for the exchange of scientific data, articles, studies, technical information, etc. between scientific institutions, scientists, researchers and other interested parties.

These systems enable the efficient exchange of scientific information by creating a centralized repository where scientific publications and data can be stored, searched and accessed. Some ESIASs also provide opportunities for interaction between users, such as forums for discussing research or the ability to comment on articles.

The main functions of the scientific information exchange automated systems are:

– information storage and retrieval;
– information classification and processing;
– scientific materials publication and review;
– interaction and cooperation;
– information monitoring;
– scientific productivity assessment.

Considering the advanced scientific (scientific and technical) information exchange automated system in the Armed Forces of Ukraine and its main specifics - application in the military environment, it is necessary to highlight a number of basic necessary functions:

– privacy and security;
– integration with other military systems.

Based on the last two functions, it can be stated that the data transfer protocols in the prospective automated system of the scientific (scientific and technical) information exchange in the Armed Forces of Ukraine must meet the following requirements:

– reliability;

– security;
– standardization;
– multithreading;
– data flow control;
– resistance to failures;
– support of operating systems used in the Armed Forces of Ukraine.

Results

Let`s consider the protocols of the transport layer (Table 1). The computer networks` transport layer is a conceptual division of methods in the multi-level protocol architecture of the TCP/IP (Transmission Control Protocol/Internet Protocol) and OSI (The Open Systems Interconnection model) models. Protocols provide end-to-end communication services for applications at this layer (Papastergiou, 2017).

User Datagram Protocol (UDP) is one of the protocols in the TCP/IP stack. It differs from the TCP protocol in that it works without establishing a connection. UDP is one of the simplest protocols of the transport layer of the OSI model, which exchanges messages (datagrams) without acknowledgment and delivery guarantee. When using the UDP protocol, the responsibility for error handling and data retransmission is assigned to the protocol layer above. But despite all the shortcomings, the UDP protocol is efficient for servers sending small responses to a large number of clients.

UDP Lite (light UDP) is a connectionless protocol that belongs to the transport layer of the OSI model and is similar to UDP. Unlike UDP, in which a packet is either completely checksum protected or the packet is not protected at all, UDP Lite allows the possibility of partial checksums that cover only part of the datagram, thus allowing the delivery of partially corrupted packets. This was created for multimedia protocols where receiving packets with a partially corrupted payload is considered a more feasible option than not receiving the packet at all.

Transmission Control Protocol (TCP) together with the IP protocol is the core protocol of the Internet, that gave the name of the TCP/IP model. The protocol is designed to manage data transmission in computer networks, works at the transport level of the OSI model.

Unlike another common transport layer protocol, UDP, TCP ensures reliable delivery of data from the sending host to the receiving host by establishing a logical connection between the hosts. Thus, TCP belongs to the class of protocols with an established connection.

TCP receives data streams from protocols of the upper layers of the OSI model, the initial source of which are application layer protocols such as Hyper Text Transfer Protocol (HTTP), File Transfer Protocol (FTP), and others. Each upper layer protocol has its own designated TCP port.

TCP divides a particular data stream into chunks and adds a header with a sequence number to each chunk. Data portions obtained in this way are traditionally called TCP segments. Each segment is then encapsulated into an IP packet and transmitted over the IP protocol to the receiving host.

After receiving the IP packet, the receiving host checks the correctness of the received data in the TCP segment by the checksum calculation method and makes sure that the previous data segments were also successfully received. The receiving host then sends a request to the sending host for a new or retransmitted chunk of data, which is also an acknowledgment that all segments with sequence numbers less than the number of the new request have been successfully received.

In turn, TCP segments are de encapsulated from IP packets, placed in the correct order, and TCP headers are removed from them. The resulting data stream is forwarded to the higher-level protocol from which the data was originally received on the sending host side.

Multipath TCP (MPTCP) is the work of the Internet Engineering Group's (IEG) Multipath TCP Working Group, which aims to allow Transmission Control Protocol (TCP) connections to use multiple paths to maximize throughput and increase redundancy.

Table 1. Comparison of transport layer protocols

Characteristic	Protocols						
	UDP	UDP-Lite	TCP	Multipath TCP	SCTP	DCCP	RUDP
Packet header size	8 bytes	8 bytes	20–60 bytes	50–90 bytes	12 bytes	12 or 16 bytes	14+ bytes
Typical costs of data packages	8 bytes	8 bytes	20 bytes	? bytes	44-48+ bytes	12 or 16 bytes	14 bytes
Object package transport. equal	Datagram	Datagram	Segment	Segment	Datagram	Datagram	Datagram
Connection oriented	No	No	So	So	So	So	So
Reliable transportation	No	No	So	So	So	No	So
Keeping message boundaries	So	So	No	No	So	So	So
Delivery	Disorganized	Disorganized	Organized	Organized	Ordered / Unordered	Disorganized	Disorganized
Checksum	Yes No	So	So	So	So	So	Yes No
Checksum size	16 bits	16 bits	16 bits	16 bits	32 bits	16 bits	16 bits
Partial checksum	No	So	No	No	No	So	No
Block maximum transmission path	No	No	So	So	So	So	?
Flow control	No	No	So	So	So	No	So
Congestion control	No	No	So	So	So	So	?
Explicit overload notification.	No	No	So	So	So	So	?
Multithreading	No	No	No	No	So	No	No
Multihoming	No	No	No	So	So	No	No
Stratification / Nagle's algorithm	No	No	So	So	So	No	?

Source: developed by the authors based on open data sources.

In January 2013, the IEG published the Multipath specification as an experimental standard in RFC 6824. In March 2020, it was superseded by the Multipath TCP v1 specification in RFC 8684.

The redundancy offered by Multipath TCP provides inverse multiplexing of resources and thus increases TCP's bandwidth to the sum of all available channels at the connection layer, instead of using one as required by standard TCP. MPTCP is backward compatible with standard TCP.

Stream Control Transmission Protocol (SCTP) is a transport layer protocol in computer networks created in 2000 by the IEG. RFC 3286 provides a technical introduction to it.

Like any other transport layer data transfer protocol, SCTP works similarly to TCP or UDP. TCP and UDP work so differently that it is incorrect to draw an analogy between the two. The whole analogy is that SCTP, TCP and UDP belong to the same layer of the OSI model. But in fact, SCTP has a wide range of innovations in its arsenal, such as multithreading, protection against SYN-flood, as well as synchronous connection between two hosts on two or more independent physical channels (multi-homing).

Datagram Congestion Control Protocol (DCCP) is a transport layer network protocol developed by the IEG. Adopted as a standard in March 2006, it provides mechanisms to monitor network congestion, avoiding the need for application layer mechanisms. This protocol does not guarantee the delivery of information in the desired order.

DCCP is very effective for applications in which data arriving out of time becomes useless. For example: streaming media, online games and Internet telephony. The main feature of these applications is that old messages become useless very quickly, so it is better to receive a new message than to try to forward an old one. But at the moment, most such applications independently implement congestion monitoring, and TCP or UDP are used as transmission protocols.

Reliable Data Protocol (RDP) is designed to ensure reliable data transmission between packet-oriented applications. It was originally designed for applications that implement remote data loading and troubleshooting, but it can be used in other applications that require reliable transmission of messages. There are two versions of RDP, described in the RFC 908 and RFC 1151 specifications, respectively.

Reliable User Datagram Protocol (RUDP) is based on the RDP protocol for transmitting telephone signals over IP networks. This protocol is not standardized and has no official specification.

RDP and RUDP protocols are used in cases where UDP cannot be used due to its unreliability, and the use of TCP causes too high complexity of the data transfer process.

From the point of view of reliability, the following protocols can be considered as providing reliable transport: TCP, Multipath TCP, SCTP, RUDP.

The organization of reliable transport in these protocols has some common features, but also differs depending on the specific protocol (Kurose, 2017).

TCP:

– uses the ACK (Acknowledgment) confirmation mechanism, where the recipient returns a receipt (confirmation) about the successful receipt of each packet;

– provides detection and recovery of lost packets by retransmitting lost packets;

– uses flow control mechanisms, such as a transmission window (Window), to regulate the speed of data transmission from the sender to the receiver.

Multipath TCP (MPTCP):

– distributes traffic between different paths using flow control and load balancing mechanisms;

– has mechanisms to detect and manage packet loss that take into account the distributed nature of a multipath network;

– provides the possibility of dynamic switching between paths in case of changing network conditions.

SCTP:

– uses mechanisms of associations (Association), channels and streams to organize data transmission;

– has mechanisms for detection and recovery of lost packets, including retransmission algorithms and duplicate detection algorithms;

– supports flow control at the channel and thread level.

RUDP:

– contains mechanisms for detecting and restoring lost packets, similar to TCP, but with less complexity;

– may have flow control mechanisms, although the specific implementation may vary depending on the library or software used.

The RUDP protocol does not meet the requirements of standardization.

Consider the protocols TCP, MPTCP, SCTP from the point of view of security.

The TCP protocol has a number of vulnerabilities to modern types of attacks. The shortcomings of the protocol are revealed in successful theoretical and practical attacks, in which an attacker can gain access to transmitted data, impersonate another party, or bring the system to a non-working state. Examples of these attacks are TCP Hijacking and TCP Reset.

Despite a number of obvious advantages of Multipath TCP over its predecessor, this protocol creates new problems. From a network security perspective, multipath routing causes cross-fragmentation of data, making firewalls and malware scanners ineffective when they only see traffic from one path. Additionally, SSL decryption will become ineffective due to end-to-end encryption protocols.

SCTP was designed with some features to improve security, such as a "4-way handshake" (vs. "three-way handshake" in TCP) to prevent SYN-flood attacks, and a large cookie to verify association authenticity. Reliability was one of the key aspects of SCTP security design. Multi-homing allows the association to remain open even if some routes and interfaces in use become unavailable. This makes it possible to achieve resilience during short-term outages to support telecommunications services, even in the event of serious network anomalies. There is protection against DDoS attacks. Encryption is not part of the original SCTP design.

Although SCTP has some security methods, it does not have the same level of support and ecosystem for security as TCP. But it should be noted that, unlike TCP, there are no well-known facts of successful attacks on infrastructures using the SCTP data transfer protocol. It is also worth noting that when using the Transport Layer Security (TLS) protocol in connection with SCTP, a sufficiently high level of information security during transmission can be achieved.

Having examined the SCTP protocol for compliance with other requirements for data transmission protocols in a prospective automated system of scientific (scientific and technical) information exchange in the Armed Forces of Ukraine, namely: multithreading, control of data flows, resistance to failures, support of operating systems used in the Armed Forces of Ukraine , it can be argued that the Stream Control Transmission Protocol fully complies with them (RFC4960, 2015; Seggelmann, 2012).

Discussions

Analyzing the latest publications in the field of research on data transmission protocols of transport and other levels of network models (Kostiuk, 2021; Ivanchuk, 2020; Malokhvii, 2022; Zhikharev, 2022; Svitlichnyi, 2018; Chaudhari, 2018; Kravchenko, 2020; Moskvin, 2022), it is possibly come to the following conclusions:

– in general, only the most frequently used protocols are considered, some of them are outdated and vulnerable to modern attacks;

– the analysis is carried out on the basis of one of the parameters of the protocols, the characteristics are not considered in the complex and the disadvantages and advantages of each protocol are not taken into account, in accordance with the task;

– research is based on consideration of protocols of higher levels of network models;

– insufficient information on the use of the latest technologies in the field of ensuring the functioning of educational and scientific systems;

– scientists of the russian federation are considering the use of more modern data transmission technologies in their automated systems (including military ones) as opposed to outdated domestic systems.

Thus, due to the insufficient number of studies in the field of using data transmission protocols in automated information exchange systems, it is not possible to give a thorough answer about the rationality of using this or that tool in certain systems. The need for modern and secure methods of information exchange necessitates the analysis of this field, with the definition and explanation of the role of protocols that can be used for data transmission in a prospective automated system of exchange of scientific (scientific and technical) information in the Armed Forces of Ukraine.

Conclusion

The transport layer ensures the reliability of information communication between two end nodes, and the TCP/IP protocol stack provides transport services to application processes. The transport services of these protocols have differences.

Among the analyzed protocols, the SCTP protocol stands out for its scalability, reliability, security support and other functions. This makes it a better option for modern networks and applications, especially in situations where seamless transmission of information is important.

Thus, in accordance with the above functions of the given system, the use of the SCTP protocol is more appropriate for the exchange of scientific (scientific and technical) information.

The perspective of further research is seen in the analysis of the expediency of using the latest data transfer protocols Tachyon, FASP and determining their compatibility with other existing data transfer protocols for their use in an automated system of exchange of scientific (scientific and technical) information.

Recommendations

The results of the above material may be useful to researchers involved in the description and creation of automated systems for military purposes.

References

1. Papastergiou Giorgos; Fairhurst Gorry; Ross David; Brunstrom Anna; Grinnemo Karl-Johan; Hurtig Per; Khademi Naeem; Tüxen Michael; Welzl Michael; Dragana Damjanovic; Mangiante Simone (2017). De-Ossifying the Internet Transport Layer: A Survey and Future Perspectives. IEEE Communications Surveys & Tutorials. 19: pp. 619–639.
2. Computer networking: a top-down approach. James F. Kurose, University of Massachusetts, Amherst, Keith W. Ross, NYU and NYU Shanghai. Seventh edition. Hoboken, New Jersey. Pearson. 2017.
3. Reference Implementation for SCTP - RFC4960. - "This is the reference implementation for SCTP. It is portable and runs on FreeBSD/MAC-OS/Windows and in User Space (includinglinux).». URL: https://github.com/sctplab/sctp-refimpl
4. Seggelmann R.; Tuxen M.; Rathgeb EP SSH over SCTP – Optimizing a multi-channel protocol by adapting it to SCTP. Communication Systems, Networks & Digital Signal Processing (CSNDSP). 8th International Symposium on: journal. 2012. 18 July. P. 1–6. ISBN 978-1-4577-1473-3.
5. Kostjuk Ju., Shestak Ja. Transportnyj riven'modeli ISO/OSI v komp'juternyh merezhah. Tovary i rynky. Mizhnarodnyj naukovo-praktychnyj zhurnal. 2021. No. 4. P. 49–58.

6. Ivanchuk O., Zavhorodniy V., Kozel V., Drozdova E. Analysis of data exchange protocols for managing Internet of Things systems. Scientific notes of the Tavriiski National University named after V. Vernadskyi. Series: Technical sciences. Volume 31 (70). Part 1. 2020. No. 2. P. 99–104.
7. Malochvii E., Molchanov G., Parzhin Yu. Research of data transfer protocols in the conditions of the Internet of Things. Management, navigation and communication systems. Coll. of science Ave. Issue 1 (67). 2022. P. 71–74.
8. Zhikharev A., Fefelov O., Mamatov M. Overview of some data transfer protocols from the perspective of their security. Scientific result. Information technologies. Vol. 7. 2022. No. 1. P. 27–31.
9. Svitlichny V., Onyshchenko Yu. Protocols, methods and technologies for protecting computer networks at the transport level. Actual issues of combating cybercrime and human trafficking (Kharkov, November 23, 2018). Kharkiv. KhNUAF 2018. P. 308–311.
10. Chaudhari, Ketulkumar Govindbhai. Analysis on Transport Layer Protocols and Its Developments (2018). International Journal of Innovative Research in Computer and Communication Engineering. 6(9). 7707–7712. Available at SSRN: https://ssrn.com/abstract=3729064 or http://dx.doi.org/10.2139/ssrn.3729064
11. Kravchenko M., Nikityn A., Spiridonov S. On the unification of data exchange between heterogeneous means and systems in a single information space. I-methods. 2020. No. 2.
12. Moskvin A. Technologies of multithreaded data transfer in information systems. Materials XXII International scientific and practical conf. named after E. Algazinova. Ed. D. Borisov. Voronezh. 2022. P. 688–696.